INFORMATION SECURITY

MARCH 2017
VOL. 19 | NO. 2

THE ROBOT AS A SECURITY ANALYST MOVES CLOSER

Why artificial intelligence and machine learning technology may be the next 'hire' on your security team.

AI OR NOT, MACHINE LEARNING ADVANCES

MIAX OPTIONS CSO ON SECURITY'S ROLE IN BUSINESS CONTINUITY

REPORT: HALF OF COMPANIES PAY RANSOMS

DOXWARE: EXTORTIONWARE REBRANDED OR NEW RANSOMWARE THREAT?

MARCUS RANUM CHATS WITH IBM'S DIANA KELLEY

TechTarget

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

AI or Not, Machine Learning Advances

As cybersecurity companies promote artificial intelligence functionality, CISOs need to ask some tough questions to get past the hype.

BY KATHLEEN RICHARDS

THE LOGIC AROUND artificial intelligence is fuzzy. Some people might argue that the heuristic algorithms used in antivirus to recognize potential threats are artificial intelligence. Others got a glimmer of hope—outside of the security field—with the landmark success of AlphaGo. In 2016, the DeepMind software won four out of five matches of the complex Chinese Go board game when it out-strategized top professional player Lee Sedol. The win astounded viewers and saved Alphabet Group, which acquired the London-based DeepMind in 2014, a million dollars of prize money.

While cognitive advances are clearly being made in numerous industries, information security—which is in dire need of help—remains a complex challenge. As companies promote AI and advanced machine learning in cybersecurity, CISOs need to ask some tough questions to get past the hype: Are these technologies bolted on to get investments as well as customers, or are they core to an innovative security platform that solves a business problem (too many alerts to efficiently monitor)? Is the company's expertise in machine learning and AI or information security?

The excitement and promise of machine learning in cybersecurity is there. But data scientists are in high demand and are hard to find. Qualified researchers who study artificial intelligence usually have some combination of computer science, cognitive psychology and engineering experience. Outside of top universities—like the MIT Robotics Lab—and fields such as defense or specialized computer programming, their numbers are probably in the hundreds.

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

Advances in machine learning and security can help in areas such as antimalware, dynamic risk analysis and anomaly detection, found Robert Lemos, who reports on machine learning in cybersecurity in this month's cover story. The technology is really good at "crunching through data," Joseph Blankenship, senior analyst for security and risk at Forrester Research, tells Lemos. But automation, speed and accuracy (decision-making) are areas where more work is needed.

Also in this issue, we talk to John Masserini, CSO of the U.S. equities trading exchange MIAX Options, about his information security strategy in an environment where disruption is calamitous. Marcus Ranum continues his "How did you get here?" series with Diana Kelley, executive security advisor for IBM. Senior Reporter Michael Heller looks at a new form of ransomware that may take extortionware aimed at businesses to another level. ■

KATHLEEN RICHARDS *is the features editor of* Information Security *magazine. Follow her on Twitter: @RichardsKath.*

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

THE ROBOT AS SECURITY ANALYST MOVES CLOSER

Why artificial intelligence and machine learning technology may be the next 'hire' on your security team.

By Robert Lemos

KEEN FOOTWEAR SELLS its iconic boots, shoes and sandals through thousands of retailers worldwide. But the Oregon manufacturer, which is working hard to honor its commitment to become "American Built," does not have the manpower to support a dedicated information security staff. With a team of six information technology professionals—all but two focused on handling the day-to-day client issues of its 450 employees—the IT staff would fall behind in triaging incidents the company's security software flagged.

"We fit squarely in the realm that we have the problems of all the big players, but we don't have the resources of a large enterprise," said Clark Flannery, Keen's director of IT in Portland.

To solve the problem, Flannery augmented his IT staff with machines. While the company had a traditional firewall and antivirus software to block the most obvious threats, Flannery opted to deploy Darktrace's Enterprise Immune System, a physical appliance that passively monitors network data and then uses machine learning technology and probability theory to model patterns of

HOME
EDITOR'S DESK
COGNITIVE SECURITY
HIGH STAKES CSO
COST OF RANSOMWARE
EXTORTIONWARE EVOLUTION
SECURITY STRATEGIST

behavior and flag anomalous activity. (The "self-learning platform" from U.K. cybersecurity startup Darktrace is based on unsupervised learning—anomaly detection—and recursive Bayesian estimation, and was developed at the University of Cambridge.)

For Flannery, who considers the system a form of artificial intelligence, the machine learning technology means that his team has less work piling up: "With this AI, we do not have to look through the minutia unnecessarily." Instead, he gets reports on events on which the team needs to focus: brute-force login attacks, shadow IT usage or other anomalous traffic.

Who's Got the (Machine) Smarts?

OUTSIDE OF ENTERPRISES adding data scientists to their security teams, machine learning is typically applied to security in three types of companies.

Traditional security vendors—think Symantec and Intel's McAfee—have adopted machine learning in their products, but also use it to reduce the workload of their analysts as they try to keep up with the deluge of new malware. In 2015, the latest numbers available, Symantec had to analyze and classify 431 million new malware variants.

Companies focused specifically on generalized machine learning techniques and artificial intelligence goals have targeted the information security sector as a lucrative application of their technology. Recorded Future, for example, initially pursued natural-language processing to produce intelligence, but has strongly focused on using the technology to gather information on cybersecurity threats.

A number of cybersecurity startups have developed their technology by applying machine learning to specific cybersecurity problems. Cylance and SparkCognition are early adopters of AI techniques to detect unknown malware, for example.

Investments have skyrocketed in these firms. Cylance raised $100 million in a Series D funding round last year, valuing the company around $1 billion, according to CB Insights. Texas-based StackPath, which uses machine learning for real-time threat detection, raised $180 million in private equity. —R.L.

ROBOT: KIRILLM/ISTOCK

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

Flannery is not alone. With the high volume of data that most security teams have to prioritize, machine learning technology is increasingly being adopted as a way to reduce the noise (alerts) that traditional security products produce and to bubble up mid- and high-level concerns to IT staff. The discipline of machine learning finds its way into many large companies through the hiring of data scientists, who use algorithms to efficiently analyze event logs for their security teams.

"If you look at any of the large companies with excellent security teams, they have all integrated data scientists and machine learning, creating new skill sets contributing to this domain of cyber and network security," John Lambert, general manager of Microsoft's Threat Intelligence Center, told attendees of the company's January BlueHat IL security conference in Tel Aviv.

MACHINES BENEFIT SMALLER COMPANIES MOST

Smaller companies, such as Keen, have turned to platforms that incorporate machine learning and AI techniques—and soon automated defense—to solve a variety of problems. "I don't need to go hire someone dedicated to security," Flannery said. "It just feels like a whole team back there—who are way more qualified than [staff] I would be able to pay."

While machine learning and artificial intelligence are often used interchangeably, the concepts are different. Machine learning is a branch of data science that uses data sets to train statistical methods of analysis; it is the launching point to developing approaches to adding intelligence to software. The predictive models and algorithms generally fall into one of three classifications:

> The promise of machine learning, especially as it evolves into something resembling artificial intelligence, is its ability to reduce complexity for human analysts.

supervised learning, unsupervised learning and reinforcement learning.

Artificial intelligence seeks to create software that can *think* about problems like a human. IBM's Watson for Cyber Security, which relies on machine learning technology and natural language processing, may be moving in that direction. The technology can consume unstructured security data—research papers, blogs, video—and uses cognitive processes developed by IBM's research and development in deep learning and neural networks to provide algorithms out of the box. Forty companies in banking, healthcare, insurance and other industries signed up in December 2016 to participate in the IBM Watson Cyber Security beta program.

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

Many cybersecurity providers claim their technologies represent the first generation of AI—IBM is not among them. In general, computational procedures or processes that can be characterized as *intelligent* remain open to debate. A software replacement for a security analyst would arguably be artificial intelligence.

"In the security industry, no one is using artificial intelligence," said Gunter Ollmann, CSO at Vectra Networks Inc., an automated threat management startup in San Jose, Calif. A mentor to tech companies and self-described executive for hire, Ollmann has performed CTO or research roles for NCC Group, IOActive, Damballa and IBM.

Security applications are more likely to utilize advanced machine learning and basic AI techniques. Machine learning technology is used in malware detection, dynamic risk analysis and anomaly detection. The technology can perform threat detection in dynamic environments, but it still requires humans in the loop.

The promise of machine learning, especially as it evolves into something resembling artificial intelligence, is its ability to significantly reduce complexity for human analysts, said Bryan Lares, director of cognitive security solutions at SparkCognition Inc., based in Austin, Texas. The company's DeepArmor antimalware platform uses machine learning, natural language programming and AI techniques to detect infections across networks and devices, including the internet of things. It is still accepting participants for the DeepArmor beta program.

Gunter Ollmann

With a greater number of devices to worry about, and a burgeoning amount of data from those devices to parse, security teams are running up against a productivity barrier. Unless the data is whittled down more effectively, security incidents will continue to be missed.

Yet, when the techniques work, systems using machine learning can bring consistency to the analysis of security events, catching those that might otherwise fall through the cracks. The application of the technology also reduces work for security analysts and IT staff by weeding out the chaff and highlighting the most serious security concerns. Machine learning technology can give IT and security teams added depth of knowledge, detecting patterns or issues they may not have known about.

PROMISE OF THE MACHINES

If the technology can move beyond threat detection and into incident response and prediction—essentially acting as a software-based analyst—then we will have moved into artificial intelligence, said William Altman, tech industry analyst at New York venture intelligence firm CB Insights.

"That's the difference between knowing someone is in

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

your house when they rob it versus knowing they are going to rob it and how they will get in before they do it," Altman said. "With the skills shortage of qualified cybersecurity pros, increased automation of security monitoring and controls is allowing for an augmented approach that allows fewer analysts to respond to the most relevant security red flags."

> "You can't say that you are going to replace your analysts. What ends up happening is that you put your analysts to better use."
>
> *— Golan Ben-Oni, CIO at IDT Corp.*

Some companies have already started down that path. Telecom firm IDT Corp., based in Newark, New Jersey, uses an incident-response system powered by AI techniques to whittle down the volume of data and speed response time. In the past, the company required at least 30 minutes to even detect and start triaging an incident, which then required a minimum of four hours to forensically analyze. And that's for incidents classified as critical, said Golan Ben-Oni, CIO at IDT Corp. Many low- and medium-severity ranked issues ended up being critical, he said.

To address the problem, IDT adopted Hexadite's Automated Incident Response Solution (AIRS) to triage incidents and act, automatically in most cases, to stop potential attacks. In 30 minutes, the company now not only automatically analyzes every alert, but can quickly place a system on a quarantined "remediation network" to isolate it. Following quarantine, a full investigation of the host is conducted with AIRS. For instance, command-and-control server IP addresses can then be pushed to the dynamic, block access lists of the firewall to protect the remainder of the organization. If the system is found to have been infected with something more critical than a potentially unwanted program, as in the case of malware, the host will be flagged for re-imaging back to factory default.

"You can't say that you are going to replace your analysts. What ends up happening is that you put your analysts to better use. It saves you from getting additional people," Ben-Oni said. "The analysts can work on problems that they never had a chance to, like getting in touch with other companies to discuss the origination of the threat."

MACHINE EVOLUTION

Machine learning is really good at crunching through data, but we are still far from replacing security analysts, said Joseph Blankenship, a senior analyst for security and risk at Forrester Research.

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

Joseph Blankenship

"One thing we need to do [is] to make any automation possible—and make better and faster decisions," he said. "So the next milestone will be when we will see something from a tool and have a high enough confidence level to not have an analyst in the equation."

Current machine learning systems have problems with false positives. While numbers are not available, Lares acknowledged that the goal is 99% accuracy in both detecting malware and determining whether a file is clean.

The challenge for companies is that they are trying to hit a moving target. Machines must be able to adapt to detect evolving threats, said Jon Miller, chief research officer at Cylance Inc., in Irvine, Calif. The company offers an AI engine called CylanceProtect for detecting malware and other threats.

"Replacing human detection of cancer with an AI solution is totally possible because cancer today is the same as cancer tomorrow," Miller said. "Unfortunately, in the information security world, there is no natural evolution. Attacks that come at you today are not the attacks that are going to come at you tomorrow."

Organizations can also expect attackers to adopt machine learning and AI techniques. Even with advances in machine learning technology, and even if everyone agrees that it should be considered artificial intelligence, attackers will use these techniques against businesses. By automating software models and the search for vulnerabilities, adversaries will be able to create their own machine learning and AI systems, Miller said. "In the end, the adversary for AI will be AI." ■

ROBERT LEMOS *is an award-winning technology journalist who has reported on computer security and cybercrime for 20 years. He currently writes for several publications focused on information security issues.*

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

MIAX OPTIONS CSO ON SECURITY'S ROLE IN BUSINESS CONTINUITY

Faced with the fast-paced demands of derivatives trading, CSO John Masserini understands the value of aligning controls with business risk.

By Alan R. Earls

ALL CISOs HAVE responsibilities and pressures that make the job fun, interesting and sometimes a bit terrifying. But consider the world of John Masserini. As CSO at MIAX Options Exchange, he is responsible for information security, physical security, business continuity and privacy for the company. MIAX Options has assembled a team with deep-rooted experience in developing, operating and trading on options exchanges. Its trading platform was developed in-house and designed from the ground up for the unique functional and performance demands of derivatives trading.

MIAX Options now lists and trades options on over 2,700 multilisted classes. The company's unparalleled system throughput is approximately 38 million quotes per second. The average latency for a single quote on MIAX Options is approximately 17.38 microseconds for a two-quote block. Disruptions are not only unwelcome, they are practically unthinkable.

Oh, and in his "spare time," Masserini has been known to coach lacrosse and is an avid baker and wine connoisseur.

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

Your organization must face an unusually complex and high-stakes threat picture. How do you develop and implement your defense strategy?

There are two critical factors to consider when developing a strong, but flexible, approach to securing an enterprise. First and foremost, the strategy must be driven by the business goals of the organization, not by the technical need for the latest and greatest tool sets. Focus on the technical infrastructure of the various revenue streams, and you'll quickly gain an understanding of the risks to the bottom line.

Once you understand the potential revenue impact posed by the lack of controls, you'll have a clear vision on a tactical and strategic approach for the security program. The second consideration should also be a way to measure the current state as well as the expected end state once the program is up and running. A favorite of mine is the SEI CMM [Software Engineering Institute's Capability Maturity Model], which measures program maturity on a scale of one to five. Start with the basics of the NIST Cybersecurity Framework as a baseline, measure your maturity using SEI CMM against it, and you'll likely end up with some very clear directions on where to start.

From your vantage point, what current threats or other cybersecurity issues do you think are or should be of greatest concern to CISOs?

Unfortunately, it's the usual suspects—phishing,

John Masserini, CSO at MIAX Options

credential abuse, excessive privileges, watering hole [attacks], malvertising drive-bys … all pose a risk to any organization that lets email in and internal users surf the web, which is everyone. Over the years, countless millions of dollars have been spent on perimeter security. But the hard facts are that, most of the time, a simple phishing email works better than trying to find that one open hole in an external firewall or application.

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

Legacy training methods have done little to educate the users. Many of the successful phishing attacks seen these days are very well crafted and could potentially fool even the most careful users. Endpoint controls have been moderately successful in blocking these attacks, but managing user access is key. From controlling privileged accounts to removing local admin to modeling user behavior—all should be leveraged in an effort to minimize the risk introduced by means of the user community.

Are there any things at MIAX Options that you think you do differently from most CISOs?

One of the approaches that has really helped me over the years, and one that is often overlooked by CISOs, is the value the business continuity plan can bring to the security program. By definition, that plan focuses on the continuity of the business—not the continuity of technology, where many security programs falter. By understanding the revenue generation processes, which are identified and protected under the BC plan, one is able to see how various applied security controls can mitigate the greatest amount of business risk with the least amount of effort. I would encourage every security executive out there to take ownership of—and understand—the business continuity plan as a foundation for their security program. ■

ALAN R. EARLS *is a Boston-based freelance writer focused on business and technology.*

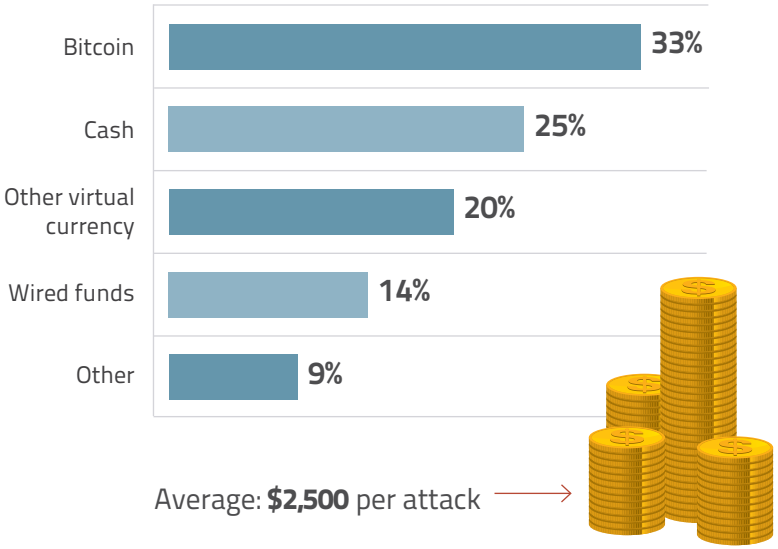
HOME
EDITOR'S DESK
COGNITIVE SECURITY
HIGH STAKES CSO
COST OF RANSOMWARE
EXTORTIONWARE EVOLUTION
SECURITY STRATEGIST

Many Companies Pay Ransoms

The financial fallout from ransomware involves more than bitcoins, one study found. BY KATHLEEN RICHARDS

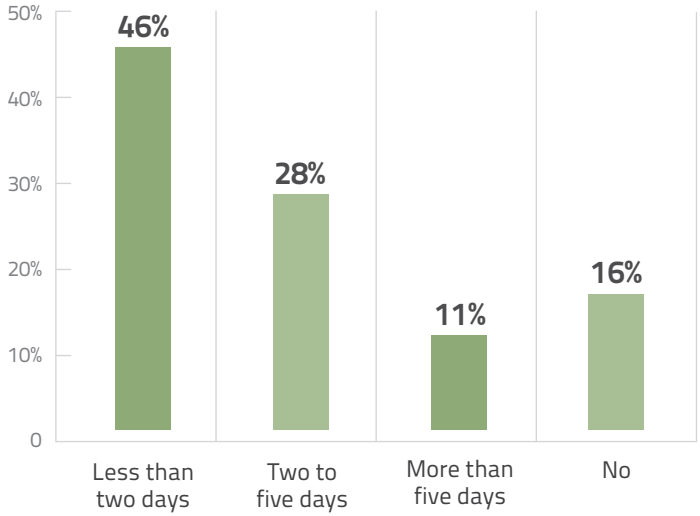
48% Paid the Attackers

How did your company pay the ransom?



Speed Required

Did the ransomware place a time limit for payment?

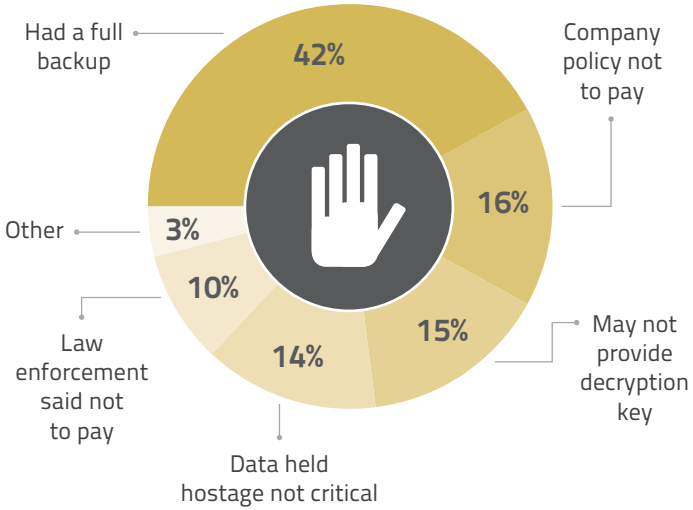


SOURCE: THE RISE OF RANSOMWARE, PONEMON INSTITUTE, JANUARY 2017; N=618; NUMBERS HAVE BEEN ROUNDED; ILLUSTRATIONS: SORBETTO/ISTOCK

HOME
EDITOR'S DESK
COGNITIVE SECURITY
HIGH STAKES CSO
COST OF RANSOMWARE
EXTORTIONWARE EVOLUTION
SECURITY STRATEGIST

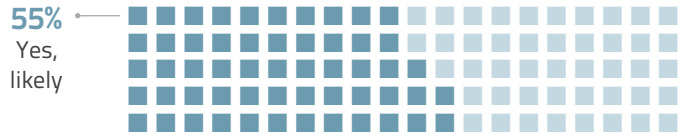
52% Did Not Pay

Why was the ransom not paid?



Stolen Data

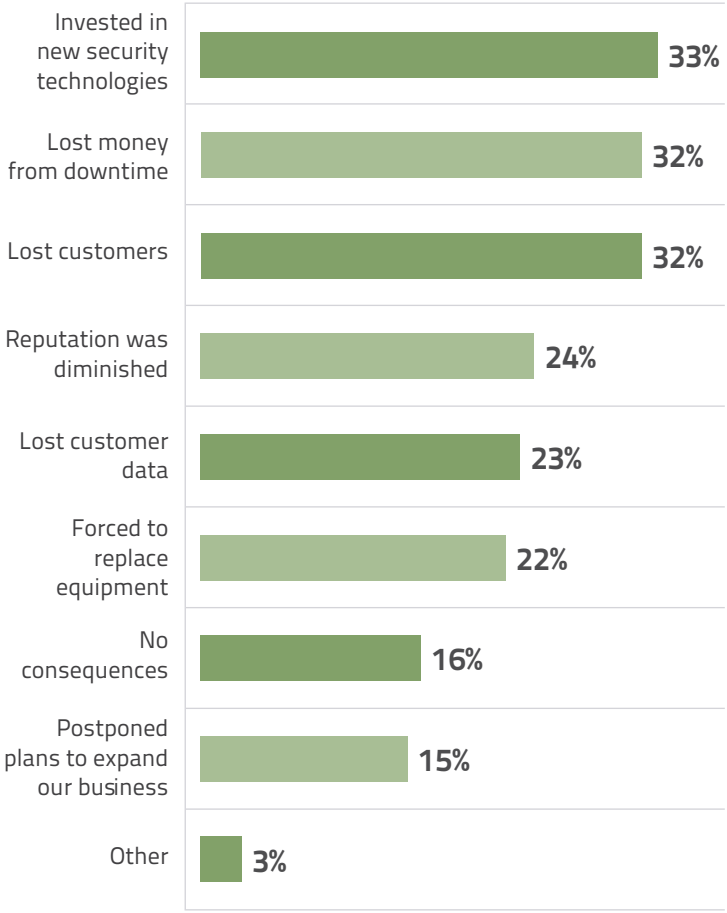
Did the ransomware exfiltrate data from the compromised device(s)?



SOURCE: THE RISE OF RANSOMWARE, PONEMON INSTITUTE, JANUARY 2017; N=618; NUMBERS HAVE BEEN ROUNDED

Financial Fallout

What are the consequences of the ransomware attack?*



*TWO CHOICES PERMITTED

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

DOXWARE: EXTORTIONWARE REBRANDED OR NEW RANSOMWARE THREAT?

A new spin on malware, called doxware, is designed to target and expose sensitive data of ransomware victims.

By Michael Heller

THE EASIEST WAY to scare enterprises these days is to announce a new ransomware threat. Doxware, which gets its name from doxing—the practice of researching targeted victims and exposing their sensitive information online—is a growing concern. But some security researchers are unsure if doxware is a new ransomware trend or a rebranding of extortionware.

"Every few years, there seems to be a change in how we refer to threats," said John Bambenek, threat systems manager at Fidelis Cybersecurity, based in Bethesda, Md. "Part of that is marketing, and part of that is the security community trying to raise awareness to threats that are getting better at being criminal."

On the surface, doxware and extortionware seem to be the same thing: malware variants that combine the data hostage threat of ransomware with the added risk of exposing the data publicly—instead of keeping it encrypted—if the ransom isn't paid. So, in the eyes of many security experts, the two terms can and have been used interchangeably.

"There does not appear to be a difference between this

HOME
EDITOR'S DESK
COGNITIVE SECURITY
HIGH STAKES CSO
COST OF RANSOMWARE
EXTORTIONWARE EVOLUTION
SECURITY STRATEGIST

and what we have traditionally called *extortionware*," said Casey Ellis, CEO of Bugcrowd Inc. in San Francisco. "This simply has a way cooler name."

Jim Walter, senior researcher at Cylance Inc., based in Irvine, Calif., said extortionware and doxware aren't really that different: "The only variation is the extra threat of specific data being released or leaked. So, in that sense, it's a little more targeted," he said. "Beyond that, it is mechanically and fundamentally the same. There is nothing novel going on code-wise."

The subtle difference of targeting is the key to the evolution of ransomware, according to Bambenek. "Traditional ransomware tends to be 'napalm the earth' spam runs that aren't specifically crafted to be attractive to a specific victim."

HIGHER RANSOMS

In contrast, doxware attacks will command higher ransoms because, unlike extortionware, where all victims are threatened with data release, threat actors will either target individuals and enterprises with sensitive data or increase the ransom for victims if sensitive data is found.

"Doxware is a new approach to extortionware that may lead to broader infections," said Chris Burchett, vice president of client security software at Dell. "In the past, doxing was usually a targeted attack, which required attackers to research the target. The new doxware uses the ransomware model of mass-target phishing attacks, but in addition to encrypting data and extorting payment to get the key, the attackers now exfiltrate the data and look through it for possible doxing targets.

"They do this because people started to refuse to pay for ransomware after they got backup solutions in place," said Burchett. "So, effectively, the bad guys are using mass-phishing attacks to 'farm' for doxing targets and ammunition."

Richard Henderson, global security strategist for Absolute Software Corp., based in Vancouver, B.C., said doxware may garner higher ransoms, but it may also not be as widespread a threat.

"Attackers will only be able to launch small campaigns of doxware because they simply won't have the ability to store the millions of files they need to comb through looking for material. Transferring the staggering number of files to the attacker may be detectable because, if the attacker doesn't move the files off the infected machine, then the extortion threat is hollow," said Henderson. "And, perhaps most critically, we shouldn't see attacks like these at the scale we've seen with pure ransomware—targets [and groups of targets] will be chosen very specifically to maximize ROI."

Travis Smith, senior security research engineer at Tripwire Inc., based in Portland, Ore., agreed that doxware is an attempt by attackers to generate more revenue and that the threat is less prevalent: "The amount of doxware or other extortion-based pieces of malware aren't

HOME
EDITOR'S DESK
COGNITIVE SECURITY
HIGH STAKES CSO
COST OF RANSOMWARE
EXTORTIONWARE EVOLUTION
SECURITY STRATEGIST

increasing at a worrying rate."

The reason, according to Smith, is too much effort is involved. "The amount of legwork required to carry out an extortion-based attack such as these requires initial research into the victim, determining the value of the stolen data, then follow-up actions required on what to do with data, depending on if the victim paid or not," he said. "The typical ransomware malware requires little interaction from the attacker's perspective, meaning a higher return on investment for the criminal endeavors.

"Extortion-based attacks will probably not increase for the general public," he added, "but may be worrisome for high-value targets, which may … have valuable data."

BACKUPS NOT ENOUGH

Another difference with doxware? The traditional mitigation for ransomware of making backups is often irrelevant.

"In this case, early detection and mitigation is far more important, as restoring data from backup doesn't help if the attacker has gotten ahold of the actual data and is willing to use it," said Barry Shteiman, director of threat research for Exabeam Inc., based in San Mateo, Calif. "It also means that [data loss prevention] comes into play as well—understanding if there is any data being exfiltrated."

Doxware is a far scarier prospect for business targets of ransomware, agreed Bugcrowd's Ellis. "In a business context, typical exfiltration prevention measures will help make life harder for doxware, but data exfiltration is a traditionally difficult problem to solve," he said. "The key here is a focus on prevention, finding these issues before the adversaries do."

Encryption and phishing defenses are also necessary to defend against doxware, according to Smith. "Backups will still continue to restore confidence in not losing a life's worth of family photos, but will do little to those who don't want private photos or sensitive documents made available to anyone on the internet. Following guidelines to prevent a phishing attack is the best method to continue to avoid an infection—not clicking links or opening attachments from strangers," he said. "Since it's impossible to prevent every piece of malware, it's advisable to prepare for an eventual infection as well. To prevent being a victim of extortion, users should encrypt all of their files while at rest." ■

MICHAEL HELLER *is a senior reporter for SearchSecurity. Follow him on Twitter: @MT_Heller.*

HOME
EDITOR'S DESK
COGNITIVE SECURITY
HIGH STAKES CSO
COST OF RANSOMWARE
EXTORTIONWARE EVOLUTION
SECURITY STRATEGIST

Q&A: IBM's Diana Kelley Got an Early Start in Computing

How did an editor become a security architect? A fascination with computers sparked a lifelong journey for IBM's executive security advisor.

BY MARCUS RANUM

THE INTERNET REVOLUTION hit close to home for Diana Kelley, who caught the technology bug and could never quite shake it. Marcus Ranum sat down with Kelley, global executive security advisor for IBM Security, to talk about the path that lead to her success. In addition to IBM, she has advised Bank of America, Intel, Microsoft, Merrill Lynch, many other tech companies and the U.S. government.

MARCUS RANUM: How did you wind up in security? What were you like as a kid?

DIANA KELLEY: [laughs] I was actually a typical nerdy—but book nerdy—kid. I had a big penchant for Gilbert and Sullivan plays and learned many of them by heart. One day, my dad came home with a Texas Instruments programmable calculator. I was about 9 years old—it was early 1970s at this point—and I absolutely fell in love with it. You could program this thing to do *stuff*. I made it calculate out *Hello*. Later, when my dad decided he was going to build his own Heathkit computer, I was the kid that got really, really excited about this whole 'computer' thing and wanted to work on it with him.

My dad was a research professor at MIT Lincoln Labs, and he had accounts on the PDP computer at Tech Square, and I got a kid account so I could dial in. It was actually a rotary-dial phone with an acoustic coupler—you wait for the beeps and the boops.

I was in the middle of this incredible revolution on the ARPANET: you could send email to people or have chats, and there were games—I think [one] was called 'Adventure.'

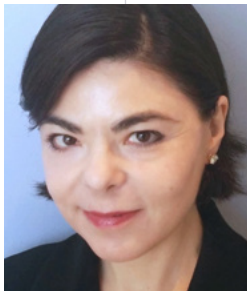
HOME
EDITOR'S DESK
COGNITIVE SECURITY
HIGH STAKES CSO
COST OF RANSOMWARE
EXTORTIONWARE EVOLUTION
SECURITY STRATEGIST

Yeah, I played that one, too. 'There is a little dwarf here.'
I was talking to people who were working on research with mice and IT, and I was just completely floored. It was the coolest thing that it all *worked*. I actually 'hacked' without knowing what I was doing: Nowadays, no 12-year-old would have plausible deniability, but in 1978 or '79, I would say I did.

All I knew was that I couldn't get to the manual pages of the system I was on, and I was talking to someone who said, 'Well, you just don't have enough access.' I was a kid; how could I get access?

Well, the mucky-mucks had access, so I figured out eventually that there was a bug in the login and people couldn't see what they were typing their password into, but you could set the terminal up to ghost their keystrokes and get their password after they entered it. I got an admiral's account, I believe, and I was on one of the .MIL systems in D.C. I was able to read everything I wanted about how the system worked, and the next day there was a phone call to my father.

I think the statute of limitations has run out on that one.
After that, I stayed on, taught myself how to code and wrote my own little adventure game. I didn't take any courses—then I was told that computers were 'nerdy' and I wasn't going to have any friends. I got less interested in computers for a while, went to college for English and


Diana Kelley

focused a lot on Shakespeare, and didn't do anything with computers except that I was the GM at the radio station, and we published our playlist on the old VAX. Sometimes, I had to go in and figure out how to do things with the formatting using Scribe [descriptive markup language]. I got out, graduated and thought, 'Well, what do you do if you have an English degree?'

I thought I was going to be an editor and find the next F. Scott Fitzgerald. So I got a job at the academic press, and we had these old Wang terminals for producing output. Every time those broke, people would come to me. At my next job, I was assistant editor at a math textbook company, and I became the go-to person for computers. I started to do more with IT and became the person picking the software and teaching everyone how to use it. The woman who was in charge of our parent company was there one day, saw me working with the people and computers, and said, 'Look, you obviously love computers, and we have a project starting to network all of our subsidiaries together—we need someone to be our IT person.' My first title was *micro specialist*.

Finally, I ended [up] being the manager/corporate systems administrator for a startup in Cambridge. They had a global set of offices that needed to be connected. This

HOME
EDITOR'S DESK
COGNITIVE SECURITY
HIGH STAKES CSO
COST OF RANSOMWARE
EXTORTIONWARE EVOLUTION
SECURITY STRATEGIST

was when Windows didn't have an IP stack and you had to install Chameleon. …

That'd be around 1992, then.

I used to tail the syslog; I'd sit there and watch it scroll by. If you knew the IP addresses by heart, you could understand what was happening.

Back in 1988 or so, that was how I saw my first-ever security incident! I love syslog.

One of my systems just started to fill up, and it was an FTP server. Christmas Eve at 6:00 p.m., there was me and a contractor sitting there, and someone had taken over our server and filled it with 'warez' [illegal software]. I realized that I hadn't protected my FTP server, and that was when I started keeping security on my checklist. I also [thought at] that moment: I shouldn't have been able to see all those passwords on that system so long ago; this is a *thing*! It's going to be the most important thing going forward. That was when I decided to start to focus exclusively on security.

Most of the security people I've talked to have had some experience like that—they got pulled in on the operational side and got serious about it. Or they started on the other side of the fence and decided to try to teach the 'good guys' how to do it right.

Did you at some point think 'I am a security person now'?

I had already known I was going to be a network person, and the only way to have a world-class network is to understand the bad guys. I realized that I had to be security-focused to be a good network architect. That was when I started learning about firewalls—including your product. [Marcus Ranum invented the first commercial bastion host firewall.] We went into the business of installing firewalls for other people, as a third party, because in those days it wasn't as straightforward as it is now.

From there, I went to a big consulting firm that specifically hired me to be a security architect in financial services consulting. I had an absolute blast: I was hired to focus on security, and here I was in the middle of the big internet build-out in the late '90s, with all the banks and brokerages trying to go online for the first time. The challenges were wonderful, and they're still challenging. ■

MARCUS J. RANUM, *the chief of security at Tenable Network Security Inc., is a world-renowned expert on security system design and implementation. He is the inventor of the first commercial bastion host firewall.*

HOME

EDITOR'S DESK

COGNITIVE SECURITY

HIGH STAKES CSO

COST OF RANSOMWARE

EXTORTIONWARE EVOLUTION

SECURITY STRATEGIST

TechTarget Security Media Group

TechTarget
275 Grove Street,
Newton, MA 02466
www.techtarget.com

COVER IMAGE/PAGE 4: KIRILLM/ISTOCK