[+] (IN)SECUREMagazine

Issue 52, 12/2016

DON'T LET YOUR SECURITY EDUCATION & AWARENESS TO TAKE THE BACK SEAT

THE DEVIL IS IN THE DETAILS: WHAT YOUR METADATA SAYS ABOUT YOU

ICS SECURITY

WILL CYBERSECURITY CHANGE WITH A CHANGE IN ADMINISTRATION?

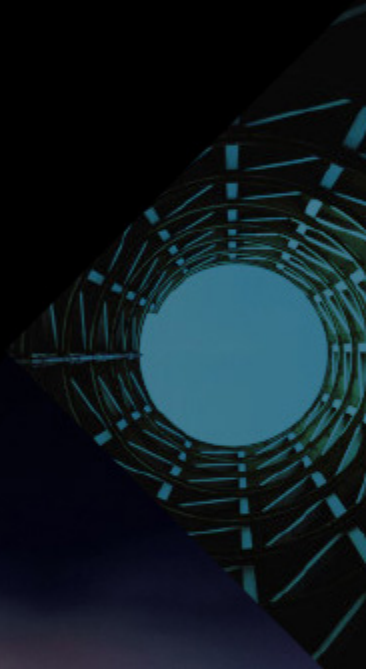
HEALTHCARE SECURITY: COMBATING ADVANCED THREATS

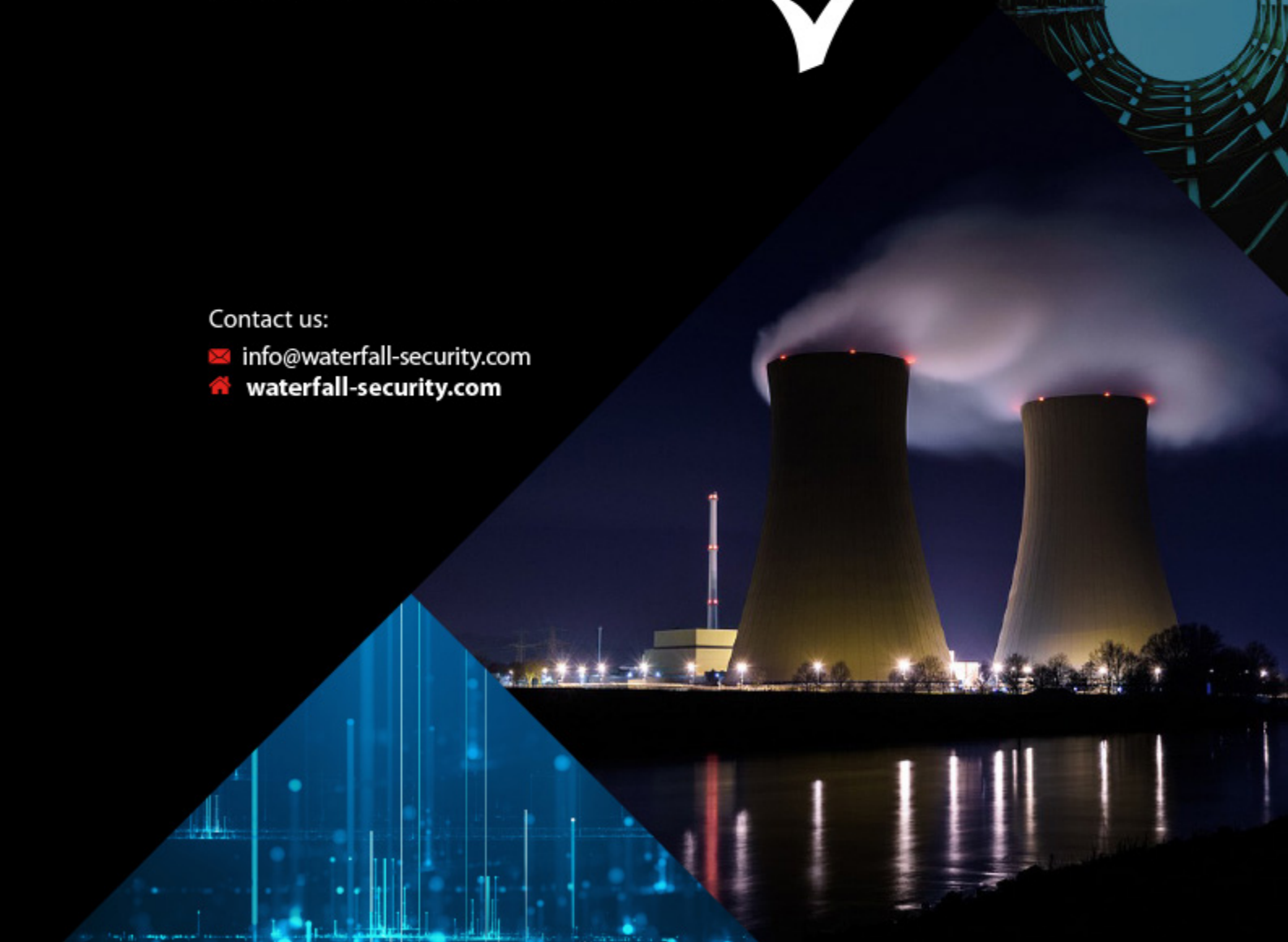
WATERFALL®
Stronger Than Firewalls

- ☑ Intrusion detection
- ☑ Patching & updates
- ☑ Access control & OS hardening
- ☒ **Do they really work?**

Prevent remote cyber attacks:

Deploy Waterfall Unidirectional Security Gateways at your industrial network perimeter and get real security ✓





Contact us:

info@waterfall-security.com

waterfall-security.com

TABLE OF CONTENTS

(IN)SECURE Magazine 52
CONTRIBUTORS LIST

- **Wieland Alge**, VP & GM EMEA at Barracuda Networks
- **Jack Danahy**, CTO at Barkly
- **Andrew Ginter**, VP of Industrial Security at Waterfall Security Solutions
- **Zoran Lalic**, Chief Risk Officer at CyberVue
- **Jeff Schilling**, Chief of Operations and Security at Armor
- **John Schuch**, Senior Architect and Security Practice Lead at Gorilla Logic
- **Gary Sockrider**, Principal Security Technologist at Arbor Networks
- **Emily Wilson**, Director of Analysis at Terbium Labs
- **Elad Yoran**, Executive Chairman at KoolSpan
- **David Zahn**, GM of Cybersecurity at PAS

Visit the magazine website at www.insecuremag.com

Feedback and contributions: **Mirko Zorz**, Editor in Chief - mzorz@helpnetsecurity.com
News: **Zeljka Zorz**, Managing Editor - zzorz@helpnetsecurity.com
Marketing: **Berislav Kucan**, Director of Operations - bkucan@helpnetsecurity.com

The global decline of cybersecurity confidence

Tenable Network Security solicited insights from 700 security practitioners in nine countries and across seven industry verticals to calculate a global index score reflecting overall confidence that the world's cyber defenses are meeting expectations.

According to this year's data, global cybersecurity confidence fell six points over 2016 to earn an overall score of 70 percent — a "C-" on the report card.

The overall decline in confidence is the result of a 12-point drop in the 2017 Risk Assessment Index, which measured the ability of respondents to assess cyber risk across 11 key components of the enterprise IT landscape.

For the second straight year, practitioners cited the "overwhelming cyber threat environment" as the single biggest challenge facing IT security professionals today, followed closely by "low security awareness among employees" and "lack of network visibility (BYOD, shadow IT)."

"Today's network is constantly changing — mobile devices, cloud, IoT, web apps, containers, virtual machines — and the data indicate that a lot of organizations lack the visibility they need to feel confident in their security posture," said Cris Thomas, strategist, Tenable Network Security. "It's pretty clear that newer technologies like DevOps and containers contributed to driving the overall score down, but the real story isn't just one or two things that need improvement, it's that everything needs improvement."

Cloud darkening – Cloud software as a service (SaaS) and infrastructure as a service (IaaS) were two of the lowest scoring Risk Assessment areas in the 2016 report. SaaS and IaaS were combined with platform as a service (PaaS) for the 2017 survey and the new "cloud environments" component scored 60 percent (D-), a seven point drop compared to last year's average for IaaS and SaaS.

A mobile morass – Identified alongside IaaS and SaaS in last year's report as one of the biggest enterprise security weaknesses, Risk Assessment for mobile devices dropped eight points from 65 percent (D) to 57 percent (F).

New challenges emerge – Two new IT components were introduced for 2017 — containerization platforms and DevOps environments.

Massive cybercrime infrastructure demolished

After more than four years of investigation, an international criminal infrastructure platform known as Avalanche has been dismantled.

The Avalanche network was used as a delivery platform to launch and manage mass global malware attacks and money mule recruiting campaigns. It has caused an estimated EUR 6 million in damages in concentrated cyberattacks on online banking systems in Germany alone. The monetary losses associated with malware attacks are estimated to be in the hundreds of millions of euros worldwide, although exact calculations are difficult due to the high number of malware families managed through the platform.

The global effort to take down this network involved the support of prosecutors and investigators from 30 countries. As a result, 5 individuals were arrested, 37 premises were searched, and 39 servers were seized. Victims of malware infections were identified in over 180 countries. Also, 221 servers were put offline.

User2 (non-admin) gets access denied by SAMRi10 when calling Net User remotely to a hardened Domain Controller

SAMRi10: Windows 10 hardening tool for thwarting network recon

Microsoft researchers Itai Grady and Tal Be'ery have released another tool to help admins harden their environment against reconnaissance attacks: SAMRi10 (bit.ly/2gbnMtI).

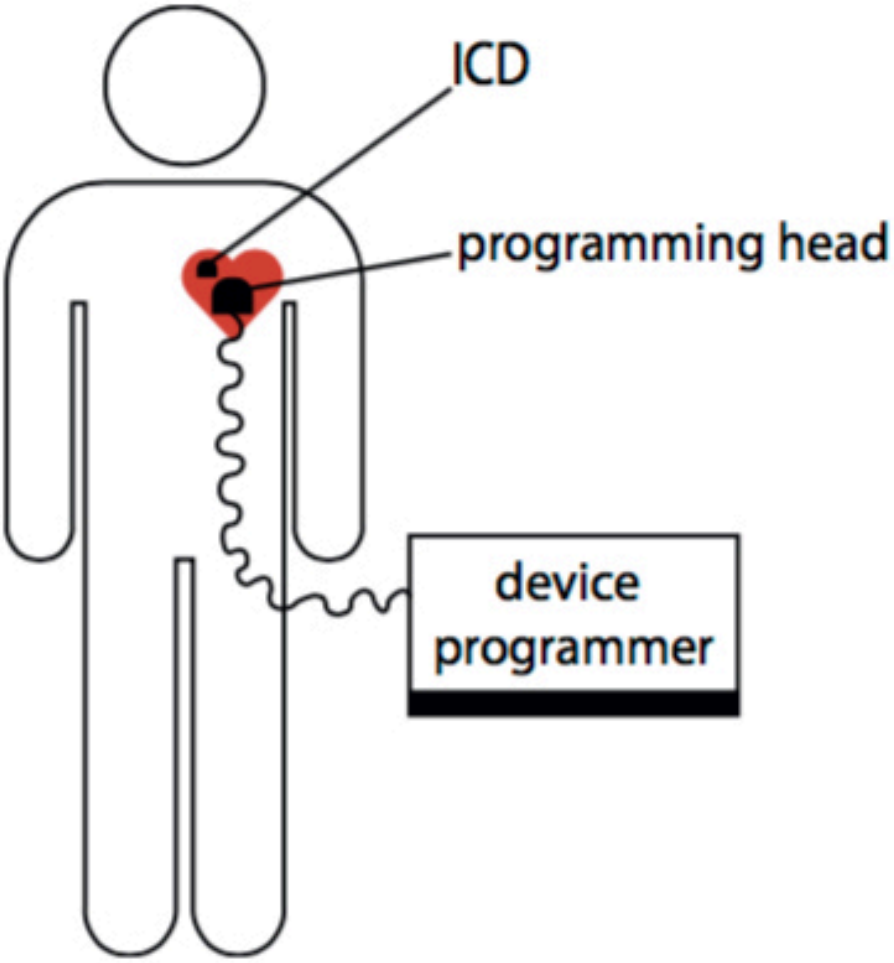
Both the Net Cease tool they released in October and SAMRi10 are simple PowerShell scripts and are aimed at preventing attackers that are already inside a corporate network from mapping it out and find their next target (workstation, server, etc.)

The former does so by altering Net Session Enumeration (NetSessionEnum) default permissions, the latter by altering remote SAM access default permissions.

"Querying the Windows Security Account Manager (SAM) remotely via the SAM-Remote (SAMR) protocol against their victim's domain machines, allows the attackers to get all domain and local users with their group membership and map possible routes within the victim's network," the researchers noted, adding that some attack frameworks have already automated that mapping process.

"Prior to Windows 10 and Windows Server/DC 2016 the option to limit remote access to SAM didn't exist. With Win 10 and Win 10 anniversary edition, the SAMRi10 will limit the remote access to Local Administrators/Domain Admins and any member of 'Remote SAM Users' (admin or non-admin)," Grady explained to us in an email.

"Hardening Windows 10 workstations and Windows Server 2016 will limit the access to their local accounts and groups info over remote SAM. Hardening Domain Controller 2016 (promoted Windows Server 2016) will limit the access to the domain accounts and groups info over remote SAM."



Insecure pacemakers can be easily hacked

A group of researchers has discovered that it's not that difficult for a "weak adversary" with limited resources and capabilities to fiddle with or even shut down a variety of insecure pacemakers and Implantable Cardioverter Defibrillators (ICDs), putting the lives of the individuals who use them in jeopardy.

The researchers have intentionally used inexpensive commercial off-the-shelf equipment and a "black box" approach to reverse-engineering the communication protocol used by the device to "talk" to the device programmer – all to prove that the hacking of these devices is not just reserved for expert attackers.

"Implantable medical devices typically use proprietary protocols with no or limited security to wirelessly communicate with a device programmer," they noted. "Our analysis of the proprietary protocol results in the identification of several protocol and implementation weaknesses."

Some security measures have been implemented, but they were not enough. The researchers managed to reverse-engineer the long-range communication protocol, activate the ICD by bypassing the current activation procedure, and intercept, modify and deliver malicious instructions to the device.

They found that they could:

- Collect personal information about the patients and info about their treatment
- Mount DoS attacks against the devices (e.g. drain the ICD battery)
- Mount replay attacks
- Send arbitrary commands to the ICD.

All these attacks don't require the attacker to be in close proximity with the patient – it's enough that they are two to five meters away.

They vulnerabilities they found apply to (at least) 10 types of ICDs that are currently on the market, all made by the same (unnamed) manufacturer. The implant maker has pushed out an update for the software.

Waterfall BlackBox: Restoring trust in network information

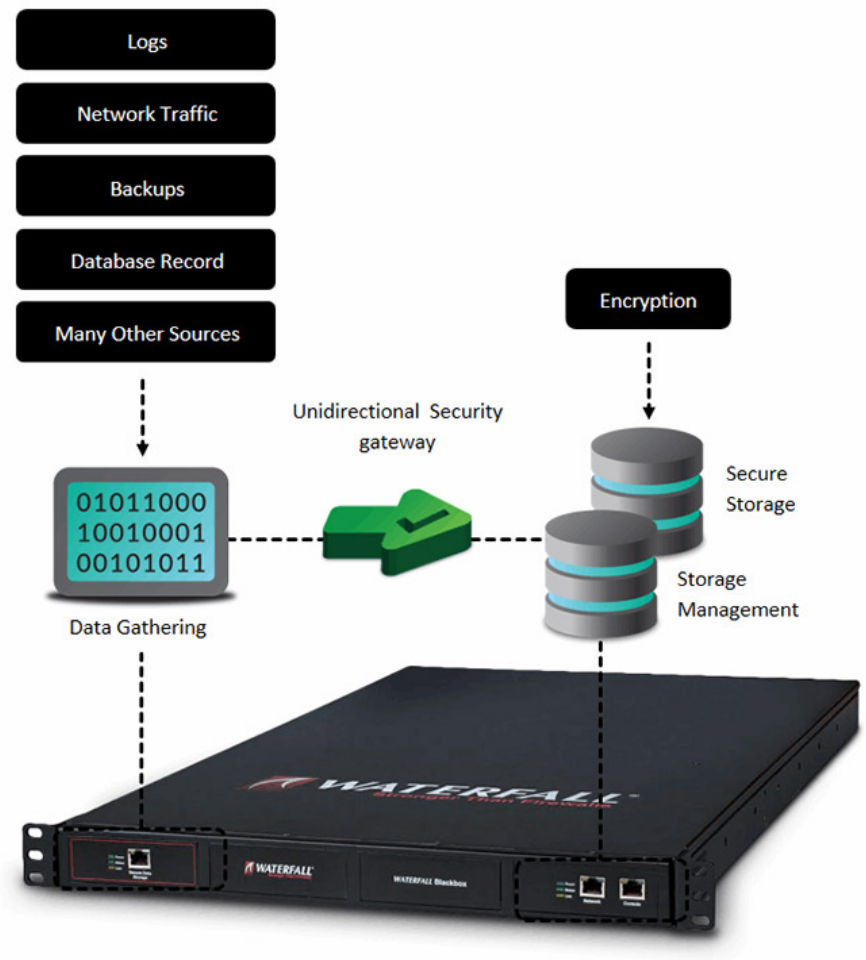
Waterfall Security Solutions announced the launch of the Waterfall BlackBox, developed to maintain the integrity of log repositories in the event of a cyber attack. Based on Waterfall's patented unidirectional technology, the Waterfall BlackBox creates a physical barrier between networks and logged data, so that stored logs become inaccessible to attackers who are trying to cover their tracks.

"We have been deploying our Unidirectional Security Gateway products in industrial networks worldwide for the past decade, while gaining unparalleled insight into real-life cyber attacks and protections as a result. As the market leaders for strong security, we have developed a number of innovative solutions, the Waterfall BlackBox being the most recent," said Lior Frenkel, CEO and co-founder at Waterfall Security Solutions. "Until now, response teams and forensic experts could not be sure if an attacker had tampered with or manipulated network and security logs in order to distort the results of incident-response efforts and audits."

Network, application and security logs are vital to forensic activity, incident response, audits and risk analyses. These logs record evidence of attacks and details of attacker activities on compromised networks. In modern attacks, once inside a network, attackers take deliberate measures to "cover their tracks" by removing or altering incriminating or revealing information in log repositories.

Covering tracks is typical of attacks on networks with local, centralized and even cloud-based logging systems. Logs and log repositories accessible from the attacked network are always suspect of being manipulated The Waterfall BlackBox secures logs "behind" a unidirectional gateway, ensuring that logs are physically kept trustworthy and out-of-reach of cyber attackers.

"The Waterfall BlackBox is a totally new solution in the market, enabling us to provide unmatched security solutions to customers in financial, enterprise and healthcare markets, in addition to our existing industrial control networks users," added Frenkel.

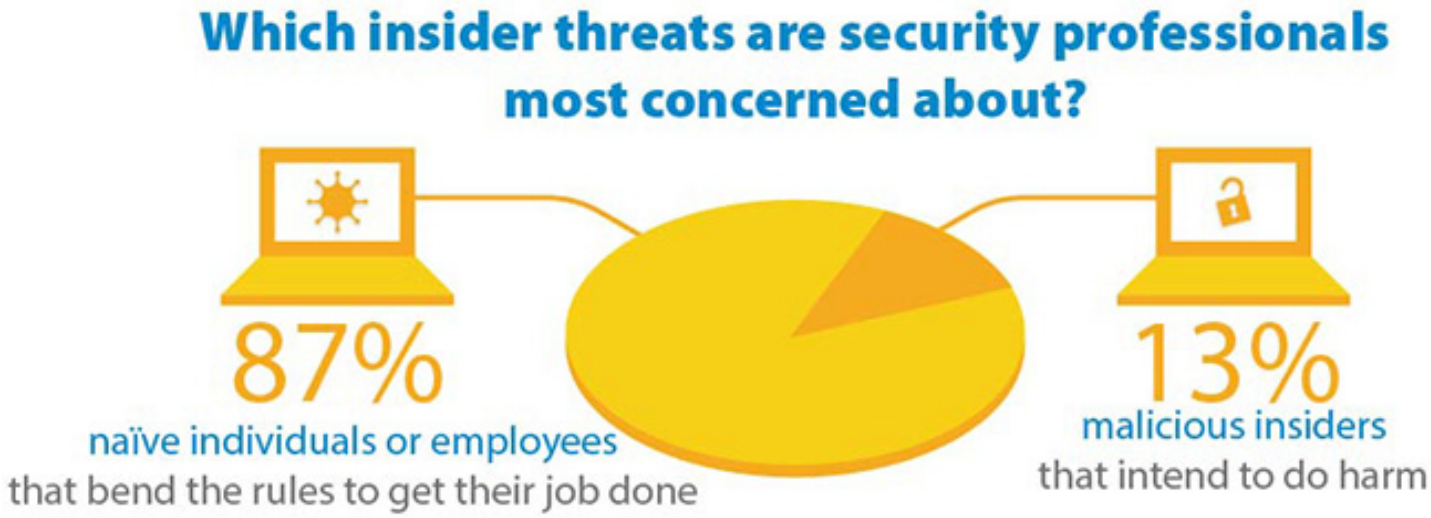


Intentional or not, insider threats are real

Despite the perception that hackers are a company's biggest cybersecurity threat, insiders, including careless or naive employees, are now viewed as an equally important problem, according to a survey by Dimensional Research.

Researchers found that 49 percent of IT security professionals surveyed are more concerned about internal threats than external threats. Malware installed unintentionally by employees was the top concern of respondents, ahead of stolen or compromised credentials, snatched data and abuse of admin privileges.

"Internal threats are emerging as equally as important as external threats, according to respondents. This means that an employee cutting corners to get their job done more efficiently is viewed as potentially just as dangerous as a malicious external hacker," said Diane Hagglund, founder and principal of Dimensional Research. "Yet these views aren't reflected in the allocation of security budgets, which is traditionally focused on perimeter security."



Europol terrorism investigations data found exposed online

700 pages of confidential dossiers, which included details about terrorism investigations in Europe, have been found exposed on the Internet by the reporters of Dutch TV documentary programme Zembla. They were housed on a private Iomega network drive located in the home of a former Europol officer who now works for the Dutch police.

The reporters discovered the documents through Shodan, a search engine for finding devices connected to the Internet. The drive in question wasn't password-protected, and easily accessible to anyone via Internet. It contained documents on historic terrorism investigations (2004 Madrid train bombings, foiled attacks on airplanes with liquid explosives, etc.) but also details about investigations that were never made public.

Europol Deputy Director of Operations Wil van Gemert said that the data leak has not affected ongoing terrorism investigations, even though they cannot be entirely sure that someone other than the Zembla reporters accessed the files.

"The concerned former staff member, who is an experienced police officer from a national authority, uploaded Europol data to a private storage device while still working at Europol, in clear contravention to Europol policy," Europol spokesperson Jan Op Gen Oorth explained.

"A security investigation regarding this case is on-going, in coordination with the respective authorities at national level to which the staff member returned. Current information suggests that the security breach was not ill-intended."

Internet freedom around the world keeps decreasing

For the sixth year in a row, Internet freedom is declining.

According to the latest Freedom on the Net report, 67 percent of all Internet users now live in countries where online criticism of the government, ruling family or the military is subjected to censorship, and such activity can result in individuals getting arrested.

Also, more governments have come to realize the power of social media and messaging apps, and are actively trying to censor them or prevent their use, particularly during anti-government protests, but also because they help thwart their surveillance efforts.

"The increased controls show the importance of social media and online communication for advancing political freedom and social justice. It is no coincidence that the tools at the center of the current crackdown have been widely used to hold governments accountable and facilitate uncensored conversations," says Freedom House, the NGO that compiled the report that focuses on developments that occurred between June 2015 and May 2016.

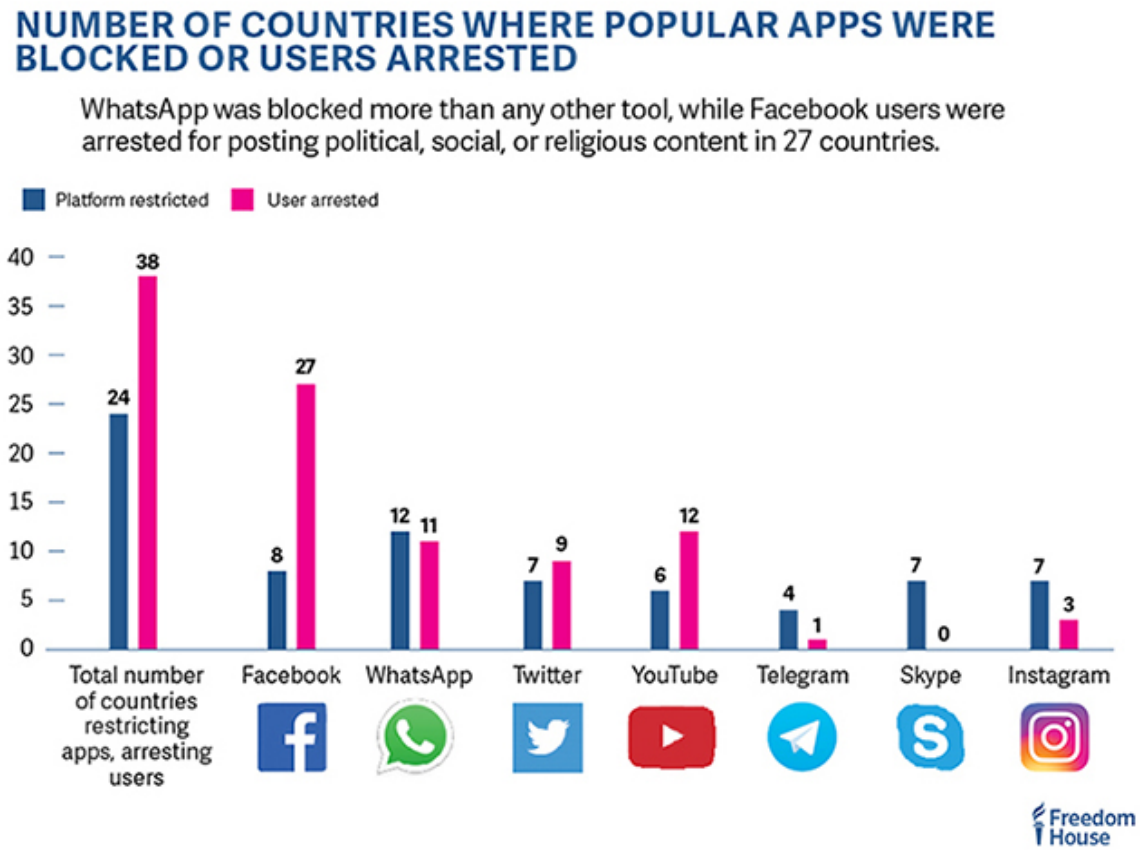
"Authorities in several countries have even resorted to shutting down all internet access at politically contentious times."

The "problem" with some communication apps is that they encrypt the exchanges, but it's interesting to note that the use of some online voice and video calling apps is being blocked or restricted in a number of countries, mainly because they eat away at the profit margins of national telecommunications firms.

The range of censored online content is also expanding, and includes news outlets that favor political opposition, sites that launch calls for protest, sites expounding LGBTI issues, and images.

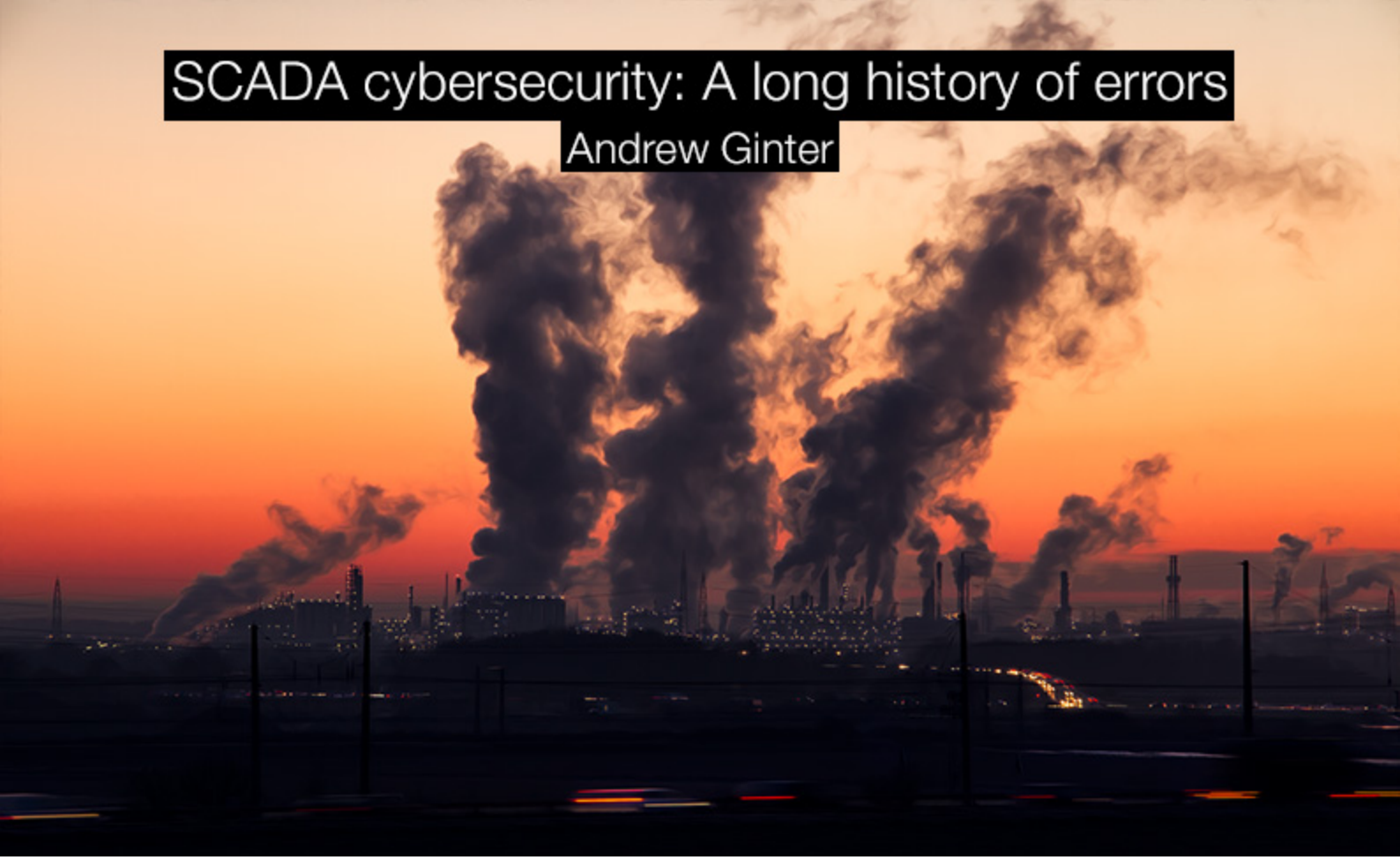
China, Syria, Iran, Ethiopia and Uzbekistan lead the pack of countries with the smallest amount of Internet freedom. On the other end of the spectrum are Estonia, Iceland, Canada, the US, and Germany.

"Of the 65 countries assessed, 34 have been on a negative trajectory since June 2015. The steepest declines were in Uganda, Bangladesh, Cambodia, Ecuador, and Libya," Freedom House noted.



SCADA cybersecurity: A long history of errors

Andrew Ginter



Much has been written about the greatest SCADA security issue: the risk that a cyber attack will shut down important industrial processes, cripple critical infrastructure, or cause an environmental or human disaster. The threat is real. The problem is that most of what has been written is either subtly or grossly wrong, and some is utter nonsense.

The first generation of SCADA security advice, published roughly during the years 2003-2011, is subtly wrong. The defense-in-depth posture advocated by this advice is costly, is often itself a threat to industrial safety and reliability, and fails to protect SCADA systems against modern attacks.

Most of this advice is based on IT security principles, which fail to protect IT networks completely – all such networks are regarded by IT experts as essentially constantly compromised. Intrusion detection and practiced incident response teams are considered best practices by IT experts. Response teams constantly seek to identify compromised computers, erase them, and restore them from backups.

The essential problem with applying IT security principles to SCADA systems is this: there is no way to restore lost production, damaged turbines, or human lives from backups.

It is, therefore, not surprising that the state of SCADA security is, on average, poor to atrocious in the vast majority of highly-computerized industrial sites all over the world.

My goal here is to outline what is emerging as a new way of understanding SCADA security, and is increasingly reflected in modern advice published since 2010 (or so). Preventing the compromise of our SCADA systems and misoperation of our physical processes must be the main priority, not detecting and remediating intrusions after the damage is done.

Physical and network perimeter protections are the essential, primary protections in this new approach. Costly IT security measures with limited effectiveness, including security update programs, encryption and intrusion detection systems, should all be secondary measures, addressing only residual risks. We can and should control our investment in these secondary measures to reflect their

limited effects in terms of risk reductions. IT experts will tell us this approach and this article are hopelessly ill-conceived. They are wrong. Anyone who works every day in the kill-zone of an "industrial incident" has a real, personal interest in deploying the strongest, practical, protective measures for SCADA systems. Everyone who is exposed every day to industrial risks is the focus for this article.

We hope to provide enough information here to make the case for effective SCADA security systems, to protect our industrial practitioners from cyber attacks, and to protect all of us by keeping our essential industries running reliably in an increasingly connected, and increasingly hostile world.

Understanding SCADA systems

SCADA systems are the computers that control important, complex, and often dangerous physical processes, many of which constitute the physical infrastructure critical to modern societies, and whose misuse generally has unacceptable consequences. To understand misuse, and how to prevent it, we need some understanding of what a SCADA system is, and how it works.

Industrial control systems are old – people were controlling physical processes with dials and gauges before there were computers, and have been using computers to assist with such control almost since the first computers were invented. As with any old field, the terminology is arcane. What the press calls a SCADA system is a misnomer.

Technically, SCADA stands for Supervisory Control and Data Acquisition. A SCADA system is an industrial control system that spans a wide-area network (WAN) over long distances. Electric grids, pipelines and water distribution systems use SCADA systems.

In contrast, DCS stands for Distributed Control System. A DCS is an industrial control system where no WAN is involved, and the entire physical process is contained in one comparatively small site. Power plants, refineries and chemical plants use DCSs. Historically, SCADA systems and DCSs were different – one kind of software could not control the other kind of processes. Nowadays, general-purpose control system software has all of the features of both SCADA systems and DCSs, so the difference between the two terms is more usage than technology.

The modern term encompassing DCSs, SCADA systems and all other kinds of control systems is Industrial Control System (ICS). This means that, technically, here we should be talking about Industrial Control System security, not SCADA security. However, since many readers are non-technical business decision-makers, we will use the terms SCADA security, ICS security and control system security largely interchangeably, as does the media.

Industrial processes can be subdivided as well. Most critical infrastructures are examples of "process industries." In process industries, the material being manipulated is more or less "goo" at some point in the physical process. For example, water purification systems manipulate water, refineries manipulate oil, and pipelines move fluids. Electric grids are considered process industries as well, because electricity is produced in a continuous stream that can be modeled as more or less a fluid. Even railway and traffic control systems are considered process systems, though this pushes the concept just a bit.

Within process industries, there are batch industries and continuous industries. Batch industries, such as refining and pharmaceuticals, are industries where the production line does not run continuously. Instead, it produces identifiable batches of outputs. Continuous industries, such as water treatment plants, power plants and offshore oil production platforms, consume inputs and produce outputs more or less constantly.

Discrete manufacturing is the opposite of process industries. While process industries work with continuous inputs, discrete manufacturing assembles small, discrete input components into larger outputs, such as automobiles, aircraft, and home appliances.

There are many similarities between control systems in process and discrete manufacturing, but there are significant differences as well.

For example, when a control system in a process plant is sabotaged and the physical process is misoperated, there is often a real risk to human life at the plant and to the safety of the public in the immediate vicinity of the plant.

When a control system in a discrete manufacturing plant is sabotaged, there can be a risk to any human operator working close to the affected machines or robots, but there is generally no immediate public safety risk.

In both cases though, there is a real risk that the physical industrial process will be shut down as a protective measure. Such shutdowns are always costly to the business operating the industrial process, and can have societal consequences when the physical process constitutes a critical infrastructure.

Most of the examples in this article are about control systems in process industries, not discrete manufacturing. Cybersecurity issues in the two domains are similar though, differing more in degree than in kind.

An important aspect common to all SCADA systems is the human operator.

An important aspect common to all SCADA systems is the human operator. Control systems at important industrial facilities almost always have one or more human operators charged with ensuring the safe and reliable operation of the physical process.

These operators use tools known as “human-machine interface” (HMI) software. This software almost always includes a graphical visualization of the state of the physical process, and often includes other elements such as alarm managers and historical trending tools.

By policy and sometimes by law, these operators are required to have a high degree of confidence that the process is operating safely in order to permit the process to continue operating. If the operator ever loses such confidence, for example because their displays freeze or a message pops up saying “you have been hacked,” they must take action.

An affected operator may transfer control of the process to a secondary or redundant HMI or control system. If however, after some seconds or minutes, the operator is still not sufficiently confident of the correct and safe operation of the physical process, that operator must trigger a shutdown of the physical process.

This means that the simplest way for an attacker to cause physical consequences is to impair the operation of some part of an operator's HMI or the systems supporting the HMI. The simplest physical consequences of such attacks are shutdowns of the physical process.

Many industrial processes can be shut down much faster than they can be started up, and it can take days to recover full production after an emergency shutdown. In some cases, regulatory approvals must be obtained before restarting physical processes, delaying plant restarts by as much as months. Worse, emergency shutdowns can often put physical stress on industrial equipment, leading to immediate equipment failures or premature equipment ageing.

IT/OT integration

Since roughly the mid-1990s, IT/OT integration has been an important trend in SCADA systems. IT is information technologies, and OT is operations technologies or, more colloquially, SCADA systems. The IT/OT integration trend is towards integrated IT and OT teams, business processes, products, technologies, and networks.

Since both SCADA/OT and IT networks increasingly use the same computing hardware, operating systems, platform applications and networking components, there are cost savings and other benefits to merging these technology teams, application platforms, networks and business practices.

Why, for example, should one relational database vendor's product be used in a SCADA network when the business had already purchased an enterprise-wide license to deploy a different vendor's databases?

The problem with naïve IT/OT integration, though, is that when the same technology is used on IT and SCADA networks, and when IT and SCADA networks are thoroughly interconnected, many of the same kinds of cyber attacks that succeed on IT networks succeed on SCADA networks – and there are a great many attacks of this kind.

The laws of SCADA security

SCADA security is focused on preventing any unauthorized operation of SCADA system computers. SCADA security is a more recent discipline than SCADA systems or automation systems, but is no less confusing.

Newcomers to the security field see a bewildering variety of types of vulnerabilities, attacks, and defensive systems.

Combine this with the perennial admonition that "a chain is only as strong as its weakest link," and the task of defending control systems can seem impossible to pull of successfully.

This bewildering variety is an illusion. All vulnerabilities in software, and in systems of hardware, software and networks, are bugs or defects. The bewildering variety is simply the result of people trying to classify all possible defects – all the possible ways people can produce software and systems incorrectly. All such classification systems are doomed to fail – people can make mistakes in an uncountable number of ways.

This perspective simplifies much of the security research, as well. When the only results of such research are new vulnerabilities in existing software products, this research is no more than post-product-release quality assurance (QA). To be fair, not all security research produces QA-like results. For example, the most useful research into vulnerabilities identifies entirely new kinds of vulnerabilities that nobody had before considered, and that all product developers must now start to consider and avoid.

Research into defensive techniques, their application and their effectiveness is, of course, much more than QA. However, the vast majority of previously-undiscovered zero day vulnerabilities and exploits revealed at events such as the annual Black Hat conference are no more than new security defects discovered by unpaid, post-release QA security researchers.

In hopes of simplifying the field of cybersecurity to the point where SCADA practitioners can make sense of and routinely apply sound security practices, I propose three laws of SCADA security. These laws address fundamental cyber-security concepts that are poorly understood, and poorly communicated.

Law #1 - Nothing is secure

Security is a continuum, not a binary value. Given enough time, money and talent, any security setup can be breached. Anyone using terms such as secure communications, secure boot or secure operating system is either selling something, or has just been sold a bill of goods.

This is important. It changes the conversation from "Never you mind, I have security covered" to "Just how secure are we?" and, ultimately, "How secure should we really be?"

Law #2 - All software can be hacked

All software has bugs. Software development teams work hard to eliminate what bugs they can, but in spite of their best efforts, all software - even security software – has bugs. Some bugs result in exploitable security vulnerabilities. For evidence of this, simply look at the support section of any software vendor's website and see how many security updates have been issued recently. In practice, this means that all software can be hacked.

This is important. Too many of us believe that patching known bugs and vulnerabilities makes us invulnerable. Others believe that the way to make software systems secure is to deploy more security software. This is all nonsense – there are vulnerabilities to be found in any software system, even security software.

Law #3 - All attacks are information and every piece of information can be an attack

Even a single bit of information – a one or a zero – can be an attack. If a plant operator is trying to turn off a piece of equipment with a zero, but an attacker changes that zero to a one, that is an attack. Passwords and malicious intent carried in the brains of people entering a plant can be an attack. Malware installed on brand new computers, or in the tiniest of computers embedded in USB keyboards, can be an attack.

More specifically, every communications message, whether Internet Protocol (IP), old-style RS-232 serial communications, or any other message always contains some sort of information, and can therefore be an attack. The Internet moves information in wholesale quantities. This makes the Internet a great enabler. It makes life so much more convenient for all of us, but also for our attackers.

Every message to any computer is also a kind of control. A computer receiving a message is executing code that the computer would not have executed without the message, and has thus been controlled to some extent by the message. Malformed messages are obvious attacks. Legitimate-seeming messages faking credentials are less obvious. Legitimate-seeming messages misusing legitimate credentials to control physical processes incorrectly are even harder to spot.

This is important. A compromised machine can be used to send messages to other machines and so attack machines deeper into a protected network or system of networks – this is called pivoting an attack. Any computer or device reachable directly or indirectly from the Internet via a path of pivoting through intermediate computers and communications links is at risk of sabotage from the Internet. This includes safety systems and equipment protection systems that are connected, directly or indirectly, to networked machines.

Any computer or device reachable directly or indirectly from the Internet via a path of pivoting through intermediate computers and communications links is at risk of sabotage from the Internet.

Putting the pieces together

Misoperation of industrial processes can have costly or even dangerous outcomes. For example, misoperation of the human-machine interface (HMI) for the SCADA system at British Petroleum's Texas City refinery in 2005 caused an explosion that killed 15 people, injured 180, shut the refinery down for one year, and cost BP one billion dollars in various kinds of damages. Note that this was not a deliberate cyber attack, but misoperation of the HMI by the plant operator in violation of a number of BP's standing policies.

The essence of a SCADA security compromise is this: Any operation that a human operator, such as the Texas City refinery operator, can legitimately instruct an HMI to carry out, an attacker with control of the SCADA system can also instruct the SCADA system to carry out. Although many safeguards are built into HMI and other control-system software components that prevent the operator from instructing the physical process to enter dangerous states, an attacker who has compromised these software components can often bypass the safeguards.

In the worst case scenario, a compromised control system can issue any unsafe command that the compromised computer's hardware is electrically capable of issuing. All software safeties can be compromised. Misoperation of industrial processes is frequently dangerous, and always costly.

These are not theoretical risks. Cyber-attackers have reached into industrial control systems and sabotaged those systems. Industrial processes have been shut down and costly, difficult-to-replace equipment has been damaged. Some examples: The Stuxnet worm physically destroyed roughly 1,000 uranium enrichment centrifuges in Iran in 2010, remote attackers caused massive physical damage to a German steel mill in 2014, and remote attackers interrupted electric power to nearly a quarter of a million Ukrainians in 2015.

The Ukrainian attack was noteworthy in that not only were there physical effects from the attack, but SCADA system hard drives were erased, as well as firmware in communications devices. The former could be corrected by re-installing operating system software and restoring other hard drive contents from backups, provided the utility had such backups, and that the backups were sufficiently synchronized with each other version-wise. Erasing device firmware meant that the communications devices had to be completely replaced. With the firmware erased, there was no way to restore the devices to a condition where they worked again. In cybersecurity parlance, this is called “bricking” the devices.

The severity of consequences of misoperation depends on the design and circumstances of the physical process. Poorly designed and operated nuclear generators pose a greater threat than poorly designed and operated washing-machine manufacturing plants. Industrial sites near large population centers are generally of greater concern than sites located far from such centers.

Industrial processes are powerful tools. At most industrial sites, whoever controls the computers, controls the tools. The concern is that every tool is also a weapon – the greater the tool, the greater the weapon. The bar for better cybersecurity must be raised to the highest level possible to protect society from online attacks on industrial sites. Most certainly, IT-based solutions do not come close.

Andrew Ginter is Waterfall’s Vice President of Industrial Security (www.waterfall-security.com). In this role, Mr. Ginter promotes, evangelizes and communicates Waterfall’s innovative technological approach to cybersecurity for industrial control networks and critical network infrastructures. He spent 25 years leading and managing R&D of commercial products for computer networking, industrial control systems and industrial cybersecurity for leading vendors including Hewlett-Packard, Agilent Technologies and Industrial Defender. Andrew holds degrees in Applied Mathematics and Computer Science from the University of Calgary, as well as ISP, ITCP, and CISSP accreditations.

Andrew is the author of a new book, “SCADA Security – What’s Broken and How to Fix It”, available on Amazon.

Healthcare security: Combating advanced threats

Gary Sockrider

From healthcare organizations to financial institutions, from universities to retail stores, every single business that collects customer data – whether it's personal details, credit card information or real-time behavior – is a target for threat actors looking to steal that information.

Organizations of every size, including some of the largest brand names that you would assume have the most robust defenses, have fallen victim to data security breaches. Health insurer Anthem experienced a major breach in which attackers stole the personal information of 78.8 million current and former members. The US Office of Personnel Management suffered an attack impacting the personal details of 21.5 million individuals. Not to mention Target, Home Depot, Sony Pictures, and so many others that have lost millions of dollars and the personal information of customers and employees alike. And sadly, a new organization joins the long list of victims nearly every day.

For healthcare organizations the data breach threat is bound to get worse, as the frequency and complexity of cyber attacks against the healthcare industry are increasing faster than those of attacks hitting almost any other sector. This is because the value of stolen patient information and its usefulness in committing secondary crimes such as identity theft is continually increasing. And until security defenses can catch up with the skill and sophistication of today's advanced attackers, healthcare organizations will continue to be attractive targets.

A look inside healthcare's current cyber defenses

Luckily, most healthcare organizations aren't starting from zero. Many providers have solidified their defenses over the years with various tools and devices in an effort to harden their

network perimeters. Such tools include firewalls, intrusion prevention systems (IPS), and security information and event management (SIEM) systems. Larger organizations might also have a dedicated security analyst, or even a security operations center (SOC) that monitors and mitigates security threats around the clock.

These tools are arranged in a perimeter and core structure that enables them to deflect attacks before they make it inside the network. For instance, an IPS actively prevents intrusions by dropping malicious packets, resetting connections or blocking all traffic from IP addresses that are known to support malware, whereas an IDS passively detects attacks based on known signatures or statistically anomalous behaviors.

More recently, SIEMs have been deployed to back up IPS/IDS systems. These systems provide a centralized security console that displays information about the overall health of the network and all activity in real-time or near real-time. SIEMs can be monitored by humans, who have the ability to immediately respond to generated alerts so they can quickly initiate whatever mitigation actions are needed. Furthermore, the event management component of SIEM systems can automatically direct responses where they need to go.

Healthcare organizations that have all of these tools deployed on their network will be the most effective at mitigating known threats. Even working alone on a busy network, an IPS system can block hundreds or thousands of attacks every day that otherwise might breach the perimeter if no security tools were in place. However, the challenge that healthcare organizations face is that they are not being attacked by known threats. In most cases, these organizations are being targeted by advanced persistent threats (APTs): stealthy attacks that are specifically designed to defeat even the most advanced perimeter defenses and can go unnoticed and unmonitored within the network for weeks or even months.

Attackers can continually launch assaults for months or even years depending on how badly they want to capture specific data

Why advanced persistent threats are so successful

Although APTs have been around in various forms since at least 2005, they didn't start getting widespread attention until 2011. APTs are described by the National Institute of Standards and Technology as a program and an effort that *"achieves its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltration of information (...) the APT pursues its objectives repeatedly over an extended period of time; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives."*

Threat actors deploying APTs typically use a combination of techniques to breach a network. One could be zero-day exploits (attackers exploit software holes that are unknown to the vendor). A second technique is trawling social media channels for employee data, and then using that data to craft realistic spear phishing e-mail probes designed to mine even more information. A third one is booby-trapping web pages that employees are likely to visit, or can be steered into visiting. When an APT is identified and eliminated by a company's security team, the threat actor might create a different attack with a better chance of succeeding in a subsequent attempt. Attackers can continually launch assaults for months or even years depending on how badly they want to capture specific data protected by the organization they are targeting.

One of the primary reasons that APTs have become so notorious is that once one has infiltrated a network, it is extremely difficult to detect. This is because its function is actually quite passive – either the slow exfiltration of data or discovery of security holes for more powerful follow-up attacks.

Furthermore, most perimeter defenses only look at traffic trying to enter the network. Once an APT has successfully penetrated the network, it can remain undetected inside it for a long, long time.

Healthcare breaches are soaring and repercussions are not trivial

In May 2016, the Ponemon Institue released its Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. According to the study, nearly 90% of healthcare organizations experienced a data breach in the past two years, and 45% suffered more than five data breaches during that same period. And like in years past, criminal attacks were the leading cause (making up 50%) of breaches within the healthcare industry.

To put this in a financial perspective, breaches could be costing the healthcare industry $6.2 billion, with the average cost of a data breach now totalling more than $2.2 million. Some of the largest breaches in the past couple years have been within the healthcare industry. In 2015 Anthem Healthcare had nearly 80 million records stolen, Premera BlueCross lost 11 million records, and the Excellus BlueCross BlueShield breach impacted 10 million customers. In 2016 we're seeing a continuation of this trend with Banner Health suffering 3.7 million compromised records, 21st Century Oncology losing 2.2 million records, and so on.

The repercussions from data breaches can be severe for healthcare organizations. In addition to lost customer confidence and revenue, sometimes providers are additionally penalized if patient records are found to not have been adequately protected. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires that health records be portable enough to follow patients wherever they need to go within the healthcare system, yet also requires that those records be protected. In 2009, Congress further strengthened regulation with the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act, which stipulates that fines could be as high as $1.5 million for every single violation of healthcare information security.

Providers must apply the same rigour and attention to breaches as they do to deadly pathogens and infectious diseases, and put in place appropriate protocols and procedures.

The importance of threat intelligence for healthcare security

The rise of attacks against healthcare organizations is why it's so important that they re-examine their approach towards cyber security. Providers must apply the same rigour and attention to breaches as they do to deadly pathogens and infectious diseases, and put in place appropriate protocols and procedures.

Although current perimeter defenses should certainly be maintained, those defenses can no longer guarantee the safety of a healthcare provider's network given the rise of stealthy and complex attacks such as APTs. These organizations need to be proactive and assume they WILL be breached at some point, and have dedicated security solutions in place that are designed to back up perimeter defenses when they are bypassed by advanced threats.

A key challenge of healthcare's current security protection is that their perimeter defenses are not designed to monitor the movement and activity of users and programs after they are inside the network perimeter. Once inside, an APT rarely starts stealing millions of records immediately. Instead, it performs reconnaissance within the network – sometimes for weeks or months – to establish its foothold, acquire elevated credentials, infect more systems, and contact its command and control servers.

Luckily, there are security programs available that are designed to examine the network as a whole, both inside and at the perimeter, and which can detect an APT's movement.

Intelligence into known threats is another area sorely lacking in healthcare's current defenses. Hundreds of IP address ranges are used to launch threats against health providers, with many of the IP addresses previously unknown as malware hosts. If threat intelligence can correlate IP addresses with other metadata such as URLs, FQDNs, email addresses, social media, and so on, the result will be higher fidelity intel with fewer false positives.

By combining this type of intel with the valuable insights gleaned after a breach, health providers would have a clearer picture of who their attackers are, what data they are attempting to corrupt or steal, and the techniques and attack tools they are deploying.

With this intelligence, breaches can be seen as components of a larger attack campaign being launched against an organization, instead of merely a series of disparate events. This enables healthcare organizations to put specific defenses in place to stop individual attackers targeting them, and even predict where and how their attackers will try to strike next.

To take cyber defense a step further, it is important that the healthcare community shares information about attackers and techniques.

To take cyber defense a step further, it is important that the healthcare community shares information about attackers and techniques so that all organizations can benefit without first needing to fall victim to an attack themselves.

Armed with this information, defenders can learn to consistently counter attacks, turning one of APTs biggest assets (its persistency) against itself. Every healthcare provider that deploys a threat intelligence program to back up its existing network defenses and starts sharing its threat data with other organizations makes the entire community stronger.

Eventually that strength and intelligence will overcome the insidious threat that APTs pose.

Gary Sockrider is a Principal Security Technologist at Arbor Networks (www.arbornetworks.com).

Don't let security awareness and education take the back seat

Zoran Lalic

Recent cybersecurity reports indicate that over 70% of all data breaches included some type of social engineering to gain a foothold in an organization.

New threats, risk and vulnerabilities pop up on a daily basis. The automatic reaction to this evolving threat landscape is technology - organizations typically implement additional layers of security such as an IPS, DLP, and web-content filtering to detect and prevent attacks. But in reality, many high-profile data breaches have demonstrated that this approach is insufficient and that hackers typically spear-phish their way into the organization's network. Attackers prefer crafting a few malicious emails to spending days or weeks trying to hack your firewall and risk their efforts being detected and blocked.

People are typically the weakest link in the security chain so, more often than not, it is they (and not technology) who become the hackers' priority. Social engineering is a very common approach to exploiting the human element during an attack. It is a non-technical attack whose aim is to trick people into performing unintended actions and give away sensitive information.

A key concept of this tactic is to use the target's own employees to bypass internal security controls. Social engineering takes many forms, including phishing, spear-phishing, vishing, pretexting and tailgating.

What can we do to prevent our employees from becoming a bridge to data compromise?

The answer is: establish and maintain a proper security awareness and education program.

Many organizations put their primary focus on technology, and eschew this essential piece of the overall information security puzzle, or set up an inadequate security awareness program just so they can say they have one. But organizations must understand that providing security training once or twice a year is not an acceptable approach in this day and age - it takes ongoing education and awareness efforts to change the employees' behavior.

The security awareness and education program must promote security, make employees proud of protecting the organization's assets, and not make them paranoid.

The program should also be fun so that employees are more willing to participate and generally more engaged in it.

My years of experience with security awareness and education program development allow me to offer you the following tips for building a good one:

1. Establish a team that will be responsible for security awareness and education.
2. Make sure your management supports the initiative and understands the program is not just about "opening and clicking on a malicious link."
3. Develop a security awareness and education policy that is approved by your management.
4. All employees, including the CEO, must go through the program.
5. Develop a security education plan that covers all attack methods through which the human element could be targeted. In addition to social engineering, also consider addressing the following issues:
   - Weak passwords
   - Insecure code writing
6. Develop material that will be part of your program:
   - **Posters** – Posters draw employees' attention and help promote and raise security awareness in the organization.
   - **Weekly/daily tip** – Weekly or daily security tips are very important to keep your employees engaged.
   - **Monthly newsletter** – A good candidate for the monthly newsletter is a sample phishing email with phishing indicators. Also, a monthly roundup that includes the latest data breaches and how the employees could have prevented it.
   - **Videos** – To make information security fun for your employees, you might want to consider funny infosec training videos.
   - **Games** – This is one of the best techniques to keep your employees engaged. Consider creating a small security contest. Ask employees to provide a "Top 10" list of places they have heard users usually hide their password. Challenge them to decrypt an information security related word. Ask them questions based on posters, monthly newsletters, weekly/daily tips and/or videos. Offer a gift card for contest winners.

UNLIKE COMPUTERS, YOUR EMPLOYEES HAVE FEELINGS

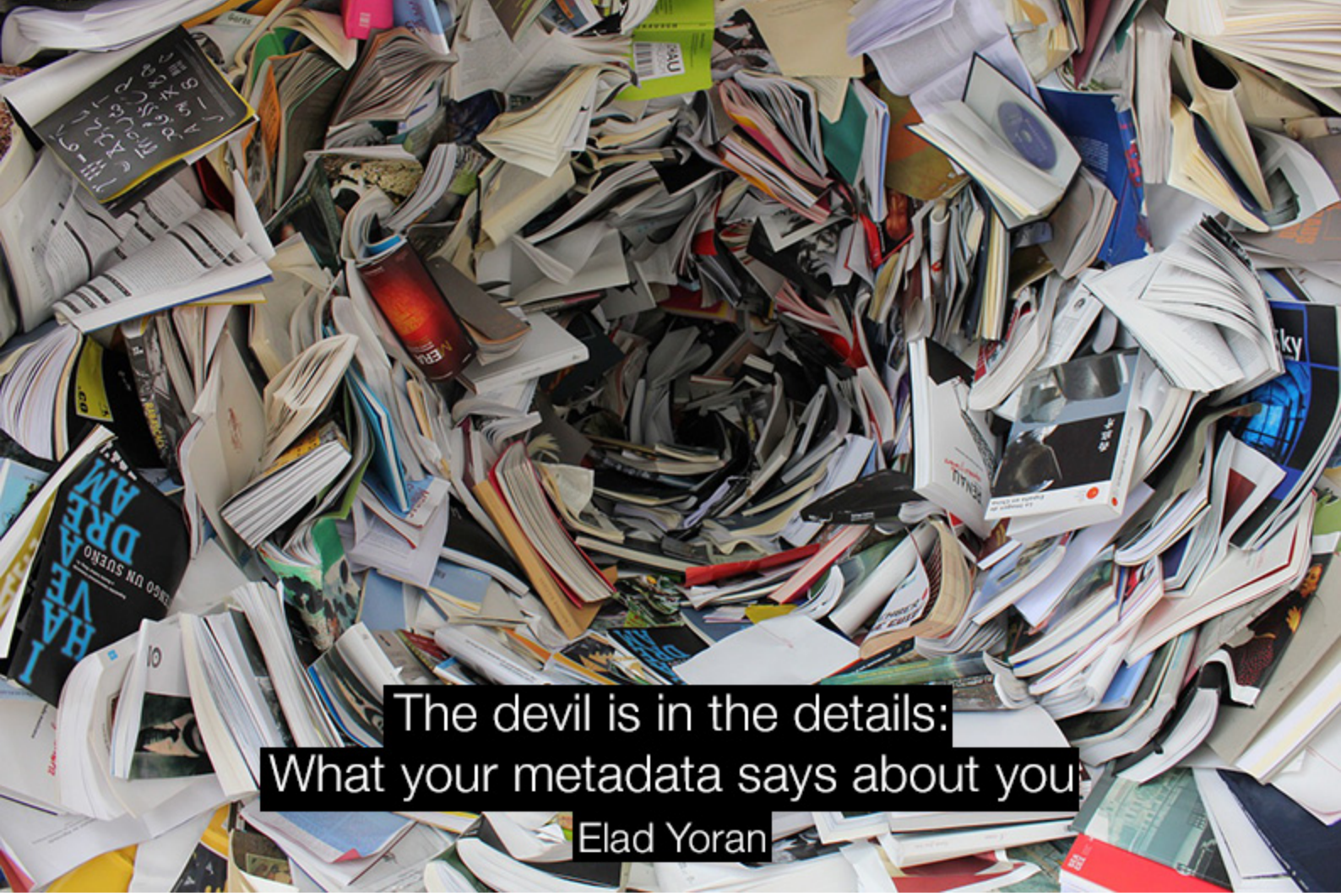
7. Announce the program ahead of time.
8. Unlike computers, your employees have feelings. During the testing do not embarrass them by releasing names of individuals that clicked on the malicious link in the phishing email.
9. In addition to standard security education that is provided to all employees within your organization on an ongoing basis, specific, role-based security education is extremely important. You will obviously not provide the same training to an HR employee who handles sensitive internal data and a marketing employee who handles customer data.
10. Employees should be made to understand that they can apply things learned through the security awareness and education program to protect themselves outside of work, making the program doubly useful for them.
11. Testing plays an essential role in the program. Test users through phishing campaigns, phishing phone calls, direct interactions (social engineering face-to-face), malicious USBs/CDs planted inside the facility, and so on.
12. Start with simple testing, and then ramp up the complexity.
13. You might be required to put the program in place because of specific standards your business must comply with, such as PCI DSS or HIPAA. However, your security awareness and education efforts must be ongoing to have a positive impact. Implementing a security education program just to be able to check the compliance box is simply a bad security practice.

14. Be sure to include training on policies, processes and standards that your organization employs and requires. Your employees and contractors must know these requirements exist and they must understand them.
15. In recent years social networking sites have turned into precious resources that organizations leverage for sales, recruiting, marketing and advertising. The time when organizations were blocking access to those sites is long gone. Unfortunately, attackers recognized the opportunity this new reality offers, and they use social networking sites to identify businesses and employees, and to learn as much as they can about them. Be aware what OSINT (open source intelligence) about your company your business and your employees put on the Internet.
16. Don't expect your program to be perfect from the beginning. It will take time to get from the initial to the desired state.
17. Every security awareness and education program must have metrics in place so that you can measure the program's maturity and track its progress, and share this information with your executive management. Metrics will answer the question "What is the impact of this program on my organization?"

A well-designed and successfully implemented security awareness and education program should result in your employees:

- Not being afraid to report an incident even if they did fall for a phishing email
- Being able to recognize phishing emails
- Actively reporting suspicious emails and activities
- Knowing their responsibilities when faced with social engineering
- Knowing what damage clicking on a malicious link and/or opening a malicious attachment can result in
- Using strong passwords, not writing them on a sticky note, and not sharing them with anyone
- Not being afraid to say "no" when they suspect they are trying to be manipulated through social engineering.

Zoran Lalic is the Chief Risk Officer at CyberVue (www.cybervueinc.com).



The devil is in the details: What your metadata says about you

Elad Yoran

Imagine the following scenario: the CEO of your company and the CEO of another company in the same industry have been engaging in cell phone conversations over the last two weeks.

A couple of the conversations took place over a weekend, even while your CEO was away with his family. More recently, other executives in your company started engaging in conversations with their counterparts at the other company, with some of the conversations taking place at night, well after business hours.

Two days ago, your CEO and CFO participated in a conference call with the partner of a major law firm and a prominent investment banker. Yesterday morning the CEO of the other company engaged in a series of calls with members of the company's Board of Directors. Yesterday afternoon, he called an investment banker and they spoke for 75 minutes.

The metadata about those communications does not include a single word said in any of these conversations. All it shows is who is speaking with whom, who called whom, when they spoke, where they were located, and for how long they spoke. Additional data revealed includes the sequence of the conversations and how they flow and spread over time, e.g. when the conversations with Board members, lawyers and bankers took place.

It is abundantly clear that a great deal of knowledge can be achieved from this scenario even though no information about the content of the discussions themselves was divulged and all participants were discreet and careful not to share information with anyone not included.

Is the data described above and the information it provides of value to your competitors? All the competitive intelligence gathered in this story is based solely on the aggregation, analysis and use of metadata.

What is metadata?

Metadata is defined as "data about data." It is the data that provides information about data in order to make it useful. While the term metadata has become more prominent in our lexicon in the digital age, a classic example is a library card catalog, which contained metadata about the books in the library, such as the author, title, genre and where to find the book. It was far more practical to browse through the card catalog than search the entire library for a single book.

The same concept applies to digital information today, however the quantity and type of digital metadata generated and collected is far larger, diverse, detailed, precise, and far more personal.

If metadata only divulges simple descriptive details, why are so many government organizations all over it? Why do intelligence agencies and law enforcement fight for the right to access metadata? Why are privacy and watchdog organizations concerned about the invasions of privacy? What makes metadata so valuable that providers like AT&T are selling it? Clearly, while many believe that it's "just metadata," a significant amount of information can be gleaned from the metadata.

If metadata only divulges simple descriptive details, why are so many government organizations all over it?

Uses of metadata

A common use of metadata is to enable targeted advertisements on social media, websites, in browsers. It is common practice for companies such as Facebook, Google and others to utilize metadata for corporate marketing. They monitor online and mobile activity by collecting and analyzing our calls, texts, chats, websites visited, posts, likes, purchases, comments, articles read, our friends, their activities, and much more.

For each and every one of us, these providers create a detailed persona including family (both immediate and distant), sex, friends, religious affiliation, where we live, where and when we vacation, medical history, and other personal information.

This metadata is collected and analyzed to create accurate digital representations of us, so that they can provide relevant advertisements to sell goods and services. And, while the knowledge that companies know so much about us may be disturbing to some, a great many find the convenience and value provided by companies like Google, Facebook and others to be worth the trade-off.

But what about other uses of metadata?

What if the mobile communications metadata of government officials is tracked? Of the police? The military? Regulators at the SEC? The IRS? The metadata – including records of communication flows, who is talking to whom, when, for how long – can reveal much about ongoing operations.

Corporate espionage has been a big problem for decades. According to a recent Harvard Business Review article, a study of the archives of the East German Ministry for State Security (commonly known as the "Stasi") revealed the former communist agency facilitated the achievement of significant economic returns for East Germany, thanks to its Stasi's industrial espionage operations during the 1960s, 1970s and 1980s.

The effect was so great that espionage was seen as more cost-effective than conducting original R&D.

We are likely experiencing the same phenomenon today, only on a much larger, global scale. We certainly hear a lot about the Chinese conducting corporate espionage and the benefits they achieve through stealing intellectual property, trade secrets and other confidential business information from American companies. But the threat is not just China - corporate espionage is a widespread and rapidly growing problem.

While the issue is compounded with international competitors that may be supported by their local government, many companies engage in a wide range of actions to gain advantage over their competitors. The scenario at the beginning of this article did not include the theft of intellectual property, yet revealed valuable information (based on metadata alone) that could be used to manipulate markets, change competitive dynamics, influence customers, and more.

Metadata may provide insight into corporate strategies, such as mergers and acquisitions. Every day business leaders engage in a broad range of sensitive conversations that should be protected, and this includes the conversations' metadata. And what about the metadata of conversations between a company and its regulators? It could indicate that the company may be under investigation.

A spike in communications between employees of an industrial company working at a specific facility and executives at headquarters can have many important implications.

Access to and analysis of the metadata of employees working on a pipeline, a mine or a refinery, could perhaps provide others with valuable business information about activity that the company may want to manage or contain.

Access to the metadata of conversations between sales people and prospective customers can tip off competitors.

With metadata that shows that executives of an automobile maker are having conversations with government officials in one country or another, one could easily piece together enough information to discern that they may be building a factory in one location as opposed to another.

Metadata may provide insight into corporate strategies, such as mergers and acquisitions.

The availability of unencrypted metadata is an issue that grows in scale as we continue to utilize more digital devices including cellphones, computers, tablets and others. All digital interactions come with metadata, and while the metadata doesn't provide the content of the interaction, it provides all the details surrounding the interaction.

By piecing together metadata from various types of events including phone calls, text messages, emails, websites visited and so on, government organizations, competitors, criminals and hackers can gain significant insight into our activities and plans.

Elad Yoran serves as Executive Chairman of secure mobile communications provider KoolSpan (www.koolspan.com). You can find him on Twitter @EladYoran.

ICS cybersecurity: Futurism vs the here and now

David Zahn

In early November 2016, Stephen Hawking pronounced that humans have 1,000 years to leave Earth as climate change, artificial intelligence, or nuclear weapons would eventually make the planet uninhabitable. Some say our doom will come much sooner. The futurist Michio Kaku believes we will become a Type 1 civilization in the next one hundred years. A Type 1 civilization is one that has harnessed the power of the planet – a power that can lead to global annihilation when hijacked by societal, religious, or political animus.

Dire prognostications make for great headlines, but not every crystal ball gives an accurate picture of the future. If we want to find existential threats in the here and now, we need look no further than cybersecurity within industrial facilities and power plants. Unlike breaches that lead to financial or information loss, a breach within an industrial site can bring injury to people and environment as well as the corporate bottom line.

The number of successful attacks where production and safety have been impacted is unknown. There is no cross-industry government mandate to disclose attacks. We know such attacks occur because some have become public; two of the more prominent ones include the Stuxnet attack on an Iranian nuclear power plant in 2010 and the loss of control at a German steel mill in 2014. The US Department of Homeland Security's ICS-CERT tracks industrial control system attacks and has logged a seven-fold increase since 2010, but most believe this number is highly underreported. So, we don't know to what extent the attacks exist; nor do we know to what degree they have achieved success.

What we do know is that the ICS that are targeted by these attacks were designed, built, and installed before cybersecurity became the concern it is today. Most facilities rely on air gapping, perimeter-based cybersecurity, and security through obscurity to keep them safe.

The reality is that air gapping is often a myth. Take the situation of a turnaround (i.e. when industrial facilities stop production to perform maintenance activities or switch production output). During turnarounds, hundreds if not thousands of plant personnel and contractors working across multiple shifts are making updates to systems and equipment, including air-gapped ones.

Each of them is an authorized user. But how secure are each of those worker's laptops? How air-gapped are these systems, really?

Perimeter-based security is critical to secure operations, but it is insufficient. Information technology personnel know this lesson well, which is why endpoint detection and response (EDR) became a best practice layer of protection for keeping systems secure in a corporate network. Cybersecurity within industrial facilities – ICS cybersecurity – is only now learning this lesson. EDR adoption to date has primarily focused on 20 percent of the cyber assets that exist within a process control network (PCN). This small slice of assets comprises the workstations, servers, routers, and switches that are commonplace in any IT network and relatively easy to interrogate and monitor.

The remaining 80 percent are the proprietary ICS that run production processes and enforce safety protocols. As these systems are proprietary, getting information about them is anything but straightforward. In fact, just knowing what systems are in an industrial facility is a challenge. Plant personnel typically rely on spreadsheets with only scant information on these highly complex systems.

To get a sense on how opaque these proprietary systems are to cybersecurity personnel, imagine not having a way of knowing how the systems running large, multi-national company's accounting and payroll systems are configured or not knowing what servers are even running those systems. If you cannot see it, how do you know if it is secure? This is unacceptable in a corporate network, but commonplace in a process control one.

There are ICS cybersecurity best practices that have emerged for PCNs. Clearly, network segmentation and the aforementioned perimeter-based protections are essential. The next step is to reach further into the industrial facility and begin securing the proprietary control systems – the ones where the digital meets the physical in a plant. The Purdue Model, which defines the technology stack in an industrial facility or power plant, defines these as Level 1 and 0. To extend cybersecurity into these levels, here are three must-haves to make sufficient inroads.

> Perimeter-based security is critical to secure operations, but it is insufficient.

Automate inventory

Inventory tracking spreadsheets is not a strategy. Getting inventory data requires manual effort from expensive engineers. Consequently, data is collected infrequently, it is incomplete, and it contains errors. Spreadsheets also do not enable higher value ICS cybersecurity functions, such as unauthorized change detection, as not all the data required for monitoring is captured.

Additionally, it is incredibly difficult to automate processes based on data trapped in Microsoft Excel.

The only answer is to gather configuration data from each manufacturer's control system. The challenge arises from the fact that there are a variety of manufacturer control systems at a single site. The data must include make, model, and version, but it also must include I/O card, firmware, control logic, and other data that defines the operating configuration of the system. Some try to get to this data by relying on network traffic monitoring.

Although this approach gathers data and can detect malicious activity, it only gets a small portion of the critical configuration data found in a proprietary control system.

Assess and mitigate risk

With a comprehensive and evergreen inventory, a risk assessment based on an adopted cybersecurity framework or standard will cover more ground. With risk levels assigned and vulnerabilities identified, personnel can develop a mitigation plan that balances risk and impact more appropriately. Such an approach may go beyond external compliance audit requirements, but they are consistent with good ICS cybersecurity practices.

A risk assessment that includes both traditional IT and proprietary control systems enables better decision-making on patch management processes. Because many industrial facilities lack sufficient closed loop visibility into proprietary systems, adopting technology that automates the work processes behind patch management is a significant leap forward.

Unlike with IT-based systems, it is highly possible that patches never get applied to a proprietary system. The old adage of "if it ain't broke, don't fix it," highlights how differently patch decisions are made for proprietary systems versus IT ones. In a PCN, the paramount concern is protecting production and enforcing safety versus focusing strictly on information security.

With a proper security baseline, engineering and cybersecurity personnel alike can track changes that matter for both traditional IT and proprietary control systems.

Monitor configuration changes

A byproduct of an automated inventory and a robust risk assessment process is an identified set of assets and configurations that require ongoing monitoring. Establishing that list, creating policies, and developing appropriate incident response protocols based on risk assignments is standard practice.

With a proper security baseline, engineering and cybersecurity personnel alike can track changes that matter for both traditional IT and proprietary control systems. When an unauthorized change is detected, the right investigatory steps are taken and tracked electronically, which supports both internal and external audit requirements.

The world is not going to end tomorrow. Nascent ICS cybersecurity is not one of the Four Horsemen of the Apocalypse, but it is an area of cybersecurity that has far reaching impact on communities and even national security, as we are talking about systems that run our critical infrastructure.

The good news is that companies are investing in securing, not just for the IT-based systems, but the proprietary ones as well. The first step many are taking is understanding what they have. With that complete picture, they are taking other necessary steps to harden the endpoints that matter most in an industrial facility.

David Zahn is the GM of Cybersecurity at PAS (www.pas.com).

Tech support scammers have started using ransomware

Tech support scammers have begun using ransomware to force users to pay for the "cleaning" of their infected computer.

Unlike most previous tech support schemes, this one tells the truth: the computer IS actually infected, with the so-called VindowsLocker ransomware. The message it shows after encrypting the files (and adding the .vindows extension to them) is somewhat bizarre:

"this not microsoft vindows support. we have locked your files with the zeus virus. do one thing and call level 5 microsoft support technician at 1-844-609-3192. you will files back for a one time charge of $349.99."

Users who call the offered number will get a tech support scammer in India, and the scammer will direct them towards a payment page/custom web form which the victims are required to fill out. The form requests the users' email, date of birth, social security number, credit card type, number, expiration date, CVV, and the amount that they need to pay. It seems that the scammers are after information that can be used to make fraudulent payments at a later date.

According to Malwarebytes, even if the victim provides this information, they won't be receiving a decryption key from the crooks. That's because the ransomware abuses Pastebin's API to deliver encryption keys to the crooks by making a private post on Pastebin.

"The author's intention was to fetch the keys from Pastebin by logging in to their account and later selling them to the victims," the researchers explained.

"However, they misunderstood the Pastebin API (they hardcoded a user_key) that was meant to be used for a single session. After the predefined period of time, the key expired. That's why the pasties were assigned to 'a Guest', rather than to a specific account. Retrieving them in this intended way became no longer possible."

Gooligan Android malware used to breach a million Google accounts

Check Point security researchers have revealed a new variant of Android malware, breaching the security of more than one million Google accounts.

The new malware campaign, named Gooligan, roots Android devices and steals email addresses and authentication tokens stored on them. With this information, attackers can access users' sensitive data from Gmail, Google Photos, Google Docs, Google Play, Google Drive, and G Suite.

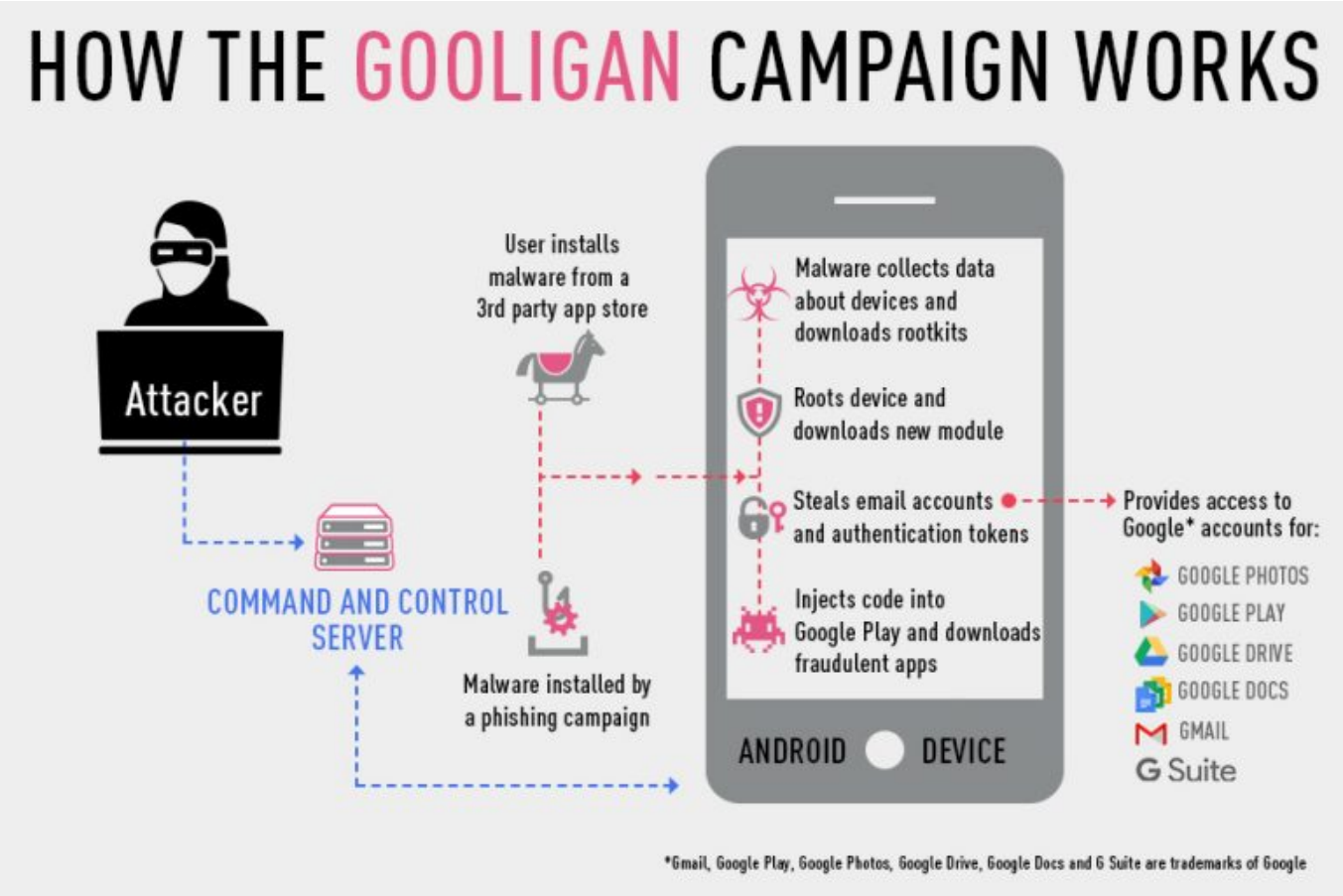
Key findings:

- The campaign infects 13,000 devices each day and is the first to root over a million devices.
- Hundreds of email addresses are associated with enterprise accounts worldwide.
- Gooligan targets devices on Android 4 (Jelly Bean, KitKat) and 5 (Lollipop), which represent nearly 74% of Android devices in use today.
- After attackers gain control over the device, they generate revenue by fraudulently installing apps from Google Play and rating them on behalf of the victim.
- Every day Gooligan installs at least 30,000 apps on breached devices, or over 2 million apps since the campaign began.

Check Point reached out to the Google security team immediately with information on this campaign. "As part of our ongoing efforts to protect users from the Ghost Push family of malware, we've taken numerous steps to protect our users and improve the security of the Android ecosystem overall," stated Adrian Ludwig, Google's director of Android security.

Among other actions, Google has contacted affected users and revoked their tokens, removed apps associated with the Ghost Push family from Google Play, and added new protections to its Verify Apps technology.

Check Point's Mobile Research Team first encountered Gooligan's code in the malicious SnapPea app last year. In August 2016, the malware reappeared with a new variant and has since infected at least 13,000 devices per day. The infection begins when a user downloads and installs a Gooligan-infected app on a vulnerable Android device, or by clicking on malicious links in phishing attack messages.



Deutsche Telekom confirms malware attack on its routers

German telecom giant Deutsche Telekom has confirmed that the connectivity problems some 900,000 of its customers experienced are the result of a hack attempt.

“Following the latest findings, routers of Deutsche Telekom costumers were affected by an attack from outside. Our network was not affected at any time. The attack attempted to infect routers with a malware but failed which caused crashes or restrictions for four to five percent of all routers. This led to a restricted use of Deutsche Telekom services for affected customers,” the company explained.

In order to mitigate the attack, Deutsche Telekom implemented a series of filter measures to their network, and has provided a firmware update for the targeted routers: Speedport W 921V and Speedport W 723V Typ (Type) B. The update should prevent this particular malware/attack from succeeding and from accidentally (or deliberately?) creating a denial-of-service situation.

“A software update is provided to all affected customers to fix the router problem. The software rollout already started and we can see the success of this measure,” the company noted, and instructed affected customers to unplug their router for 30 seconds, as the reboot clears the malware from the device.

Locky hidden in image file hitting Facebook, LinkedIn users

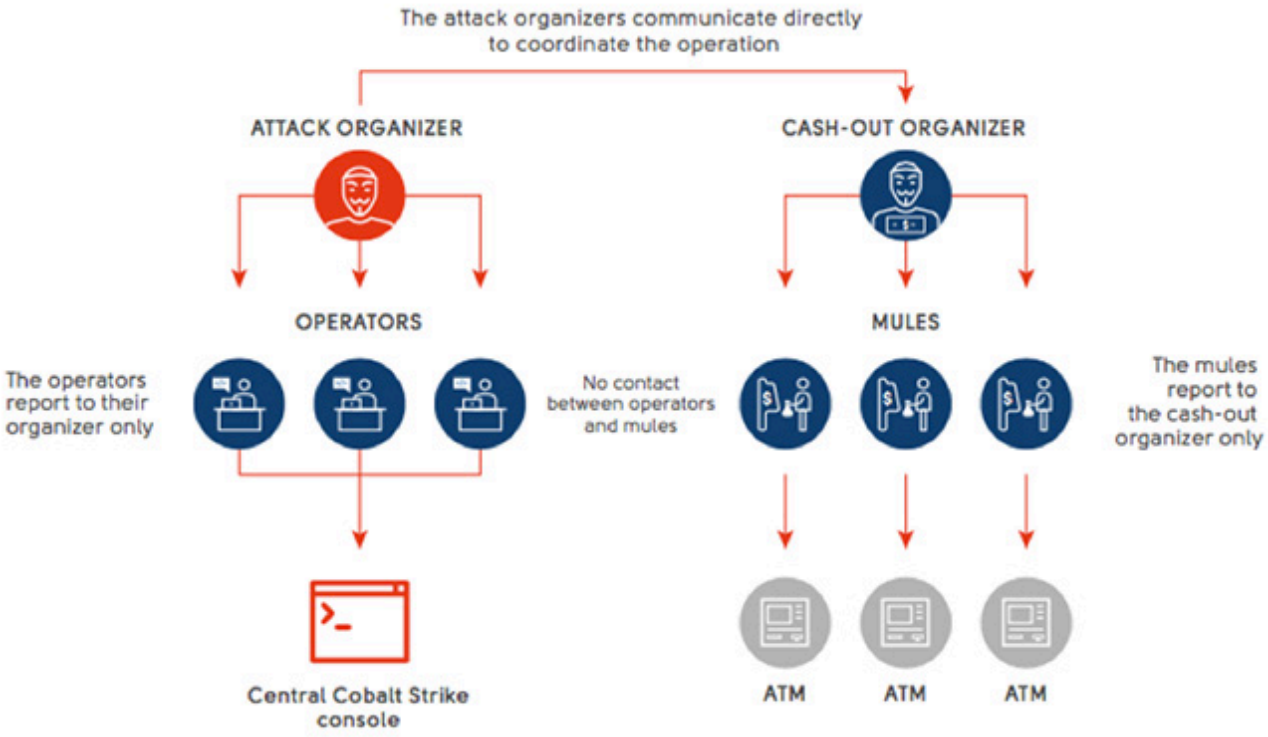
Malware masquerading as an image file is still spreading on Facebook, LinkedIn, and other social networks. Check Point researchers have apparently discovered how cyber crooks are embedding malware in graphic and image files, and how they are executing the malicious code within these images to infect social media users with Locky ransomware variants.

“The attackers exploit a misconfiguration on the social media infrastructure to deliberately force their victims to download the image file. This results in infection of the users’ device as soon as the end-user clicks on the downloaded file,” they noted.

They dubbed this attack vector ImageGate, and have shared their knowledge with Facebook and LinkedIn in early September.

As the malware delivery campaigns continue, it’s safe to say that the social networks have yet to fid a way to fix this issue without damaging their own functionalities.

As they are searching for a solution, the Check Point research team advises users not to open any image they have received from another user and have downloaded on their machine.



Cobalt hackers executed massive, synchronized ATM heists across Europe, Russia

A criminal group dubbed Cobalt is behind synchronized ATM heists that saw machines across Europe, CIS countries (including Russia), and Malaysia being raided simultaneously, in the span of a few hours. The group has been active since June 2016, and their latest attacks happened in July and August.

The group sent out spear-phishing emails – purportedly sent by the European Central Bank, the ATM maker Wincor Nixdorf, or other banks – to the target banks' employees. The emails delivered attachments containing an exploit for an MS Office vulnerability.

"If the vulnerability is successfully exploited, the malicious module will inject a payload named Beacon into memory. Beacon is a part of Cobalt Strike, which is a multifunctional framework designed to perform penetration testing. The tool enables perpetrators to deliver the payload to the attacked machine and control it," IB Group researchers explained in a recently released paper.

Additional methods and exploits were used to assure persistence in the targeted machines, to gain domain administrator privileges, and ultimately to obtain access to the domain controller. From that vantage point, they were able to obtain Windows credentials for all client sessions by using the open source Mimikatz tool.

The attackers would ultimately gain control over a number of computers inside the bank's local network. Some of them are connected to the Internet, and others not, but the latter would receive instructions from the central Cobalt Strike console through the former.

"After the local network and domain are successfully compromised, the attackers can use legitimate channels to remotely access the bank, for example, by connecting to terminal servers or via VPN acting as an administrator or a standard user," the researchers noted. The attacker have also installed a modified version of the TeamViewer remote access tool on the compromised devices, just in case.

Once constant access was assured, the criminals searched for workstations from which they could control ATMs. They would load the ATMs with software that allows them to control cash dispensers.

The final strikes happened in a few hours on the same day, when money mules would go to the targeted ATMs, send an SMS with the code identifying the ATM to a specific phone number, the criminals would make it spit out the cash, and the mules would leave with it.

Over 2.8 million cheap Android smartphones come with preinstalled backdoor

If you're using a cheap Android smartphone manufactured or sold by BLU, Infinix, Doogee, Leagoo, IKU, Beeline or Xolo, you are likely wide open to Man-in-the-Middle attacks that can result in your device being thoroughly compromised.

This discovery comes less than a week after researchers from Kryptowire identified several models of Android mobile devices that contain firmware that collects sensitive data about their owners and secretly transmits it to servers owned by a company named Shanghai Adups Technology Co. Ltd.

Among these mobile devices are also some BLU smartphones.

The origin of the vulnerability (CVE-2016-6564)

Those and other devices (roughly 55 device models) are open to attack because they sport the same firmware by Chinese software company Ragentek Group.

This firmware contains a binary that is responsible for enabling over-the-air (OTA) software updating, but unfortunately the mechanism is flawed.

For one, the update requests and supplied updates are sent over an unencrypted channel. Secondly, until a few days ago, two Internet domains that the firmware is instructed to contact for updates (the addresses are hardwired into it) were unregistered – meaning anybody could have registered them and delivered malicious updates and commands to compromise the devices.

Luckily, it was researchers from Anubis Networks that did it, and the move allowed them clock over 2.8 million devices that contacted the domains in search for updates. Many of these devices are located in the US, as most of the models are sold by Best Buy and Amazon.

But even though the domains are now owned by these security companies, the fact that updates are delivered over an unencrypted channel allows attackers with a MitM position to intercept legitimate updates and exchange them for malicious ones (the firmware does not check for any signatures to assure the updates' legitimacy).

MitM attackers could also send responses that would make the devices execute arbitrary commands as root, install applications, or update configurations.

Ransomware success creates apathy towards traditional antivirus software

In the last 12 months, 48 percent of organizations across the globe have fallen victim to a ransomware campaign, with 80 percent indicating that they've suffered from three or more attacks, according to a global survey conducted by Vanson Bourne.

In response to ransomware attacks, 67 percent of businesses globally have increased IT security spending, and 52 percent reported that they are changing their security strategies to focus on mitigation. Fifty-four percent also agreed that their organizations have lost faith in traditional cybersecurity, such as antivirus.

"Ransomware has become one of the most successful forms of cybercrime in 2016 and is on the top of every security professional's list of most prolific threats," said Jeremiah Grossman, Chief of Security Strategy at SentinelOne.

"It's not surprising to see high levels of apathy towards traditional antivirus software, and we don't expect the ransomware epidemic to slow down anytime soon. The situation is likely to get far worse, as some of the ill-gotten gains will be invested into research and development designed to improve encryption strength and utilize new delivery methods, as witnessed with Locky."

According to the survey, 81 percent of respondents globally that suffered ransomware attacks reported that attackers were able to gain access to their organization's network through phishing emails or social media.

Half reported that the attacker gained access through a drive-by-download caused by clicking on a compromised website, while 40 percent stated that the attack came through an infection via botnet.

Employee information (42 percent), financial data (41 percent) and customer information (40 percent) were the types of data most often affected by these attacks. Respondents identified the most likely motives of their attackers as financial gain (54 percent), operational disruption (47 percent) and cyber espionage (42 percent).

"These results further shed light on ransomware, where now, any and all types of sensitive data are targeted and can lead successful extortion," concluded Grossman.

Researchers set to work on malware-detecting CPUs

Adding hardware protections to software ones in order to block the ever increasing onslaught of computer malware seems like a solid idea, and a group of researchers have just been given a $275,000 grant from the National Science Foundation to help them work on a possible solution: malware-detecting CPUs.

The group includes Dmitry Ponomarev, professor of computer science Binghamton University, Lei Yu, associate professor of computer science at the same, Nael Abu-Ghazaleh, a professor of computer science and engineering at University of California-Riverside, as well as graduate students that will work on the project at both universities.

This project, titled "Practical Hardware-Assisted Always-On Malware Detection," will be trying out a new approach: they will modify a computer's central processing unit (CPU) chip to feature logic checks for anomalies that can crop up while software is running.

"The modified microprocessor will have the ability to detect malware as programs execute by analyzing the execution statistics over a window of execution," Ponomarev noted.

"Since the hardware detector is not 100-percent accurate, the alarm will trigger the execution of a heavy-weight software detector to carefully inspect suspicious programs. The software detector will make the final decision. The hardware guides the operation of the software; without the hardware the software will be too slow to work on all programs all the time."

Encryption ransomware hits record levels

The amount of phishing emails containing a form of ransomware grew to 97.25 percent during the third quarter of 2016 up from 92 percent in Q1.

PhishMe's Q3 2016 Malware Review identified three major trends previously recorded throughout 2016, but have come to full fruition in the last few months:

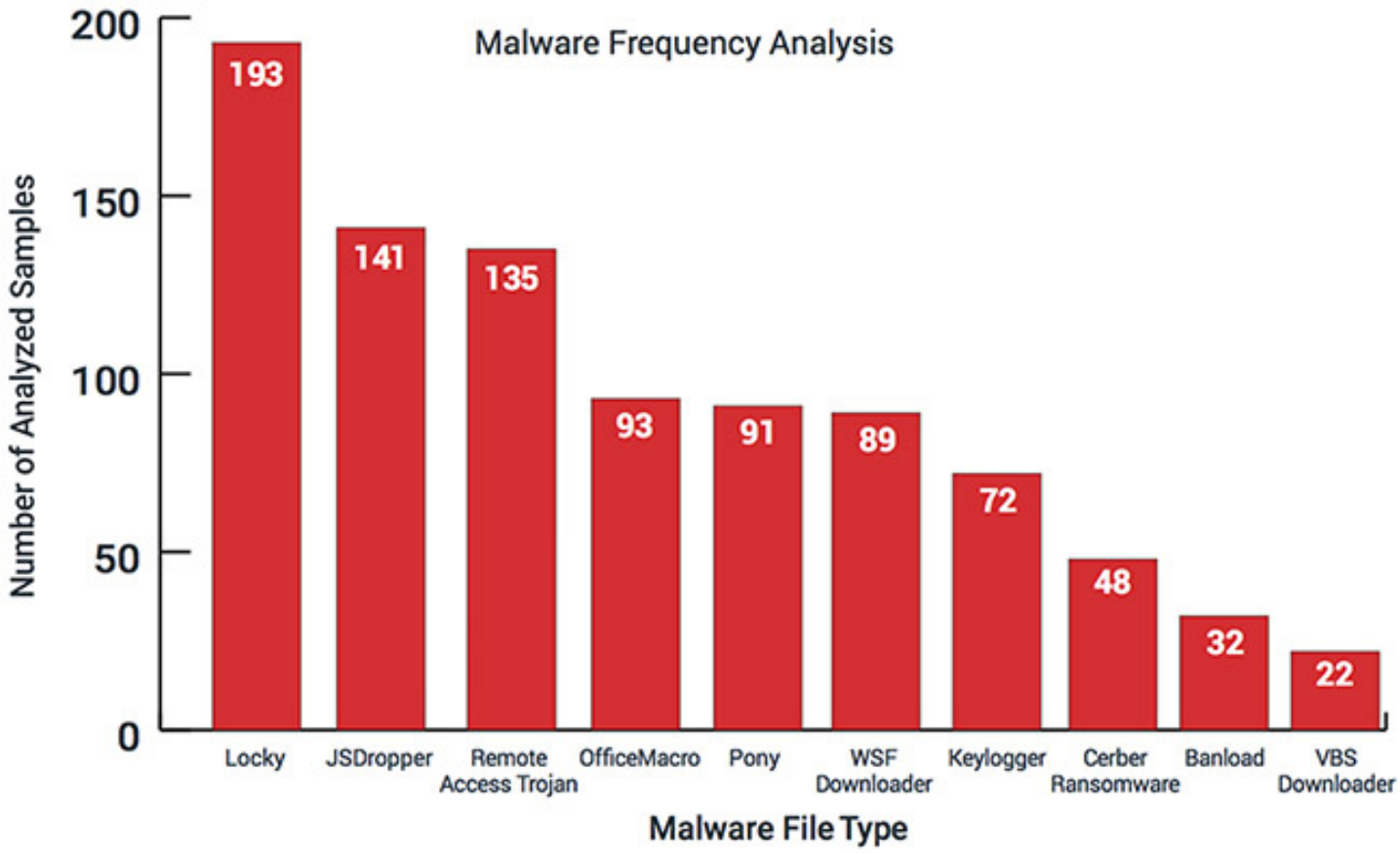
Locky continues to dominate: While numerous encryption ransomware varieties have been identified in 2016, Locky has demonstrated adaptability and longevity.

Ransomware encryption: The proportion of phishing emails analyzed that delivered some form of ransomware has grown to 97.25 percent, leaving only 2.75 percent of phishing emails to deliver all other forms of malware utilities.

Increase in deployment of 'quiet malware': PhishMe identified an increase in the deployment of remote access Trojan malware like jRAT, suggesting that these threat actors intend to remain within their victims' networks for a long time.

During the third quarter of 2016, PhishMe Intelligence conducted 689 malware analyses, showing a significant increase over the 559 analyses conducted during Q2 2016. Research reveals that the increase is due, in large part, to the consistent deployment of the Locky encryption ransomware. Locky executables were the most commonly-identified file type during the third quarter, with threat actors constantly evolving the ransomware to focus on keeping this malware's delivery process as effective as possible.

"Locky will be remembered alongside 2013's CryptoLocker as a top-tier ransomware tool that fundamentally altered the way security professionals view the threat landscape," explained Aaron Higbee, CTO at PhishMe. "Not only does Locky distribution dwarf all other malware from 2016, it towers above all other ransomware varieties. Our research has shown that the quarter-over-quarter number of analyses has been on a steady increase since the malware's introduction at the beginning of 2016. Thanks to its adaptability, it's showing no signs of slowing down."



Will cybersecurity change with a change in administration?

Jack Danahy

The 2016 United States presidential election has brought cybersecurity into public view with a forcefulness I have not seen in 25 years. The preferred coffee-shop-topic of system administrators, intelligence chiefs, and cybersecurity wonks - the risks and impact of hacking - has now become daily news for everybody.

The Democratic Party's private emails were released to the public during their national nominating convention. Emails from Hillary Clinton's campaign chair, John Podesta, including many relating to her foundation, her other advisors and employees, were similarly dropped a few weeks later. Finally, more of the her emails were found on a laptop owned by her closest associate, Huma Abedin, as her husband underwent investigation for his own alleged cyber misbehavior. As the election day drew closer, concerns were raised about the integrity of the voting systems by some security firms, there was a massive denial of service attack against large swathes of the US internet infrastructure, and cyber tensions continued to rise.

The ultimate impact of all of these things on the election is still debated, but this is the first time that cybersecurity concerns have moved the needle in a national US election.

With this backdrop, we should expect substantial changes in the national cybersecurity strategy with the change in administration. For one, these constant exposures of private communication should cause any public official to blanch. And secondly, you can be sure that President-elect Donald Trump and his transition team will be looking for ways to stop the cyber bleeding and prevent future embarrassment and injury.

Cybersecurity as a battlefront

To predict likely changes, let's first look at the 2016 Republican Party Platform Cyber Strategy. With the recent naming of Republican National Committee chair Reince Preibus as President-elect Trump's Chief of Staff, it's

reasonable to assume that the RNC platform is going to form at least part of the new administration's strategy.

Unfortunately, that platform is pretty limited. It focuses mainly on cyber security as a venue for warfare (*"We must stop playing defense and go on offense to avoid the cyber-equivalent of Pearl Harbor"*) and retaliation (*"[Cyber attacks] will continue until the world understands that an attack will not be tolerated — that we are prepared to respond in kind and in greater magnitude"*). Also, according to the platform, responding to a cyber attack isn't just the government's responsibility (*"... users have a self-defense right to deal with hackers as they see fit"*).

The platform considers cybersecurity as a battlefront, but it ignores the reality of our own weaknesses. When it says *"We must stop playing defense…"*, it makes me believe that they think that the many well-known government breaches were complex attacks that required specialized expertise to overcome our airtight cyber defenses. But most individuals in the cybersecurity arena know that the opposite is true: the task of gaining access to the average system is simply not that hard, and can be executed with basic software, managed malicious services, and modest social engineering skills.

The reams of stolen government data and published reports on our gaps scream that we must first develop a better defensive strategy. But is that likely?

THE REAMS OF STOLEN GOVERNMENT DATA AND PUBLISHED REPORTS ON OUR GAPS SCREAM THAT WE MUST FIRST DEVELOP A BETTER DEFENSIVE STRATEGY

Resiliency, not retaliation

We can take further direction from then-candidate Trump's campaign website, where we see more encouraging signs. Here we find the top priority to be the *"immediate review of all US cyber defenses and vulnerabilities, including critical infrastructure"*, and the formation of a "Cyber Review Team" with members from the military, law enforcement and private industry.

There are additional priorities listed - cross-department coordination on cyber threats, *"a focus on both offense and defense in the cyber domain"*, and cyber attacker deterrence and response - but this first initiative shows at least an understanding that the existing system needs plenty of help, that no one is yet sure where to start, and that there is a need for additional expert insight to make this new review and recommendation process meaningful.

As I and many others have written, the whole idea of cyber-retaliation is fraught with potential for missteps and the creation of movie-style villains who pose as adversaries to sow the seeds of apocalyptic cyber discord.

Attribution is so hard to get right, and requires so much cross-border cooperation, that it seems a better use of our time to work on making our systems and networks more resilient, and make the definitions of acceptable and unacceptable cyber behavior more clear, more widely adopted, and more actionable.

THE NEW ADMINISTRATION WILL LIKELY TAKE SOME CUES ON TOPICS FROM PRESIDENT OBAMA'S CYBERSPACE NATIONAL ACTION PLAN

What can we really expect?

What will we see in the first several months of President Trump's term? I think we will see some actual motion on at least creating the body that will raise visibility for existing, known vulnerabilities in the federal infrastructure. This is the kind of national defense-focused effort that also "protects personal freedoms and choices", i.e. it's a good bipartisan olive branch and potential early win for a new administration.

The new administration will likely take some cues on topics from President Obama's Cyberspace National Action Plan (CNAP), a move that would bridge partisan concerns and probably save some time. The CNAP was a pretty good plan, but like most plans, it floundered as its complexity called for additional and unavailable security expertise and resources. I expect to see additional recruiting for advisors and investigators to bring more pre-breach preparation for the protection of the federal infrastructure.

The acquisition of this type of skilled personnel should be easier now, with a new administration and new opportunities for meaningful exposure and advancement.

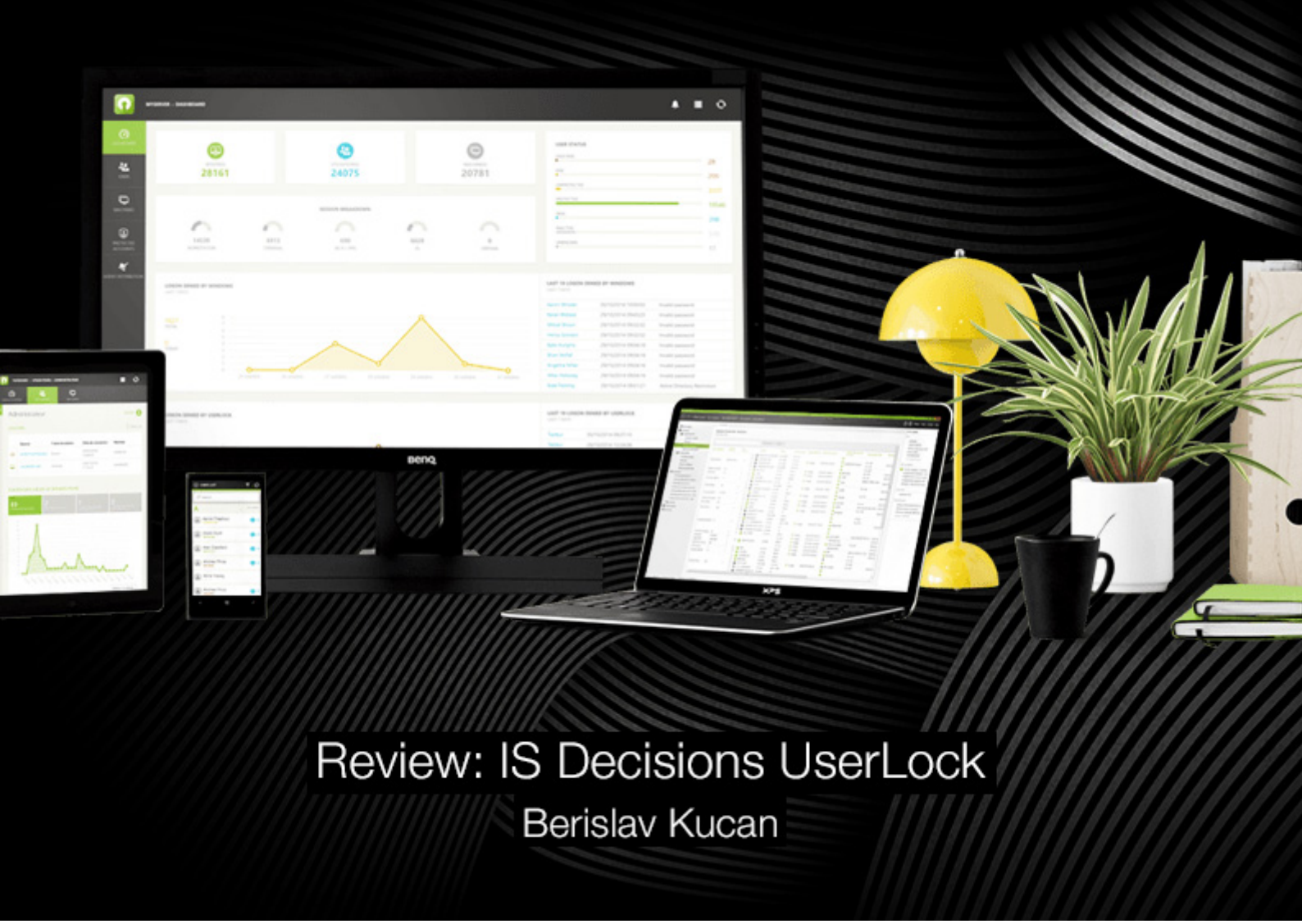
My cybersecurity predictions for the first year of President-Elect Trump's term are as follows (from most likely to least):

1. The Cyber Review Team will be formed, and will likely include or even be headed by former Joint Staff J6/Cyber Directorate head TG Keith Kellogg. He was already an advisor to Mr. Trump, and he has been advocating better national cyber security for at least 15 years, making him a practical and realistic advisor.
2. There will be recurring dust-ups among federal organizations asked to explain their shortcomings with respect to earlier analyses (by GAO and others) or any new weaknesses found by the Cyber Review Team. The new administration will need to make it safe to admit insecurity if we are ever to address these issues.
3. There will be a repositioning of some improvement efforts and investments to link them more substantially to voter concerns about their own privacy and security. Cybersecurity has seldom made a big splash legislatively, and it will need to be repackaged as relevant to voters in order to get time on the floor.
4. There will be reports released within the first 180 days regarding systemic weaknesses found and in need of remediation. After this period, the new administration takes at least partial responsibility for their persistence.

It is certainly about time for this attention to arrive. It's been almost 20 since the first big presidential toe-dip into cybersecurity (President Bill Clinton's Presidential Commission on Critical Infrastructure Protection), and for many years these problems have been fully, but quietly, acknowledged. The events of the past 18 months have pulled back the curtain sufficiently so that the public is now more aware of cybersecurity issues, at least as they affect the services that they care about. At the same time, politicians have a current and natural urgency to move this forward, even before the 2018 midterms.

This combined pressure, perceived by a new administration, may finally be enough to move the national cyber security posture forward. I hope it does.

Jack Danahy is the CTO at Barkly (www.barkly.com) and a 25 year veteran in the security industry. He was the founder and CEO of Qiave Technologies (acquired by Watchguard Technologies in 2000) and Ounce Labs (acquired by IBM in 2009). Jack is a frequent writer and speaker on security and security issues, and has received multiple patents in a variety of security technologies. Prior to founding Barkly, Jack was the Director of Advanced Security for IBM, and led the delivery of security services for IBM in North America.



Review: IS Decisions UserLock

Berislav Kucan

According to a Rapid7 survey, 90% of organizations are worried about compromised credentials and around 60% say they cannot catch these types of attacks. French IT security company IS Decisions tries to tackle this major problem with UserLock, a solution that provides access security and concurrent login control for corporate networks.

Setup and deployment

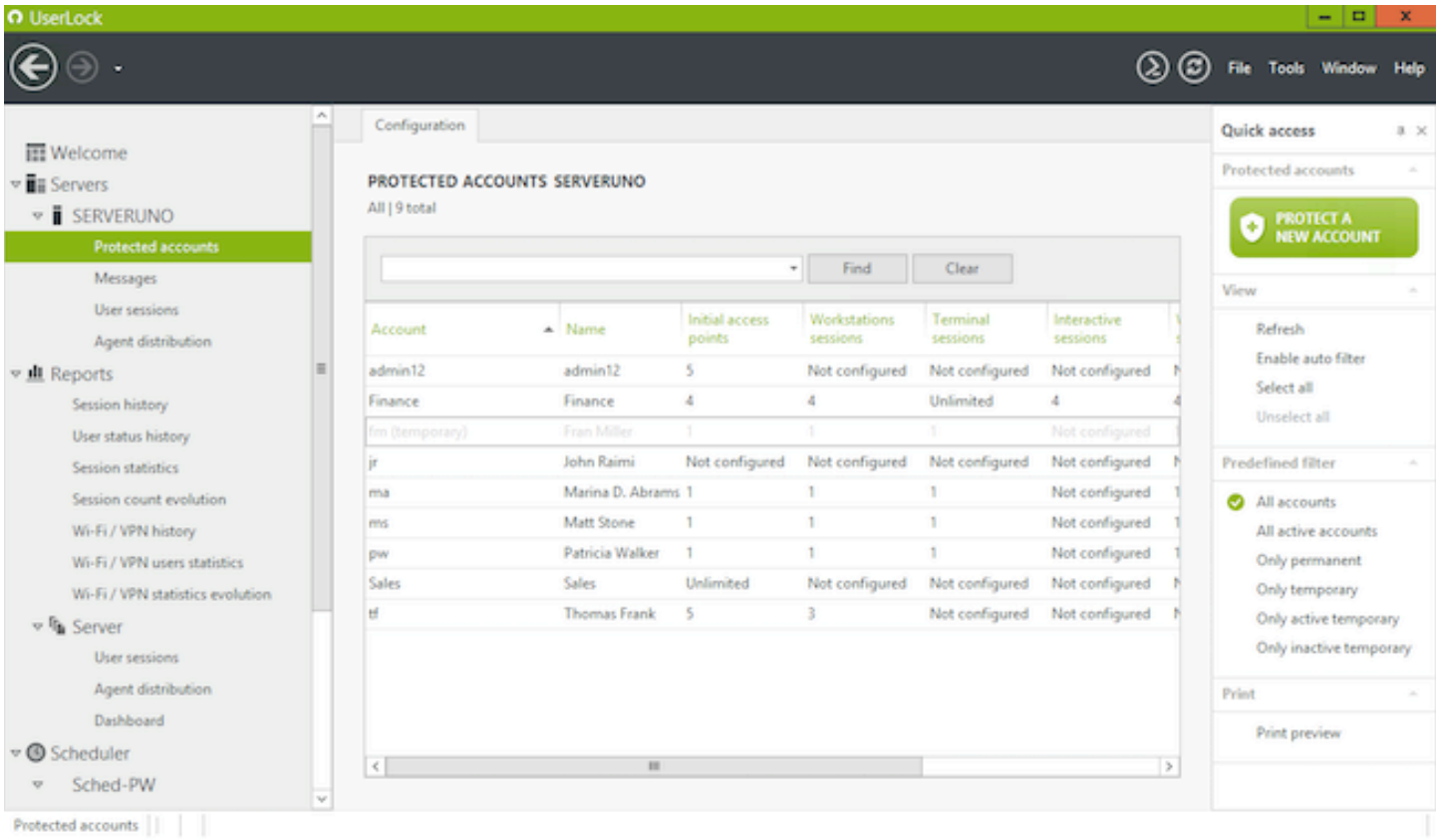
UserLock works alongside Active Directory, so no modifications are needed to AD or its schema. The software should be installed on a Microsoft server ranging from Windows Server 2003 to Windows 2012 R2.

The console is installed by default on the same computer, but you can deploy it to any other server or workstation. The installation procedure is quick, and a Microsoft Access database used for logging is bundled within. Or, you can use your own database solution.

To function properly, UserLock requires *Remote registry* and *Microsoft File and Printer Sharing* to be enabled on all machines that UserLock will protect. In case one of these is not enabled, the software will point you in the right direction to mend the situation.

The user interface is rather straightforward, especially for a seasoned Windows server administrator. The first thing you (the admin) need to do after setting up UserLock is to deploy its agents across the network.

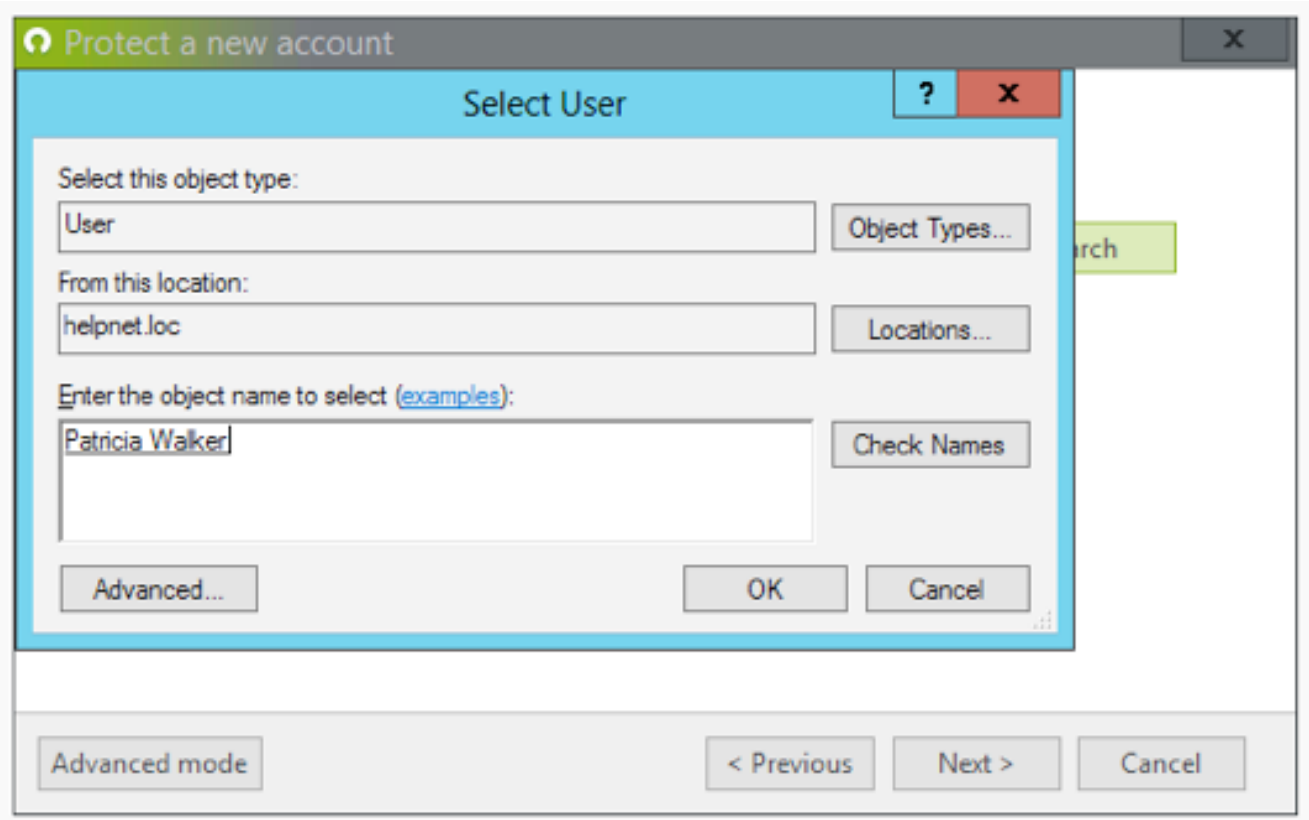
This can be done automatically, or you can select the specific resources that you want to protect and install agents solely on them. If you need them, 32-bit and 64-bit MSI packages of the desktop agent are also provided.



Protected accounts

Connection rules and restrictions are defined by user, group or organizational unit through an internal UserLock entity named *Protected account*. This account is based on the accompanying data from the Active Directory. Any entity from the domain can be used as a basis for a protected account, for instance AD user *pw* and group Sales will become protected accounts *pw* and *Sales* inside UserLock.

Upon creating a list of resources you are planning to monitor, it is time to get down to business.

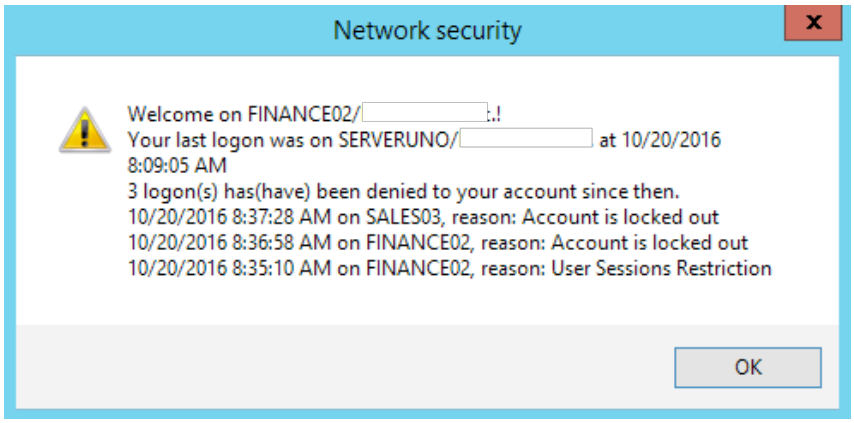


When it comes to monitoring user behaviour, there are almost countless variables that can be taken into consideration, and this is where UserLock excels. For each protected account you can customize:

- **Initial access points:** number of unique locations where a user can enter the network
- **Concurrent sessions:** number of concurrent sessions per user with detailed specifics (workstation, terminal, Wi-Fi, VPN, IIS)
- **Session limits:** detailed customization per session type
- **Workstation restrictions:** you name it, it can be done – allow/deny, names, IP ranges, OUs, etc.
- **Hour restrictions:** rules enforced for specific timeframes, such as allow/block connections during or after working hours
- **Session timings:** limiting session duration, locked time, etc.

All of the predefined messages shown as a result of enforcing the rules can be customized. You can use your own text and reuse the internal variables (ex. %SessionType%) to provide dynamic details describing the situation.

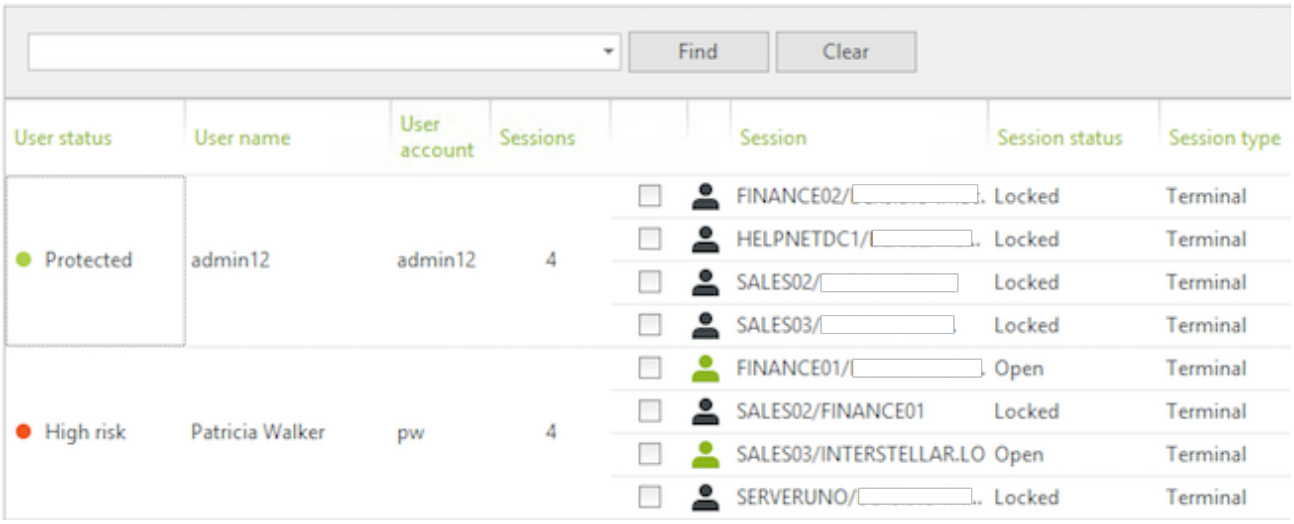
As per specific protected account policy, the actions and the alerts can be either informational (user gets just a descriptive pop up) or proactive (session or account gets blocked).



Actions

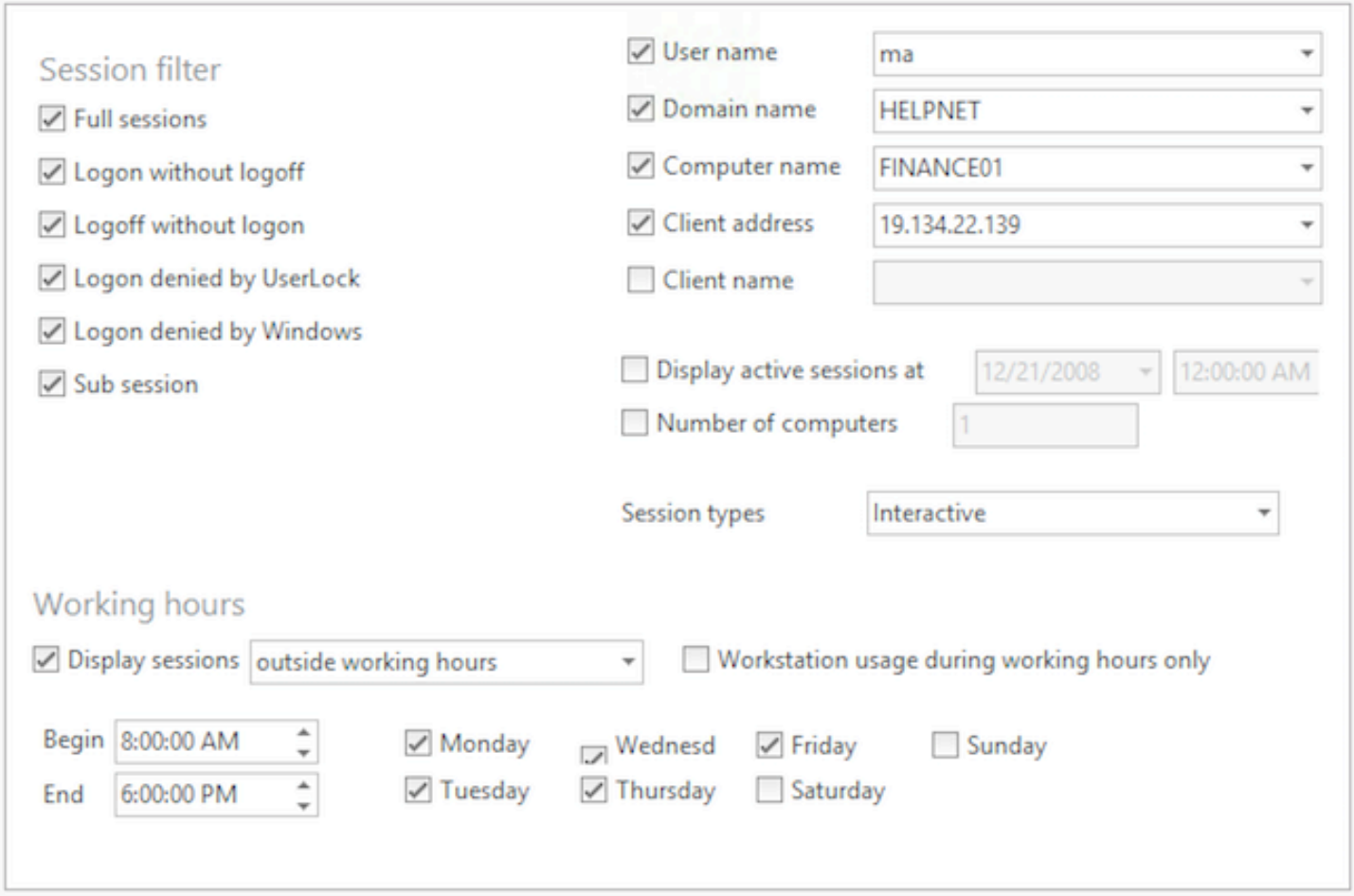
Based upon the rule set for every protected account, the administrator is able to enforce a set of actions that can mitigate a potential problem by locking access to specific user and/or resources. Within the UserLock server interface, it is easy to track current open sessions and analyze red flags.

Some of these accounts will get automatically blocked (as per your policies), but you can always block a *high risk* user manually. This will disconnect all his active sessions and block the credentials until the issue is taken care of.



Reporting

The attention to detail that IS Decisions has shown when planning the protected account rules can also be seen in the built-in reporting mechanism. The software collects a wide range of usage patterns per each protected account and you can generate a report based on every one of these parameters.



Besides the fields pictured above, there are also options to audit the logs per specific entities other then users (groups, OUs), as well as further timeframe parameters.

The reports are launched in the application and can be exported in PDF, TXT, XLS, CSV, HTMNL, MHT and RTF format.

Logon time	Logoff time	User	Domain
10/20/2016 7:42:58 AM	10/20/2016 8:01:57 AM	Patricia Walker	HELPNET
10/20/2016 7:44:28 AM	10/20/2016 7:47:14 AM	Patricia Walker	HELPNET
10/20/2016 7:48:13 AM	10/20/2016 8:06:17 AM	Patricia Walker	HELPNET
10/20/2016 8:06:11 AM	10/20/2016 8:13:46 AM	Patricia Walker	HELPNET
10/20/2016 8:08:24 AM	Account restriction	Patricia Walker	HELPNET
10/20/2016 8:08:37 AM	Invalid password	Patricia Walker	HELPNET
10/20/2016 8:08:43 AM	Account restriction	Patricia Walker	HELPNET
10/20/2016 8:09:05 AM	10/20/2016 8:16:47 AM	Patricia Walker	HELPNET

IS Decisions Session history 1/2

USERLOCK IS A POWERFUL PRODUCT THAT FOCUSES ON PREVENTING THE INTERNAL AND EXTERNAL THREATS RELATED TO COMPROMISED CREDENTIALS

Scheduling

All of the reports UserLock generates can be scheduled. The scheduler itself contains every possible time aspect you'll need to optimize the creation and delivery of the selected reports. The scheduled reports are generated in a PDF format. There are no options to select other file types, but if you delete .pdf from the file name and add one of the other supported file types, it will work. This screen definitely needs to be upgraded in the next version.

The scheduler can also be used for automating the clean-up of existing older records.

Documentation

The UserLock documentation is quite extensive. While the software itself is easy to configure and manage, there is a large number of online resources that can help users discover the benefits of using the product. There is a step by step getting started guide, which you can follow to understand every aspect of what UserLock can do.

The use cases section of the support page specifies 10 detailed usage scenarios which demonstrate UserLock's powerful access protection capabilities.

For the purpose of this article, I have tested UserLock 9, which was released a couple of months ago.

Pricing

UserLock's licensing scheme is based on per maximum simultaneous sessions in your network. The unit price for 50 to 99 user sessions is $16.80. There are a couple of predefined price tiers and in the biggest one the unit price for 1000 to 1999 user sessions would be $9.38.

For larger deployments, you should contact IS Decisions to get a custom price quote. The important thing to add is that these are perpetual licenses. Pricing includes new releases and technical support for the first year.

Final thoughts

Stolen user credentials were at the root of some of the biggest hacks in the last few years. UserLock is a powerful product that focuses on preventing the internal and external threats related to compromised credentials, by providing the administrators with detailed options for monitoring and restricting access to their Windows-based networks.

Berislav Kucan is the Director of Operations for (IN)SECURE Magazine and Help Net Security (www.helpnetsecurity.com).

"Build security in from the start" for app developers

John Schuch

Most application developers are familiar with the directive "Build security in from the start." They've heard it and read it numerous times during debates about application security. However, there is not a whole lot of information on what it actually means. Aside from the lack of information about what exactly is meant by the term *security*, there is also a lack of information about when it is specifically NOT a good idea to build it in from the start.

This article will attempt to clarify this topic by laying out the aspects of security that need to be covered by application developers, and by specifying at which point in the application lifecycle they should occur.

Identity management and access control

One of the first tasks to start working on is designing the integration with your identity management system. If you are developing an application that is used solely by your company's employees, you will most likely be integrating with the identity management system that your company already uses. In that case, you need to determine the roles of the various users of your application.

Your application may have only one role (user) which would certainly make your life simple. Most likely, though, there will be different roles for different users, giving them access to different parts of the application. You will need to understand the roles that are managed by your identity management system, so that you can know whether you can use existing roles or whether new ones need to be created.

You will then need to integrate this with your access control system. Different roles will have different capabilities in the application and the access control system needs to be set up to enforce those rules. Another interaction with the identity management system that needs to be understood is the creation and deletion of users.

In some applications, both actions are performed completely outside of the application. Most internal applications are this way. The creation and deletion of users is handled by workflows in the identity management system and the application does not play any part in that process.

On the other hand, applications whose user population is composed of the general Internet population must have some method for creating and deleting users. In these instances, many organizations choose to delegate identity management to a third party like Facebook or Google. If handled strictly according to the third-party protocols, this can be a valid solution from a security standpoint, although it drags along some business issues that may or may not be acceptable to your stakeholders. Note that a solution like this does not address the need for access control or session management.

Session management

Your access control system will manage sessions for you, but it is your responsibility to determine how you want to handle user sessions in the event of a server failure. The implementation will vary depending on your access control system and your web container, but you will still need to find a solution that implements the right balance of user (in)convenience and a possibly costly failover solution.

Encryption and data management

Every piece of data that passes through your system must be identified and you must determine what level of protection the data requires. This is done through a data classification process. I will assume that you are not handling credit card data, as that requires more advanced protection techniques that are beyond the scope of this article.

When your data classification is complete, you will know which of the data you are handling requires encryption during transit and at rest.

Each piece of data that requires encryption will need to be encrypted through the entire system, not just from the browser to the front-end servers. That will require using an encrypted transmission protocol when the data is transferred between servers, and using encryption whenever the data is stored. Doing this early in a project is important so that you can get your DevOps or data center support team involved. They will be the ones who implement the transport layer encryption, the certificate management, and the key management. Some of the things they need to set up may take some time so it's critical to get them involved early on.

Key storage

If you mean to implement encryption in your application, your next and absolutely most important task will be to determine your strategy for secure key storage. If your environment already supports encryption you will most likely be able to make use of your existing key storage mechanism. If not, you will need to come up with one.

While there are key management systems you can purchase, you can also "roll" your own. If you choose the latter option, you should, at a minimum, follow these guidelines:

1. Do not store keys with the data they protect.
2. Create a secure location to store the keys.

Key rotation

Another critical part of your key management is to have a method for rotating the keys. First you will need to determine an appropriate expiration period (all keys have expiration dates). Pick one that is appropriate for your organization and the data you are protecting. Next, determine the process you will use to rotate your keys.

Ideally you want a process that will be completely innocuous to your application. This is especially true if you are developing an application that will have zero downtime. You wouldn't want to have to take your high-traffic website offline just to rotate the keys.

Application architecture

This topic could use an entire book, but the key points to keep in mind when architecting your system is that:

1. All incoming connections to the server must be assumed to be potentially hostile, even if they have a valid session.
2. All client environments are completely insecure at all levels.
3. All networks outside your private-network perimeter are completely insecure.

Your server-side code has to be written as if it is under attack from authenticated, in-session hostile code, and your client-side code has to assume that every byte of code from every server response can be examined and subverted by expert hackers.

Logging is going to be covered later in this article, but during this design phase make sure that you are able to track transactions end-to-end through the system. This will help you identify when an attacker has figured out how to inject a transaction at a point downstream from where a transaction should be initiated.

At this point we've covered all the security-related items that must be built in up front. The remaining items are things that can wait until later in the project. In some cases they can't be initiated until the project is well under way, and in other cases they are activities that must be done continually throughout the life cycle of your application.

Vulnerability scanning

You won't be doing vulnerability scanning up front but you will need to start scanning after you get some code running. You don't want to wait until you are ready to move to production to start scanning. You might be overwhelmed with the number of vulnerabilities. If you start scanning your code early in the project you will be able to keep the number of vulnerabilities that need to be fixed to a manageable level.

You might also uncover some bad habits of some developers that can be fixed, or some vulnerabilities in your platform or libraries that need to be patched.

External libraries

What is your strategy for verifying that the external libraries that you have downloaded from the Internet are not "bad"? Security experts are divided on the true risk of cross-build injection attacks, but you still need some way to determine that your external libraries do not contain malicious code. On the server-side, this generally means relying on widely used libraries, and closely controlling the library sources and versions.

For browser-based dependencies this should be less of an issue because all client-side code should be regarded as potentially compromised.

Logging

Make sure that you are not writing any sensitive information into your logs. You don't want your log files to be an easy way for attackers to obtain this data.

You might be tempted to continue providing the ability to log sensitive information at debug level, as this can come in handy when you are dealing with an incident in production. But you have to have strategy for scrubbing sensitive data from logs.

Availability

There's not much you can do to defend against a denial of service attack at the application layer. However, you can put some effort into finding ways to prevent attackers from wasting resources. For example, you can use a CAPTCHA to prevent illegal account creation, or think of ways to prevent attackers from sending simple requests that consume database connections or other resources.

The security-related tasks that must be completed during application development have been listed above. Your application may not need all of them, but depending on what you need, you now know which tasks need to be performed up front.

John Schuch, CISSP, is a Senior Architect and Security Practice Lead at Gorilla Logic (www.gorillalogic.com).

Executive hot seat: Lior Frenkel CEO at Waterfall Security Solutions

Interview by Mirko Zorz

Lior Frenkel is the CEO and co-founder of Waterfall Security, the leading provider of unidirectional security gateways. His experience spans research, design and development of mission critical systems and national cyber security technologies and programs. He holds multiple patents and patent applications, primarily in the area of cyber security for OT and IT environments.

What are the most common misconceptions surrounding the security of industrial control systems?

The most common misconception surrounding the correct approach to the security of industrial systems is that the traditional IT security technologies such as firewalls can be applied to industrial systems, and provide adequate and relevant security.

You need to remember that IT security is all about 'protect the information'. Information is a virtual asset, which can be easily copied, relocated and also backed-up and restored.

On the industrial side, the goal for security is to prevent the attacks from happening at all. The main security target is to prevent damage to the physical assets –machines and processes which are controlled by the network. A damaged pumping station, for example, can not be 'restored' from a backup, nor can you use a remote site to pump this station.

Generally, what are the unique security challenges related to industrial control systems?

In general, the unique challenge is the increasingly expanding attack surface. An industrial system is filled with dials, gauges, and sensors that monitor and control the industrial process.

Today they are all connected for better monitoring and management with industrial software, protocols, databases and applications. These devices, all interconnected, are a great playground for an attack or malware.

Furthermore, when you connect these to an external IT network, to the Internet and to cloud based services, the attack surface expands dramatically. Throw in the fact you do not want any adverse entry into your network, potentially harming your equipment, and now you have something that keeps you awake at night.

What's your philosophy when it comes to securing industrial control systems?

First I'd like to point out that this is not my personal philosophy, many regulatory bodies and standards organizations share this philosophy. Organizations such as the US Department of Homeland Security, ANSSI, the national authority on cybersecurity in France, and many others around the world advocate unidirectional communications for industrial control systems.

Ours is a vastly different approach to risk management for industrial control systems and critical infrastructure. It takes an evolutionary approach that led us to design and develop unidirectional security gateways. The unidirectional security gateway creates a safe way for external parties, headquarters, vendors, cloud services, and others, to have real-time access to industrial information, without access to the industrial environment.

The unidirectional gateway technology creates an impassable, physical barrier preventing all external online attacks from reaching into industrial sites.

Waterfall's Unidirectional Security Gateways create replica copies of control system applications and devices, such as relational databases and process historian databases, on the external network. Corporate users and corporate applications have access to real-time data by querying the replica servers.

Unlike firewalls, there is no physical path into the control network, and you are not relying on software to keep out the attacks.

What are the essential features of a robust unidirectional security gateway? What should customers be on the lookout for?

Customer should be looking for full unidirectional solutions, supporting robust communications, off-the-shelf connectivity, high availability, high throughput, and the full range of hardware and software features required of industrial-grade solutions.

They should look for a vendor who does not produce per-customer customizations or carry out costly custom engineering of any sort. Unidirectional gateways are a major pillar of a serious security program, and one should select a vendor that can support its current needs as well as future ones.

What ICS-related threats can we expect in the near future? What type of impact could they have?

It's no exaggeration to say that every day we read about another break in the security of industrial components like PLCs, routers, sensors, etc. and in every industry possible.

The most well-known was the attack on the Ukrainian electric grid when the lights went out for hundreds of thousands, but recently we've heard about attacks on hospitals, smart buildings, rails and ship navigation systems, mining, water works… there is no end to the list.

The only commonality among them all is that these are industrial systems were predominantly "secured" by firewalls, and that must come to an end. The impact can be financially damaging, or cause loss of human life or serious negative consequences on our environment. In any scenario, there's no reason to use any lower form of cybersecurity protection.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security (www.helpnetsecurity.com).

RSA Conference 2017

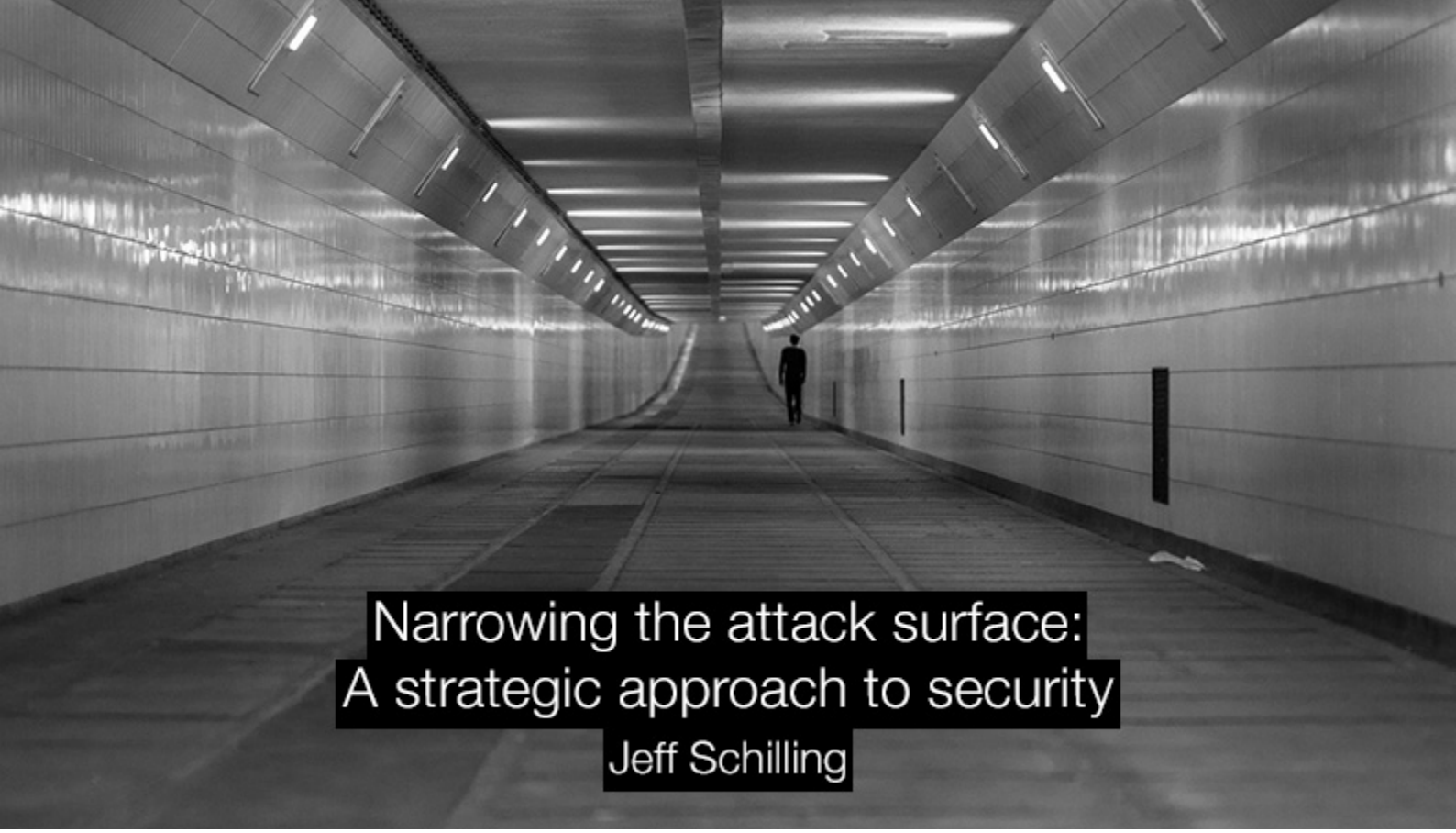
bit.ly/2fS5laM - San Francisco, USA / 13 - 17 February 2017

In the digital world in which we now live, information is a highly valued commodity. Safeguarding that information, therefore, has become a top priority. RSA Conference's mission is to connect you with the people and insights that will empower you to stay ahead of cyber threats. This event is your best resource for exchanging ideas, learning the latest trends and finding the answers you are looking for.

ICISSP 2017

www.icissp.org - Porto, Portugal / 19 - 21 February 2017

The International Conference on Information Systems Security and Privacy aims at creating a meeting point for researchers and practitioners that address security and privacy challenges that concern information systems, especially in organizations including not only technological issues but also social issues.



Narrowing the attack surface: A strategic approach to security

Jeff Schilling

With the sustained onslaught of ransomware and high-volume destructive attacks, it's clear that operations are growing in complexity and threat actors' skills are improving. What's worse, security teams are often asked to do more with less, and there is little tolerance from organizational decision-makers for any shortfalls.

Is there any hope for a security operations team to keep up? Absolutely. It all starts with a comprehensive security strategy that addresses an organization's unique threat landscape, followed by scrutiny of IT architecture, and focusing resources where they are needed to identify and mitigate threat actors' attacks before their objectives are achieved.

Dissecting threats

The core of any security strategy should be a reduced attack surface to limit where threat actors can have success. In order to achieve this objective, the threat landscape as it applies to a particular organization must be fully grasped. This typically consists of three major threat categories:

1. *Commodity threat* - The commodity threat is that group of threat actors who are common to all. Commodity actors don't necessarily have a target in mind; they are truly fishing with dynamite as they recon the Internet looking for low hanging fruit. While commodity threat actors don't normally build custom tools for their attacks, they can leverage many open source attack frameworks. Normally, well-orchestrated signature-based security controls and a well-patched environment will minimize the success commodity actors can achieve. This allows a security team to focus on the more sophisticated threats.

2. *Targeted threat* - There are threat actors that seek to attack specific organizations. Unlike the commodity threat actors that send out millions of phishing emails, the targeted threat is more likely to send out just ten spear phishing emails, targeting specific individuals who have the access they want. These emails come from spoofed email addresses to increase the likelihood that a potential victim will open the email. Dealing with this group of threat actors is when a good security team really earns its pay. These are the threat actors who mostly avoid signature-based detection and require sophisticated security operations to be caught. They are most commonly referred to as an APT, and this group includes

sophisticated criminal gangs and low-level nation-state actors.

3. *Advanced targeted threat* - These are the threat actors that aren't widely known because they work very hard to stay out of the news. They are the high-end nation-state actors who like to move down low in the OSI model to gain access. They don't just live on the application layer - they tap networks through both physical and remote means. The Advanced Targeted Threat will coordinate close access, on-premises operations with remote operations. They are after national secrets, sophisticated technology and intellectual property. Not all organizations are targeted by these actors: But for those who are, a good security strategy can bring some success in warding off these bad guys.

THE MOST SIGNIFICANT CHALLENGE MOST SECURITY TEAMS FACE IS AN ARCHITECTURE THAT WAS NEVER DESIGNED WITH SECURITY IN MIND

Examining IT architecture

In my opinion, the most significant challenge most security teams face is an architecture that was never designed with security in mind. And, after framing the threat landscape, the next step is to take a hard look this important area. Based on 24 years of military experience, I've learned that understanding the physical terrain that you want to protect in combat operations and leveraging that terrain in your defensive plan is of critical importance. This basic security principle translates well to the "cyber terrain."

The right place to start doing this is Active Directory. If a security team is not involved in how the Active Directory is organized and managed, they will likely never have much success in protecting the environment. Active Directory infrastructure has a tendency to grow and organize itself based on ease of management, not security principles. Some IT service management teams are downright negligent in how they have set up their environment.

The first thing I look for in Active Directory is how organizational units (OU) are organized. There should be a security strategy applied to how OU's are built out. This provides the ability to logically segment an environment and deny access to resources based on risk of the members of that OU.

For example, a security team is always going to have that group of legacy business applications that for one reason or another cannot be patched in a timely manner. If all of these servers are placed into a high-risk OU group, exposure can be limited to the rest of the network if these servers are compromised due to a lag in patching. This same principle can be applied to the user group OUs. If there is a high-risk category of users, e.g. users authenticating to your guest Wi-Fi, this group should be managed in a different OU than the "normal" user population. This ensures that this high-risk and transient user group has limited access network resources.

The last thing to consider in an Active Directory security strategy is how to manage and create accounts with elevated privileges. At the end of the day, the most sophisticated actors usually try to elevate privileges so that they "become" an "insider."

Multifactor authentication and a close monitoring of users that have elevated privileges will put up a significant barrier for most threat actors and limit the attack surface area.

The next step when assessing architecture is to look at the segmentation of datacenters. The NIST model of the three-tier datacenter architecture should be the goal. Whether it is segmentation between a webserver, application and database, or micro-segmentation between development, testing and production, this is a task on which the success of the security team depends.

The way software development happens today, engineers go to their software libraries at repositories, such as GitHub, and download libraries to achieve whatever feature they are trying to develop in a project.

Often the software developer has no understanding of what ports and protocols are required, so they like to provision servers in a "trust all" mode. Instead, every server should be provisioned with a "zero trust" model approach, meaning that all ports and protocols should be closed and only the ones required by the application should remain open.

Another common mistake is combining server functions on one host, e.g. hosting an application on the webserver. IT service managers like to use this strategy because of its low cost; however, this practice is high-risk and does not allow for the security team to manage a well-segmented environment.

The last point of discussion on architecture is remote access. This is a very short conversation—all remote access into an environment MUST have multifactor authentication. Users loathe this because it makes accessing the environment remotely more difficult and/or time consuming. However, without this security control, it is not a matter of "if" but "when" an environment will be compromised and owned by a targeted or advanced targeted actor.

ONCE THE ARCHITECTURE IS OPTIMIZED, THE NEXT STEP IS TO NARROW THE FOCUS OF SECURITY OPERATIONS TO ENSURE THE BEST BANG FOR THE BUCK

Refining security

Once the architecture is optimized, the next step is to narrow the focus of security operations to ensure the best bang for the buck.

In my experience, threat actors are usually only interested in two percent of a network, but they use the other 98 percent to gain access to it. With limited resources available, security teams should purposefully focus those resources to mitigate the highest risks.

The first step, which is the one nobody wants to conduct, is classification of data and business applications to understand which are the most critical to protect. The old military saying "Those who protect everything protect nothing" really drives this point home. I have met with organizations that have 20+ security classification categories. That level of granularity is unnecessary. It is far more manageable and repeatable to start simple with three categories:

1. *Low:* The data or application is public knowledge and there can be no damage if it is compromised

2. *Medium:* Workloads and data are critical for business operations and, if disrupted, there will be a serious impact on business.

3. *High:* Compromise or disruption at this level can have existential consequences for the organization.

Once the classification is done, security dashboards and custom views of the security telemetry received from controls based on risk can be established. On our security team, we refer to these as "Named Areas of Interest," meaning we are focusing on these critical systems more than on other systems of lower risk.

Another strategy to consider is how much of your security team's efforts should be put towards trying to protect user terminals. Cutting-edge security teams are assuming their user base is already compromised. Instead of trying to monitor tens of thousands of user terminals, they are closely monitoring the ingress and egress points between the users and business applications, looking for anomalous activity.

They are also putting in some architectural designs that treat identity as a security perimeter, such as requiring sandboxed browsers for web applications and multifactor authentication.

Banks and popular cloud applications are already using this exact strategy to protect their infrastructure from their customers, who they assume are compromised.

AN "EGO-FREE" APPROACH HELPS EVERYONE ACKNOWLEDGE THAT TEAMWORK IS NECESSARY TO KEEP SOPHISTICATED HACKERS AT BAY

Keeping pace

Even with these strategies in place, security teams will always struggle to keep up with evolving threats. Diligence is key to anticipate and stay ahead of what could potentially harm an organization. Another important element is to have a team in place that is not afraid to admit they don't know everything.

An "ego-free" approach helps everyone acknowledge that teamwork is necessary to keep sophisticated hackers at bay. This is a dynamic field in a constant state of flux; thus, a security strategy should be fluid and flexible and - most importantly - regularly evaluated, assessed and adjusted.

Jeff Schilling is Chief of Operations and Security for Armor's (www.armor.com) cyber and physical security programs for the corporate environment and customer hosted capabilities.

Black Friday sales and enterprise data: Compromised information on the dark web

Emily Wilson

At Terbium Labs, we see a lot of stolen data. As a dark web data intelligence company, our systems alert us to countless sets of stolen credentials, databases for sale, leaks of insider information, and personal details released in revenge-motivated doxing attacks.

Organizations face a difficult task in combatting stolen information on the dark web. Companies are running against the clock when it comes to third parties exploiting or announcing a data leak.

Who will be the first to leak the story? How much can someone damage a customer's account before someone realizes it's been compromised? What kind of backlash will the organization face as a result of a leak that could have been prevented?

In this article, I break down the three types of compromised data we see and the two ways in which that data appears on the dark web. Depending on the motivation behind the theft, stolen information appears very differently and, realistically, companies need to plan for both types of data leakage.

Three types of data: Yours, mine, and ours

When we talk about identifying data, we are really talking about information that falls into one of three categories: attributed data, unattributed data, and misattributed data.

Attributed data comes with a clear declaration of ownership, typically in the form of a title: "Your Company's Employees" or "This Retailer's Database". With attributed data the exploitation clock ticks even faster. If you can see the title on the listing, on the paste, on the dump, so can others.

Aside from the other criminals who might try to exploit the information, there are countless outlets devoted specifically to announcing the latest data breach (to say nothing of the traditional media sources, which are quick to pick up on a leak large enough to garner at least a mid-level headline).

Attributed data usually surfaces for two reasons: when someone is trying to build publicity and, perhaps more frequently, when someone makes it easier for others to exploit that stolen data (e.g., "these credentials belong to a video streaming service, use them there").

Unattributed data is a different beast altogether. Most of what we see is unattributed data, sets of information with no name and no other indicators. Whether you're dealing with a list of credentials, a spread of credit card numbers, or a stripped-down database dump, unattributed data gives you little to no sense of its source, and even less sense of its ownership.

We often see long lists of email addresses and passwords with no other identifying information. Are they customers from an online retailer? Are they social media accounts? Are they bank account logins? Are they personal email accounts of members of a political party? Often, these sorts of data leaks are samples linked to from ads offering the full, attributed data sets for sale. Other times they are presented as proof by novice hackers to show off their achievements, or parts of doxing attacks where the source of the data is of less interest than the data itself.

Misattributed data is compromised data that isn't what it claims to be. A few months ago, news broke about a massive breach across several popular webmail hosts. Contrary to early reports, there was no single breach, and the list of email accounts was compiled from a plethora of smaller, distributed breaches over time, as part of the natural flow of having email addresses affiliated with other online accounts. That is misattributed data.

Misattributed data can be wrong on two counts: incorrect about the source of the leak, or incorrect about the ownership of the data. In the case of the webmail hosts, there's no denying the accounts belonged to Gmail, or Yahoo, or Hotmail. But that's not where the breach took place, and that is not where the data originated.

Finding any of these three types of data online can be difficult at best and impossible at worst. Compromised information appears in two main ways: as an invitation for vandalism (information is dumped publicly), and for sale (the details are safeguarded behind a paywall). Even if you are constantly looking for the appearance of data with your name on it, you are not going to catch everything – as I mentioned earlier, most of the compromised information we see is unattributed. And when information appears for sale, you may only have one or two samples to serve as indicators of compromise.

PUBLIC DUMPING OF INFORMATION OCCURS WHEN PEOPLE BELIEVE THAT THEY WILL GET MORE BENEFIT OUT OF DOING IT AND ANNOUNCING THE LEAK

Nice data you have there: Vandalism on the dark web

Public dumping of information occurs when people believe that they will get more benefit out of doing it and announcing the leak, or that the information is impossible to sell. The criminals' motivation here may be retribution, hacktivism, or "just because we can."

Some of these leaks appear as part of a broader operation, e.g. in the case of work done by, or in the name of, Anonymous. #OpWhiteRose, an Anonymous operation targeting the KKK, was far better served by publicly leaking information than by trying to turn a profit. A list of Klan members probably would not have garnered much interest on a marketplace, and the media may not have even picked up the story. Once the information appeared publicly, however, it fueled investigations and excited curiosity that was guaranteed to provide some attention.

SECURITY IS AN ONGOING RISK MANAGEMENT PROBLEM

Going once, going twice: Data for sale

In order to understand the sale of stolen data on the dark web, you first need to understand this: the dark web is a transient, but well-oiled machine of anonymous e-commerce.

The markets may go up and down, and vendors may trade in illicit goods, but by and large the dark web functions like any other part of the Internet. Like other commercial entities, these dark web vendors market themselves by offering promotions, sales, and samples.

Black Friday is a particularly popular day for fraud sales. These samples are important when thinking about detection and remediation. Sometimes a sample of data – a single card, a handful of credentials, a snippet of source code – will be the only insight into a much larger compromise of your systems.

Secondly, know that dark web sales are anonymous by design. When dealing with transactions in the fraud space, where no physical goods need to be shipped, vendors on fraud markets allow the buyer a relatively hands-off experience in their transactions.

Given the foundational anonymity of the dark web, trade in stolen data relies heavily on vendor reputation. In many cases, the vendor's reputation is more valuable than the actual origin of the data for sale.

Data for sale will only appear with as much detail as necessary to make a sale. Vendors have no reason to reveal the source of their information unless it will provide additional benefit to the buyer – benefit that outweighs the potential costs of exposing your source. Why announce a compromised point of sale or an ongoing exploit? Why cut off your supply chain? Vendors only need to provide as much information as buyers require to take action with the stolen data. In many cases, that is not much information at all.

What does this mean for companies?

We've discussed how data appears online – in full, when exposed as part of a vandalism-motivated campaign, or as brief indicators of compromise when up for sale. Data appears with and without attribution, and is often attributed to the wrong source.

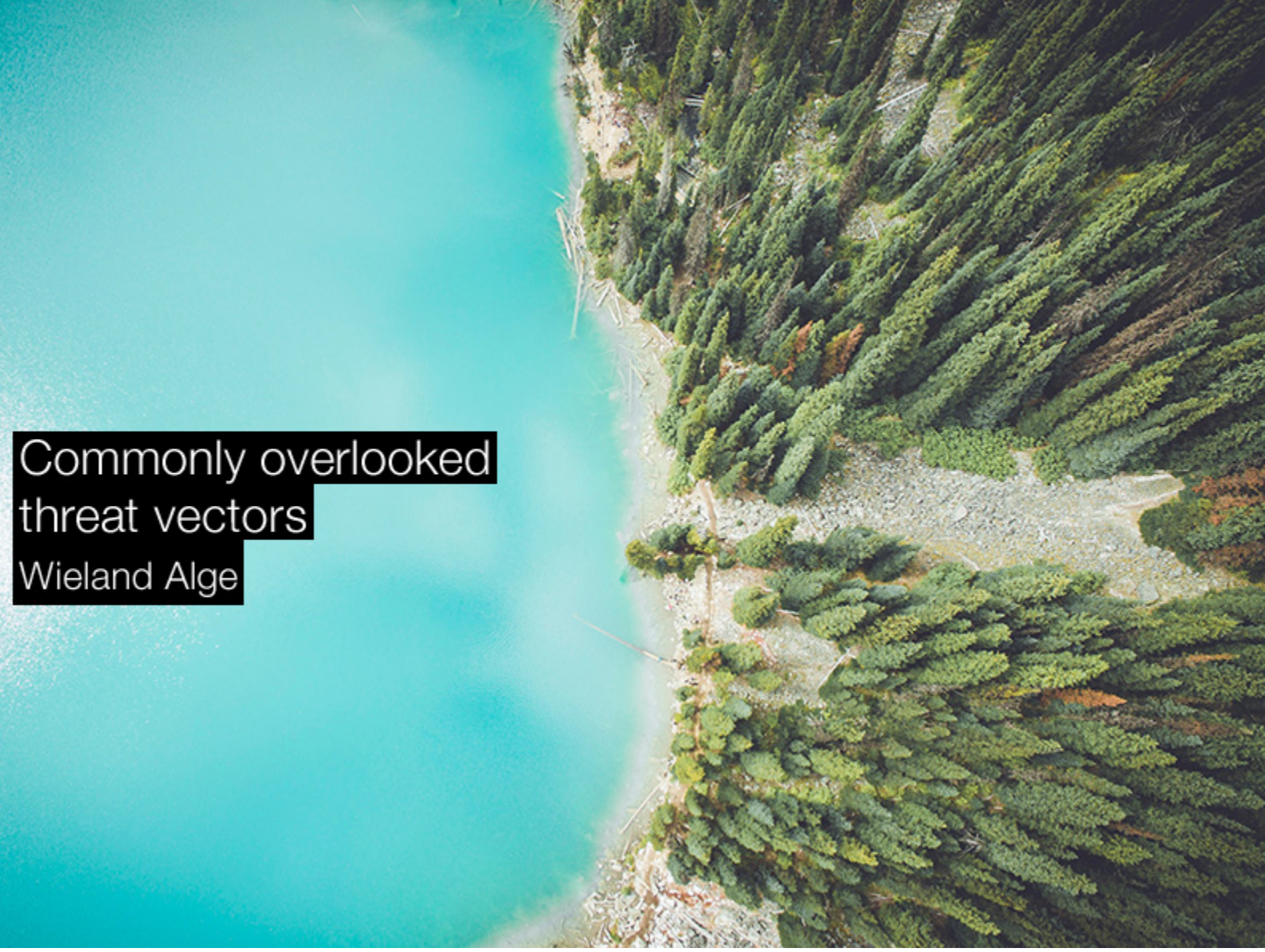
So how can organizations plan to deal with compromised data? By knowing as quickly as possible when it appears online.

Security is an ongoing risk management problem, and companies must plan more broadly than monitoring their networks for suspicious activity. Proactive monitoring of sensitive information serves as the early warning system for data leaks – knowing the moment something appears online, and being able to quickly assess whether or not your company is the source of that data.

Sometimes you may have only a snippet of information to work off of, and that single indicator of data for sale is as valuable as triaging a leak of thousands of customer records in a vandalism-motivated campaign.

If you cannot realistically prevent every single breach (and you can't), you should be in a position to catch a leak as soon as it happens and to take action quickly. The trade in stolen data is not going away. The best you can do, for yourselves and for your customers, is to be prepared.

Emily Wilson is Director of Analysis at Terbium Labs, a dark web data intelligence company based in Baltimore, Maryland (www.terbiumlabs.com).



Commonly overlooked threat vectors

Wieland Alge

If you're a CISO or CIO, then you're probably having sleepless nights thinking about the possible risk of cyber attacks and the impact that a successful breach could have on your business. The problem you face is one of growing magnitude – you know that cyber attacks come in many different shapes and sizes and that hackers have a seemingly expansive arsenal of tools at their disposal.

You're probably already investing in the latest security devices, employee training, and new detection and prevention technologies to try to keep ahead of the game. In fact, research from IDC suggests that you and your peers will continue to increase this investment, spending a predicted $101.6 billion on cyber security in 2020, an increase of 38 percent when compared to 2016 figures. But if businesses are increasing investment in cyber security, why is the number of breaches still increasing?

You often hear experts talking not just about increased spending, but targeted spending in the right places. As hackers diversify their attack tactics and look for vulnerabilities in different places, businesses should be looking to block commonly overlooked threat vectors.

These vectors are not unknown to them, but they currently don't get the same attention by the defenders as those that are more "traditional."

With that in mind, here are some highly vulnerable threat vectors, and best practices for making sure that they're adequately protected.

Web applications

Modern, advanced attacks exploit multiple vectors, including user behavior, systems, and applications, and a comprehensive security posture should extend across all these vectors. Web applications in particular offer a huge attack surface.

According to the 2016 Verizon Data Breach Investigations Report (DBIR), 82% of breaches in the financial services sector were the result of successful web application attacks. This percentage stands at 57% for the information sector and at 50% for the entertainment sector.

Some larger businesses have literally thousands of web applications. There are already a lot of known vulnerabilities, both on the back-end database and client-facing side. Unless organizations start focusing on application security, that number will continue to grow.

So, make sure that every web application is protected by a web application firewall, that they don't have direct access to databases, and that the databases they have access to only contain the needed information.

Constantly assess your most critical applications and prioritize fixing the vulnerabilities that could lead to the most damaging data breaches. Also, get your management to promote and developer teams to implement a secure coding philosophy.

Hybrid elements

In most businesses, at least some network components are moving out of traditional, physical data centers to cloud environments. Unfortunately, it's often misinterpreted that the cloud service provider takes on the security responsibility for these elements. In fact, they become part of a shared responsibility model – the cloud provider maintains the security of the cloud infrastructure, while the customer is responsible for the security of what they're running in that cloud.

For example, there is no way for a cloud provider to know that a workload is experiencing data leakage – they aren't controlling the application. Similarly, a zero-day attack targeted at an application may have no outward indication of its malicious nature, so companies must bring their own security to these hybrid elements.

If you move your web application to the public cloud or if you use a SaaS application like Office 365, make sure that you have the same security and access controls that you have for your on-premises infrastructure.

Leverage the agility and elasticity of the cloud to deploy more firewalls at the right places to protect network and application traffic that is running specifically in the cloud. Use the same data encryption that you would use on premises for data that is created and stored in SaaS applications (such as Office 365 and Salesforce). Make sure that your hybrid elements are protected with the same identity and access control measures as other parts of the infrastructure.

Remote workforce

Most organizations have at least some members of their workforce permanently outside the corporate perimeter, or located across various branch offices. Most of these employees use mobile devices that are not company owned. These remote and mobile workers are often not as well protected as those inside the corporate perimeter, simply because businesses overlook this attack surface. But today's attackers will try to exploit "human networks" as well as computer networks, and it is harder to control those working outside the physical boundaries of the network

All users need to be protected against things like phishing, spear phishing, typo-squatting and social engineering.

The demands for the CIO are three-fold. First, you must to make sure that the security between the branch offices, central offices and the Internet is equally robust. Second, you need remote access and security for employees that are outside an office. Third, you need to make sure that SaaS and other line-of-business applications are available and that data is secure regardless of where the workforce is located.

Dispersed networks need a more advanced firewall infrastructure. Each branch office represents several attack surfaces, such as user-to-service and user-to-cloud. A firewall at each location can secure these attack surfaces and improve user productivity.

Firewalls in all locations can also ensure that micro-segmentation can happen across all of your network, not just at the HQ.

Good human security requires a combination of enforcement, monitoring and user education that encompasses all employees, no matter where they're located.

Latent threats

When we think of email-borne threats, we commonly think of spam and phishing. Most of these hazards are generally noticed when they arrive in the mailbox. And while this type of attacks are, of course, legitimate concerns, the latent threats existing in corporate inboxes are also very real and can be very dangerous.

A latent threat is one that gets introduced into the email system from an external or internal source, and hides itself until it's ready to work. It may be waiting for a particular date to activate, or it may be quietly gathering intelligence.

Latent threats are also referred to as APTs, and there are plenty of examples of these in action. For example, the Sony Pictures hack in 2014 was widely regarded as a perfect example of how an APT can be put to work with devastating consequences. The hackers monitored the victim organization's network for a long time and were able to carefully plan when and where to strike. They took advantage of the fact that the company had installed lots of security technologies, but was making no effort to monitor and scan for latent threats.

Good human security requires a combination of enforcement, monitoring and user education that encompasses all employees, no matter where they're located.

The latent threat problem is a much bigger issue than you might think: our research team found that out of 20,000 Office 365 mailboxes, 93% of user accounts had at least one APT present.

This same analysis showed an average of 125 threats per account. Left alone, these latent threats can pose a real problem, regardless of any efforts to protect your infrastructure from new threats.

Make sure to regularly scan and clean up any and all existing threats from your infrastructure, so that your internal network is not a biotope for enemies.

Micro-segmentation often leads to detection of suspicious behavior. Always assume that one or more of your users and their devices have already been hijacked.

Similarly, on-premise or hosted web applications must be regularly scanned and patched for vulnerabilities. Invest in the right people – not just technologies – that are capable of detecting an APT actor moving around in your systems.

Supply chain

Third parties throughout an organization's supply chain are now one of the greatest risks to security. They have played a role in many of the headline-grabbing mega data breaches over the last few years – Target, Home Depot and AT&T Services, to name a few.

Most businesses will have some controls in place for supply chain security, but the commonly overlooked element of the supply chain is SMB suppliers. This is usually because those in charge of security believe that the time and effort required to review every SMB partner's security far outweighs the risks they pose. But hackers are now actively pursuing weak links in the supply chain, and those could be the seemingly insignificant vendors way down the security priority list.

My advice to you is:

- Embed a risk-based information security management scheme within the supplier management program
- Educate from the top down about the importance of cyber risk management, and produce a plan for balancing time with risk
- Allow third-party access to data and core systems only when it's strictly necessary
- Instead of paper policies and audits, consider funding the suppliers' security, and control the interface from the source
- Make sure that data protection policies are equivalent across all third parties that have access to critical assets.

Hackers are now actively pursuing weak links in the supply chain, and those could be the seemingly insignificant vendors way down the security priority list.

A note on commonly targeted threat vectors

Two of the five commonly overlooked threat vectors are also included in the five commonly targeted attack vectors, namely: email, the network perimeter, endpoints, web applications, and remote users. Each vector requires specialized protection and it is important to have and use the right tools, people and processes to cover all threats.

With so much to do, it is tempting to throw plug-and-play technology at the problem, but this is a naive approach. Disparate security solutions from multiple vendors come with the cost and complexity of dealing with multiple administrative interfaces, disjointed monitoring, and multiple support processes. This complexity can eventually lead to gaps in security.

Instead, easy-to-use solutions, consistent user interfaces, centralized management and monitoring will help organizations reduce administrative overhead, ensure a comprehensive security posture and free up time to review the security of those overlooked issues that might be hiding in plain sight.

Wieland Alge is the VP & GM EMEA at Barracuda Networks (www.barracuda.com).

Kaspersky Lab sets up a global ICS-CERT

Zeljka Zorz

The European Network and Information Security Agency (ENISA) has been doing its best to advise critical industries in EU member states on industrial control systems (ICS) security, and Japan's CERT is actively dealing with ICS and SCADA issues, but for years the US Department of Homeland Security's ICS-CERT has been the entity to which many industry operators have turned for information and help. Now there is another one.

Formally launched in October, the Kaspersky Lab ICS-CERT aims to be an entity that collaborates with critical infrastructure operators, vendors and government institutions around the world.

"We see a lack of general coordination and information exchange in the world regarding ICS/SCADA security," Andrey Doukhvalov, head of future technologies and chief security architect at Kaspersky Lab, tells me.

"ICS organizations demonstrate low knowledge of the modern attack and don't really know how protect their assets. There are many standards and recommendations, but they are all optional."

The DHS ICS-CERT - a government service, based on government regulations - does not have authority to force commercial ICS organization outside of the US to change their environment and add more security. Kaspersky Lab hopes its ICS-CERT - a private organization and non-commercial project - will have more success.

Doukhvalov says that both organizations provide more or less similar services for clients and partners, and that they are not competitors. "We already have a good relationship with the US ICS-CERT as well as with Idaho National Lab and US government organizations responsible for ICS/SCADA security. Our researchers inform those organizations when they discover a new SCADA 0-day or see significant incidents."

The collaboration with the US ICS-CERT and other CERTs in the ICS protection area will continue.

"We see our role as global proxy in the field of ICS/SCADA security. Since Kaspersky Lab has a presence in most countries in the world, we can educate and help organizations globally to become more secure and ready for future threats," Doukhvalov points out. "We have accumulated very good knowledge on ICS protection and we felt we should to share it and provide our vision and competence to community."

Kaspersky Lab ICS-CERT will provide information and expertise to its members free of charge. They will help companies to assess current defense situation on their industrial objects, offer periodic reports showing the current threat landscape, statistic information, training, help with the implementation of resilience measures, provide forensic investigation, do vulnerability research, and more.

"Our website (ics-cert.kaspersky.com) has a related services subscription for all interested legitimated users. We encourage vendors, industrial and ICS organizations to subscribe and use this service in any of the three available forms. But note that we require NDAs and a verification telecom meeting for all subscribers that want to get information on zero-days and other vulnerabilities," Doukhvalov explains.

KASPERSKY LAB ICS-CERT WILL PROVIDE INFORMATION AND EXPERTISE TO ITS MEMBERS FREE OF CHARGE

The team is interspersed across several continents. There are vulnerability researchers who are already actively analyzing existing ICS/SCADA software and hardware for security issues, and report discoveries to vendors and CERTs. Other experts are providing services mostly online but also go on-site.

Since Kaspersky Lab is a global company, they have virtual members in every country where they have a presence.

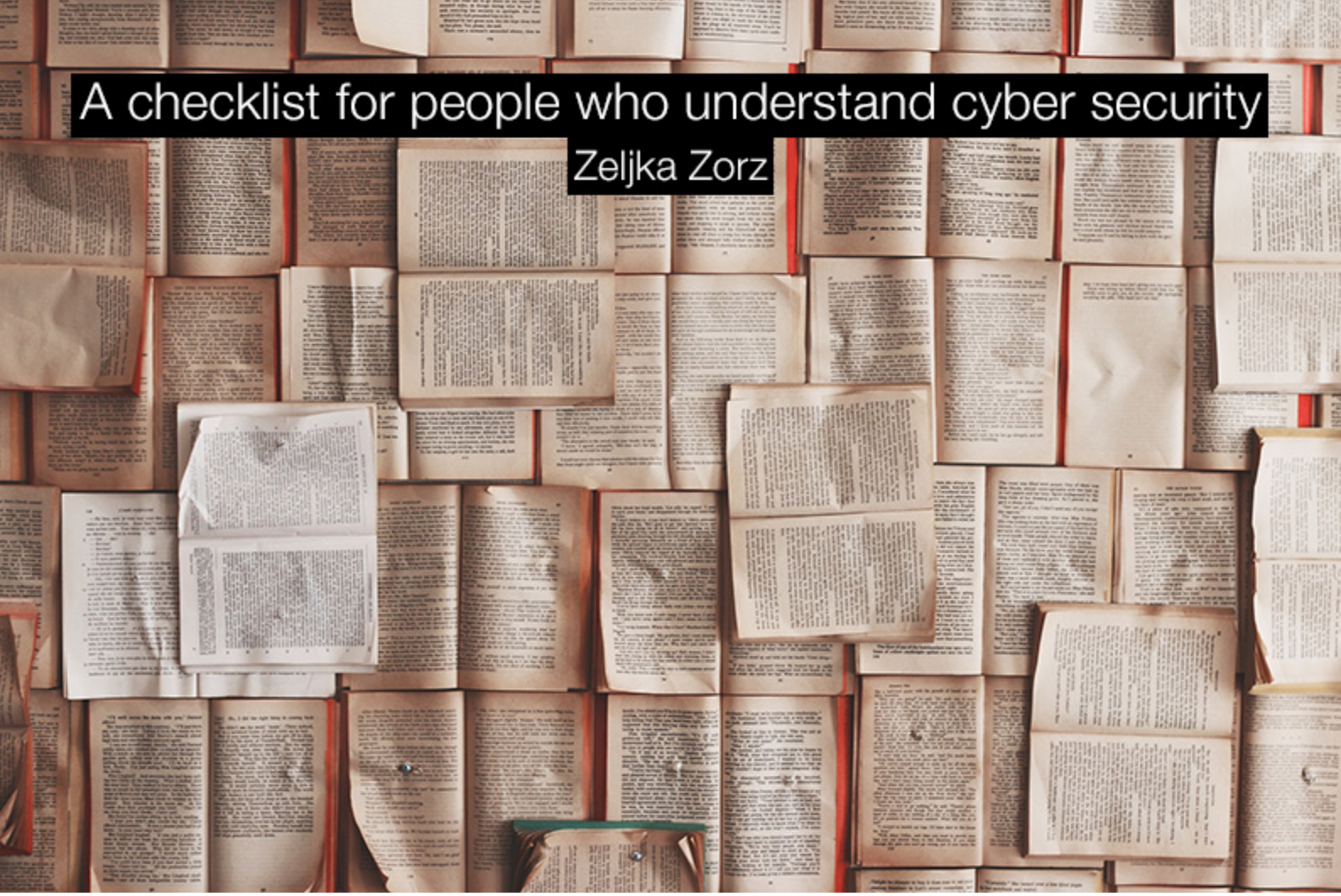
"However, we do not want to create a completely new company inside of Kaspersky Lab, rather to use existing resources - experts help from other Kaspersky Lab teams - per request," says Doukhvalov.

"We will grow the team if we will see demand from the community. We already have a number of requests from different companies and individuals to share information, and this confirms to us that we are on the right track."

They hope their initiative will stimulate information exchange between automation vendors, integrators, possible clients, security experts and providers, and will lead to a higher level of ICS protection.

Naturally, they also hope that the CERT will help the company be recognized as one of the most experienced players in industrial automation cyber security.

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine & Help Net Security (www.helpnetsecurity.com).



A checklist for people who understand cyber security

Zeljka Zorz

By now, it's pretty much an accepted reality that it's only a matter of time until an organization – any organization – gets breached by cyber attackers.

But system penetration does not mean game over for the defenders, as attackers still have to do other things to achieve their goal (steal business information, login credentials, intellectual property, etc.). This means there are many other opportunities and ways to stop an attack from succeeding.

How to do it, though?

Independent research institute The U.S. Cyber Consequences Unit (US-CCU) is offering a helpful tool for defenders looking not only to block attackers, but to increase attackers' costs, i.e. reduce their returns, and to stop them achieving the ultimate goal of the incursions. It's called the US-CCU Cyber-Security Matrix and, as Scott Borg (one of the authors) tells me, it's a cyber security checklist for people who actually understand cyber security.

"Most detailed checklists are designed to be applied mechanically by technically proficient idiots. This one is designed to be applied intelligently and creatively by people who actually know what they are doing," he points out.

The idea behind the US-CCU Cyber-Security Matrix

The recent history of destructive cyber attacks provides many examples of organizations that had their cyber defenses fail in very costly ways, because they had "checked all the boxes" without thinking through what business operations were defending and what kinds of attacks they needed to stop.

The era of generic, one-size-fits-all cyber security is coming to an end. Organizations today need to customize their security to fit the specific kinds if threats they will be facing and the specific operations they most need to protect.

This is where the matrix comes in, as a "menu" from which to choose adequate and cost-effective defensive measures and policies.

"All the changes we have made to this document during its development are essentially efforts to respond to recent changes in the cyber security environment. In addition to adding many new checklist items, we have gradually eliminated a number of old security measures that we have concluded are no longer cost effective," he notes.

The change from checklist to matrix has lead to the security measures being arranged in a way that will help defenders to think through what each security measure is supposed to accomplish.

Every security measure is listed under a heading that indicates the kind of attacker action it is designed to foil, as well as a heading that indicates the kind of system it is designed to secure.

"The real power of this tool comes from the way it prompts its users to apply their own intelligence and insight," Borg adds. "Although this matrix is written in jargon-free language, so that it will be intelligible to a novice, it really comes into its own in the hands of an experienced expert."

Organizations can use this tool to improve their cyber security to a considerable degree, even before they have spent more money on security tools and services, and the matrix can ultimately be a guide when it comes to shopping for security products.

The basis for the matrix

The content of the matrix comes entirely from real world experiences and observations. None of it is recycled from other checklists, except for the items from the US-CCU's own previous checklist (released in 2007, adopted across the world, and recommended or referenced as a best practice document by the likes of the American National Standards Institute and US-CERT).

That initial checklist was also based on things that the authors have observed first hand.

Although effectively authored by Scott Borg and John Bumgarner, CEO and CTO of the US-CCU, respectively, this matrix also contains measures suggested by a number of well known and reputed information security specialists.

In fact, as the matrix is still taking shape (the latest draft is available for download) and is scheduled to be published in 2017, the authors are inviting anyone who has any relevant knowledge, experience, or insights to contribute.

"Some of the people who have helped improve this document are already thanked in the introduction. We are eager to thank anyone by name in the final version who can come up with suggestions for making this tool better or more complete," says Borg.

"We are trying to collect as many suggestions and ideas as possible before the end of the year, but I imagine we will be making changes right up until the point when we send this document off to be physically printed. We are great believers in the value of printed books, as well as electronic ones, especially when those books are going to be used regularly for reference."

The publication date has still not been set in stone, as it depends on the quantity of suggestions they receive, as well as what sort of sponsorship they manage to attract (the US-CCU is a non-profit, 501(c)(3) organization).

eBay has already provided some sponsorship, but more is needed to print and translate the document

"If our earlier US-CCU checklist is anything to go by, this new reference tool will be used worldwide, downloaded well over a hundred thousand times, and used constantly as a printed reference by tens of thousand of cyber security professionals. Sponsoring this tool would be a good way for a corporation to draw attention to its commitment to better cyber security," Borg concluded.

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine & Help Net Security (www.helpnetsecurity.com).

What's the Risk of a Bot Attack on a Website in Your Industry?

distil networks

Distil Networks Protects Your Web Applications from Bad Bots, API Abuse, and Fraud.

Digital Publishing
32%

Real Estate
31%

Ecommerce
18%

Directories & Classifieds
17%

Airlines & Travel
8%

Your Industry ??%

Contact Distil Today for a Free Threat Analysis

www.distilnetworks.com | @DISTIL | sales@distilnetworks.com | International: 1-866-598-6787 | UK: +44 203 3184751