2019
SECURITY REPORT

ixia
A Keysight Business

TABLE OF **CONTENTS**

SECTION 01

INTRODUCTION

Welcome to the third annual Security Report issued by Ixia, a Keysight business. Each year, the Ixia Application and Threat Intelligence (ATI) Research Center summarizes the most interesting and prominent internet security trends. We analyze ATI data to help organizations understand where they can improve. We also analyze the data to predict the biggest hotspots for the coming year. In all our work, we aspire to help cybersecurity professionals strengthen their security posture by sharing knowledge of active exploits, new and old.

The Top 5 Security Issues from 2018

- Poor or lacking product security exposed businesses to additional risk
- The human attack vector, via Phishing and Malware, remained reliable
- Poor cyber hygiene continued to persist year after year
- The good intention of sharing product vulnerability information actually led to more attacks
- Crypto mining/jacking continued without abatement

Key Observations

A

In 2018, we observed many successful attacks based on historic vulnerabilities. Legacy attacks dating back to as far as 2009 remained effective. Hackers successfully compromised systems when the systems were unpatched, or because no patch was available for a legacy system. Widespread availability of exploit software that targets well-known vulnerabilities also contributed to the phenomenon. Bad security hygiene, in the form of default login and password credentials, also contributed to the problem.

B

Public cloud architectures created a second vector for new security attacks. Both home-grown and commercial software packages exhibited vulnerabilities. We categorize these into two basic groups: code vulnerabilities and configuration vulnerabilities. Misconfigured security and access policies were a major source of data breach in 2018.

C

Beneath the threats observed lies an unavoidable truth: Network and application complexity pose serious security threats. Complexity continues to grow within enterprise and service provider IT environments. This growing complexity is creating new security vulnerabilities every day. Thwarting security attacks starts with a continuous commitment to security best practices. Tools augment your ability to mitigate threats, but only security best practices can prevent them.

SECTION 02

THE IXIA APPLICATION AND THREAT INTELLIGENCE RESEARCH CENTER

Ixia's strategy starts with an elite team of dedicated cybersecurity professionals that form the Ixia ATI Research Center. This globally distributed team works around the world and around the clock from locations like Singapore, California, Texas, Massachusetts, France, Romania, and India. They monitor and analyze the ever-evolving indicators that could threaten the security of IT networks. The team distills that knowledge into research and rule sets. We incorporate these insights into Ixia solutions to maximize your ability to detect and combat the latest threats.

The ATI team also contributes to the larger security community. The Ixia ATI team shares what it learns with vendors that have been hacked, private agencies (e.g., www.mitre.org), government agencies (e.g., NIST and DARPA), and at global security conferences such as Black Hat and RSA. Ixia also promotes a summer security school in Bucharest, Romania, to help train new security engineers.

The ATI team assesses and validates products that are meant to secure the enterprise. The team serves as a front line of defense, monitoring internet-connected products and analyzing observed behavior to discover exploitable weaknesses in any vendors' product. Security alerts and incidents happen all hours of the day and night, so the team takes a follow-the-sun approach. Dozens of engineers combine to form a single global team that can create and disseminate the latest security intelligence.

In many cases, the team can go from discovery to an Ixia product update within a 24-hour period.

Input to the research process comes from many sources:

- International exploit databases
- The Dark Web
- Scan of security news alerts and crowdsourcing
- Twitter handles of other security researchers
- Partner feeds
- Honeypots actively looking for attacks in the wild
- Independent research (testing and reverse engineering) by the ATI team

Members of the team constantly poll multiple sources to get insights into vulnerabilities. They normalize, correlate, and organize the data to get a clear direction on the threats and how to prioritize them. Team members then investigate the threats and either validate or dismiss them. They research everything to make sure that the threat detection and prevention content deployed in our products is 100 percent correct. This deep research also gives them the utmost confidence in our data and predictions.

The BreakingPoint company established the ATI team in 2005. Ixia acquired BreakingPoint in 2012. The BreakingPoint solution is a security attack and traffic generator that network equipment manufacturers, service providers, governments, and enterprises use to validate network and security resiliency while under load and attacks. Generating traffic using threats based on real-world research is just one way that Ixia and Keysight help harden solutions for applications as diverse as automotive and Internet of Things (IoT) solutions.

Ixia's ATI threat intelligence feed incorporates data in a way no other provider offers. While others in the industry create automated intelligence platforms or open source feeds, those solutions are generally tailored to provide insights related to specific products in a vendor's portfolio. For example, a feed from Microsoft may focus on vulnerabilities related to products and threats relative to the Microsoft portfolio. Ixia threat feeds look at the internet on a global scale, and provide actionable intelligence based on internet-wide telemetry.

ATI intelligence takes the form of a "rap sheet." A rap sheet captures threat intelligence via a proprietary database of known bad actors or offenders. The database is constantly updated, providing real-time actionable threat intelligence. The team validates blacklisted sites continuously, updating the database to ensure new threats are tracked and false positives are removed. Automated rap sheets provide updates as often as every five minutes, delivering the data in real time to Ixia visibility solutions.

The ATI team serves as the guard to security guardians - challenging others in the industry to improve their product security, and constantly monitoring to spot issues before they become epidemics. Ixia is committed to making it as hard as possible for hackers to succeed.

SECTION
03

TOP 5 SECURITY THREAT INSIGHTS FROM 2018

2018 included a mixture of exploits, including some new, as well as many which we had seen before often modified to incorporate more known, unpatched vulnerabilities.

From the attacks observed, we can draw five major conclusions about the state of security threats in 2018:

1. Software security cause the majority of product vulnerabilities

2. Humans are the weakest link: We click lots of avoidable phishing and malware links

3. Cyber hygiene is at an all-time low: Vendors and IT need to clean up their act

4. Security vulnerability disclosures are a double-edged sword: Both hackers and vendors benefit

5. Crypto-jacking activity reached new peaks in 2018: This threat continues to grow

1. Software Security Flaws Cause the Majority of Product Vulnerabilities

Software security flaws contributed to a record number of security incidents in 2018. We saw more new devices than ever before, but we also saw more devices designed and deployed without proper measures to stop, or even limit, threats.

This was especially true for web applications, where bad actors succeeded by exploiting well-understood SQL injection and cross-site scripting vulnerabilities. The use of these two web attack vectors covers the full range of attack delivery, from common spam attacks to automated remote exploitation – the act of taking control of vulnerable servers on a global scale.

Zero-day exploits gave hackers an advantage over IT security teams, who struggled to stay ahead of constant vulnerability disclosures. Some open source organizations attempted to proactively mitigate vulnerabilities by standardizing security controls and measures inside commonly used web development frameworks. However, code fragmentation makes it difficult for these central improvements to address the widespread problem.

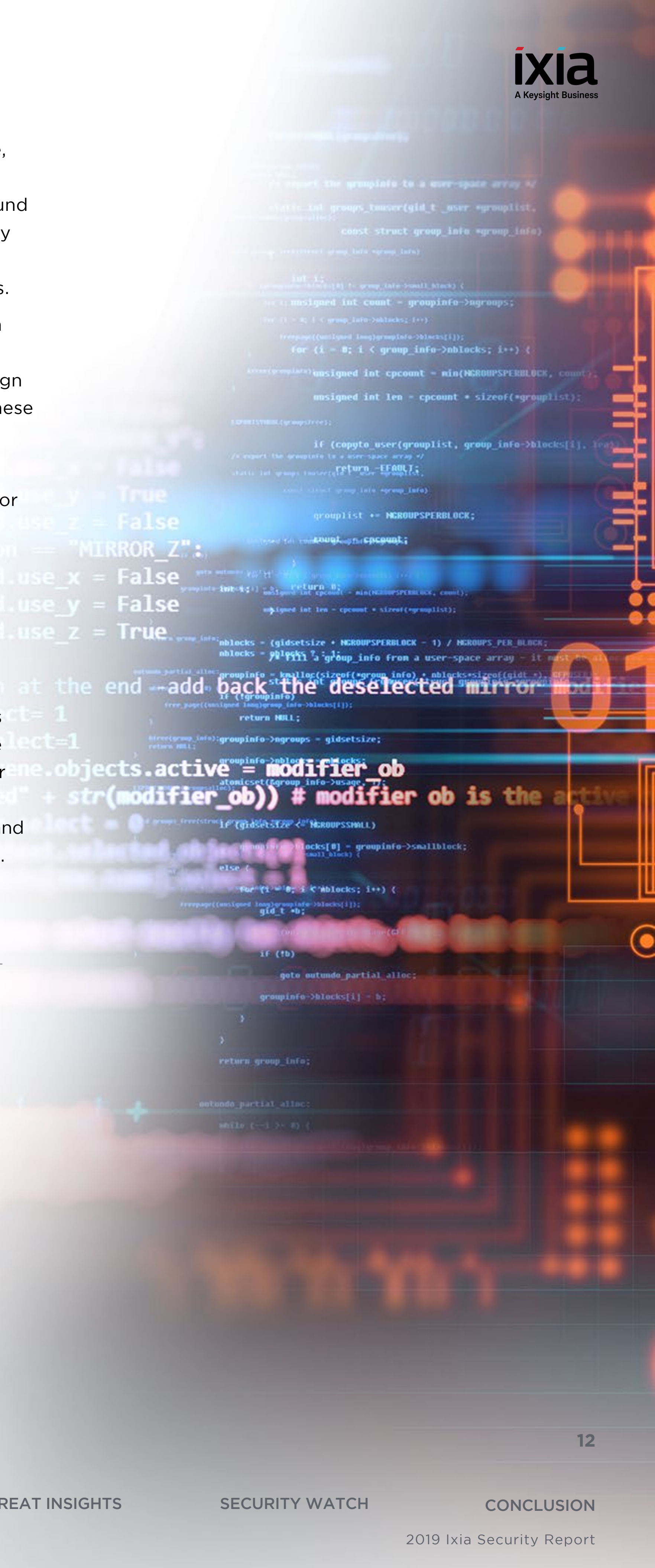
Code sharing carries other risks, too. For example, a recent study[1] examined code fragments on the popular coding site Stack Overflow. The study found that many Stack Overflow answers contain security vulnerabilities. Developers need to ensure they validate all code for common security design flaws.

To solve this problem, web developers and system architects must be educated on security best practices. Until developers embrace software design best practices, attackers will continue to exploit these vectors, sometimes at scale and with substantial consequences, as in the case of Equifax.

Recent examples of exploits that resulted from poor software security practices included:

- Android debugging
- Apache Struts
- Cisco Smart Install

As Gabriel Cirlig explained in a 2018 blog post [2], numerous Android devices have debugging that is either turned on by default or enabled by unaware users. This leads to thousands of devices with their root access exposed on the internet. The Trinity malware took advantage of this product weakness and deployed crypto miners into many of these devices.



[1] https://laurent22.github.io/so-injections
[2] https://www.ixiacom.com/company/blog/trinity-p2p-malware-over-adb

But how long can software vulnerabilities follow you? Figure 1 provides insight to this question. The Trinity malware exposed the Android root vulnerability in the summer of 2018, yet attacker interest continued months later, with Ixia honeypots seeing thousands of attempted attacks daily in December 2018.

The Apache Struts product security weaknesses (CVE-2018-11776) also continued to plague the internet. The vulnerabilities are similar to those observed in 2017, which resulted in the highly publicized Equifax hack that exposed sensitive data of 143 million people.[1] These vulnerabilities put thousands of web applications at risk. Bad actors exploited these weaknesses, using Cryptojacking scripts to infect servers and compromise devices, infecting the devices with crypto mining malware.

[1] https://www.bugcrowd.com/threat-report-apache-struts-cve-2018-11776/

But how long can software vulnerabilities follow you?

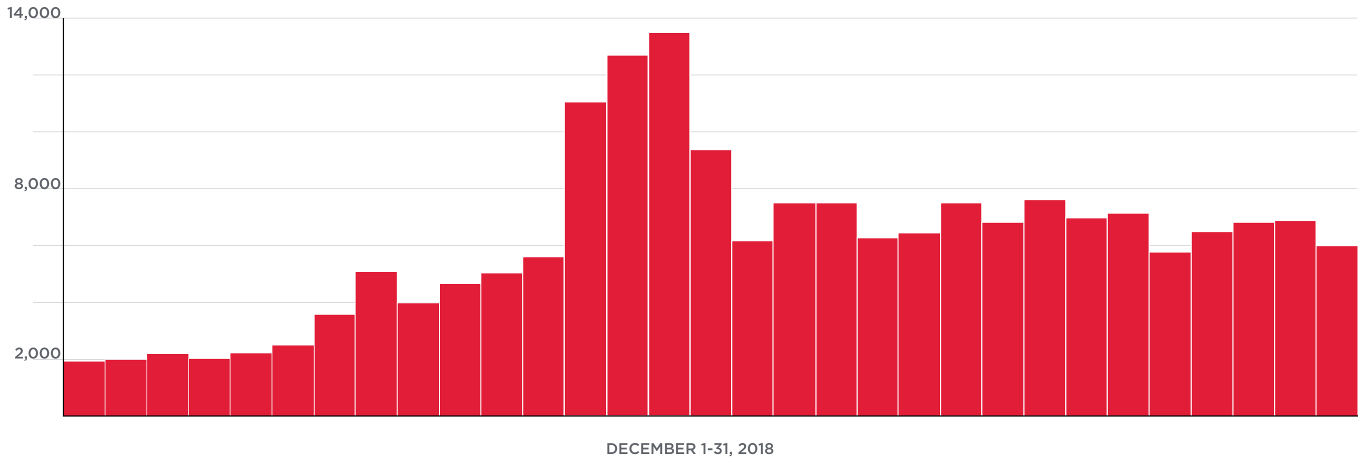


Figure 1. Trinity malware uptick in December 2018

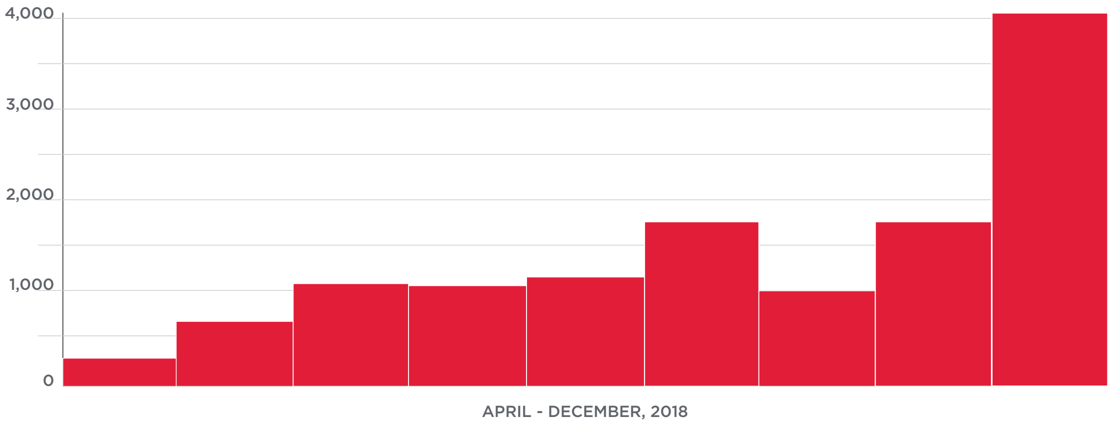


Figure 2. Cisco Smart Install attack attempts in December 2018

Cisco devices were also targets of this type of exploit in 2018. Cisco's Smart Install feature, designed to provide simple configuration of new devices inside a network, provided the attack vector. Nearly two years earlier, researchers documented the security vulnerability and observed an exploit tool known as SIET[1] in the wild. In 2018, new vulnerabilities in devices supporting the protocol revived interest in the exploit. Ixia honeypots started seeing thousands of daily exploit attempts after details of a new vulnerability came out, as shown in Figure 2.

[1] https://github.com/Sab0tag3d/SIET

Recommendation 1:

Buyers should research the common vulnerabilities database and confirm fixes with vendors before deploying new hardware or software upgrades. The CVE database can help customers gauge the security track record and response time of a vendor.

2. Humans are the Weakest Link

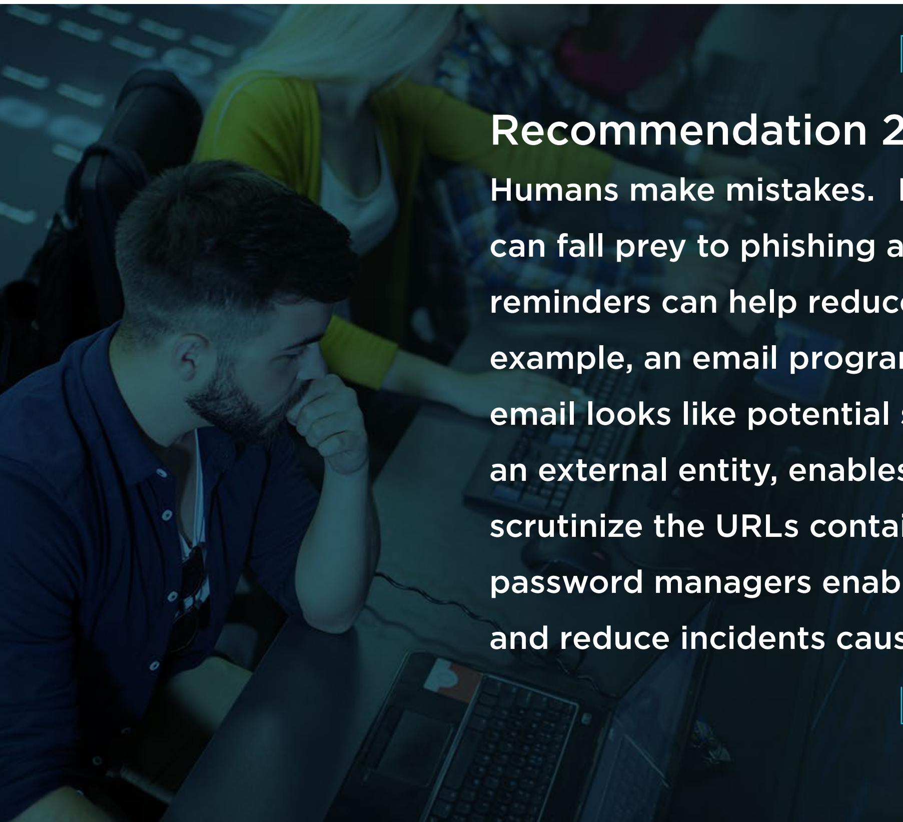
Many recently documented compromises (such as the John Podesta/U.S. Democratic National Committee hack[1]) started with a phishing attempt. As any security researcher can confirm, a well-crafted and well-timed phishing attempt can confuse even the most tech-savvy expert into making a mistake that leads to a network compromise. An attacker can use the results of a successful phishing attack to execute an attack and drop malware on the target's system. Once deployed, the attacker can attempt to move toward systems of higher value inside the network.

Security against the human vector requires a combination of the following:

- Educating users about the risks that exist in the wild
- Detecting and blocking phishing and malware that try to pass the network edge
- Blocking endpoint infection attempts if a phishing attack succeeds
- Detecting and blocking lateral movement when the previous techniques have failed

In 2018, Ixia systems detected 662,618 phishing pages in the wild, and 8,546,295 pages hosting or infected by malware. Clearly, exposure reaches far beyond organizations with weak perimeter security. A successful attack on your infrastructure requires only a single errant click on an email or hypertext call-to-action. While many infected pages that house these attacks are taken down in hours or days, some malware samples live online for years on abandoned websites. One good example is a web page that serves an old version of the Cerber ransomware. Ixia first detected it on November 21, 2017, yet it is still online today. Even though this particular attacker is no longer active, the legacy of the malware lives on, infecting anyone that receives a recycled link.

[1] https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a



Recommendation 2:

Humans make mistakes. Even the most highly trained people can fall prey to phishing attacks. Technological aids or reminders can help reduce the probability of an attack. For example, an email program that highlights when an incoming email looks like potential spam or phishing, or when it is from an external entity, enables you to pay attention and carefully scrutinize the URLs contained in the email. Also, tools such as password managers enable computers to reinforce security and reduce incidents caused by human error.

3. Cyber Hygiene is at an All-time Low

IT product vendors created code or configurations that caused many successful security breaches in 2018, but IT operations and security personnel also shared the blame. Well-known attacks and attack vectors remain successful because security personnel did not address architecture vulnerabilities and apply patches.

This oversight is primarily due to two factors: ignorance of the latest patches, and challenges deploying frequent patches in a timely manner. Both factors leave businesses vulnerable. Many successful breaches in 2018 did not involve new versions of malware or attack methods – existing exploits targeting unpatched vulnerabilities proved to be very effective again in 2018.

Here are some examples of this type of exploit:

- Persistent brute forcing (public facing systems that can be brute forced)
- EternalBlue (disclosed in 2017)
- Dahua digital video recorders (a 5-year-old vulnerability)
- CVE-2009-4140, a web application vulnerability from 2009

Brute-force attacks have not let up in their 20th year on the internet, and only continue to grow in popularity as devices proliferate. A remote brute-force attack involves repeatedly guessing common usernames and passwords. This type of attack often targets an administrative console for a web application, a remote desktop session, or a listening service (like Secure Shell or Telnet). These services exist on nearly every type of device, from the largest assets in the world to millions of small embedded devices found everywhere. IoT endpoints in particular had many vulnerabilities in this category.

Hackers most frequently attacked Telnet and SSH with brute-force attacks. IoT-targeting botnets (such as Mirai and its clones) prefer to target these two protocols. However, as the graph below shows, any service employing default or weak credentials is at risk.

There are multiple solutions to help prevent brute-force attacks:

- Utilizing public/private keys for remote administration of servers
- Two-factor authentication for remote administration
- One-time-use factory-shipped passwords for embedded devices (IoT)
- Disabling remote access until enabled by the user with a custom password

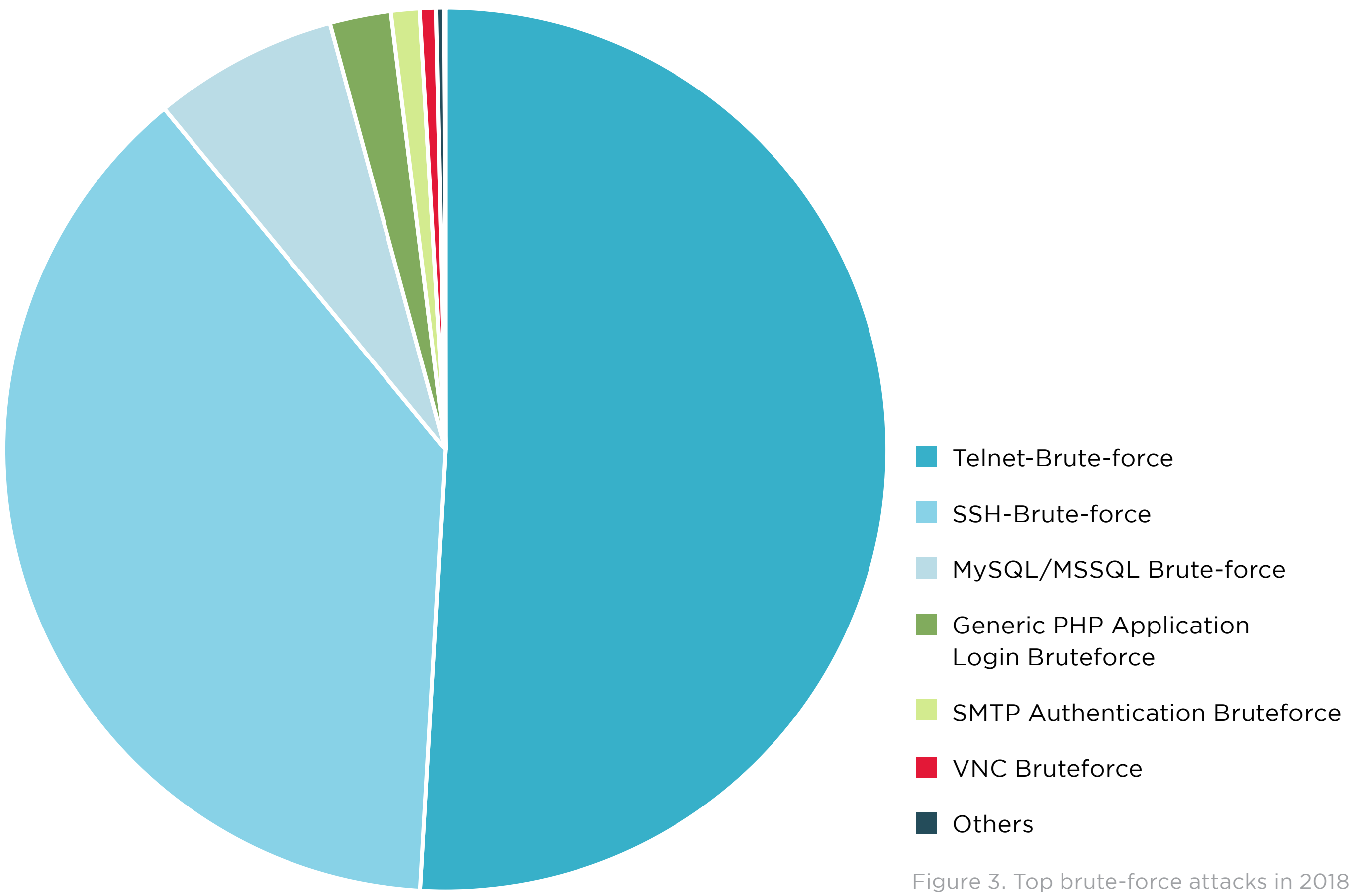


Figure 3. Top brute-force attacks in 2018

Another well-known attack that continues to proliferate is EternalBlue (CVE-2017-0144). The infamous WannaCry malware leveraged EternalBlue in May 2017. Despite EternalBlue's age, it continued to gain momentum in 2018. This vulnerability only impacts hosts running Windows 7 or previous editions. Bad actors heavily scanned for vulnerable systems throughout 2018; the number of scanning attempts for this vulnerability was three times greater in December 2018 than in January 2018. See the Ixia data in Figure 4.

Mirai and other botnets continue to scan for vulnerabilities that are more than 5 years old, such as Dahua DVRs and video cameras. Many victims do not even realize they are affected. Ixia began tracking Mirai-based bots soon after they started spreading. Ixia solutions identify the command and control anomalies, as well as the bots themselves, based on packet attributes.

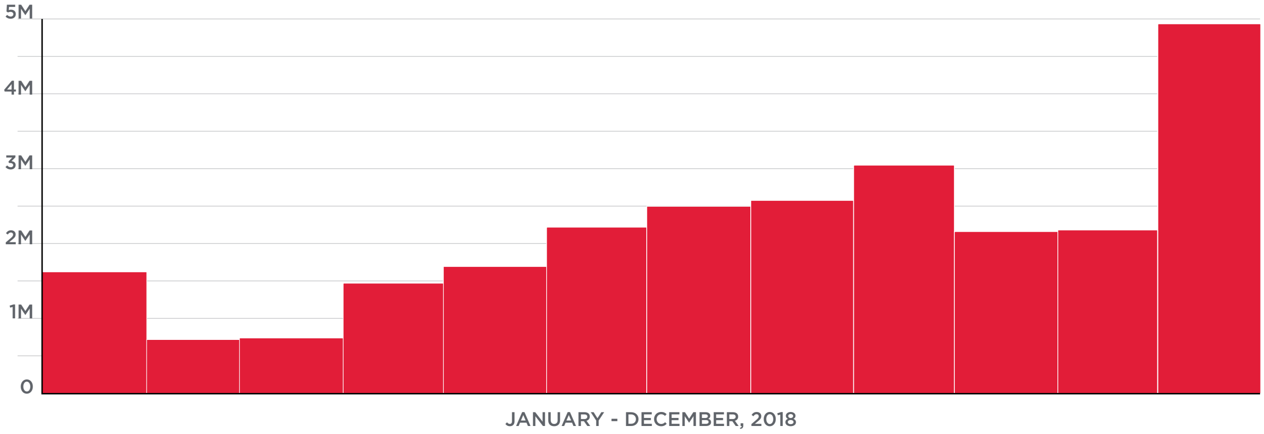
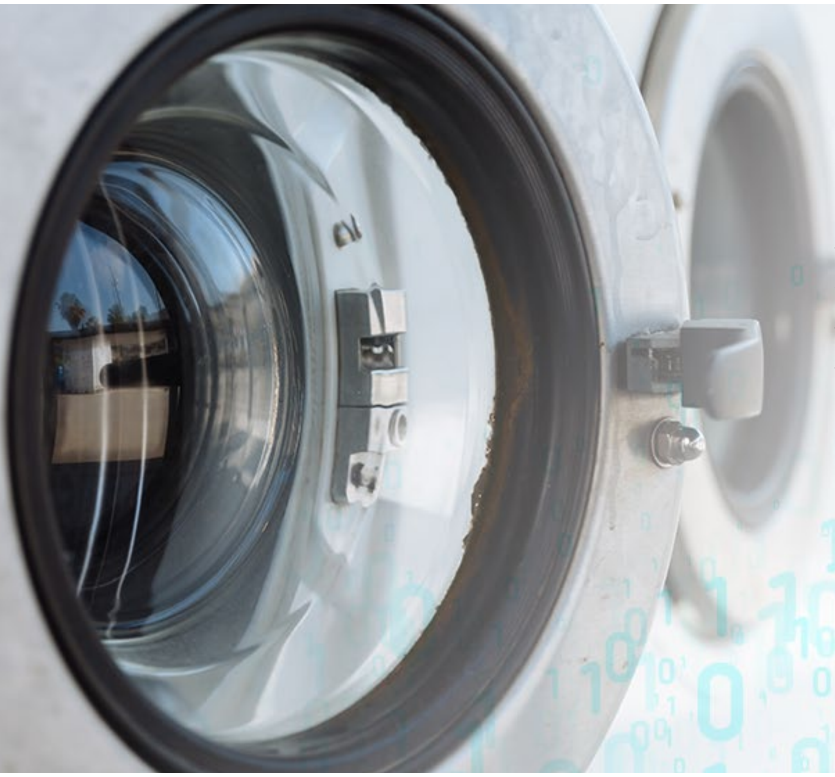


Figure 4. EternalBlue scanning attempts by bad actors in 2018



One victim was a laundromat company.

The botnet would compromise the company's internet-connected security cameras, adding them to the botnet. The cameras would livestream footage of whatever they pointed at. As the exploit continued, the traffic would overload system resources. Once this happened, the cameras would stop working. The owner would reboot the cameras, and they would return to factory defaults. The cameras would behave normally for a few days, and then the cycle would repeat. The owners were unaware that the equipment kept failing because of product security design defects. Instead, they assumed they had purchased a cheap product with poor reliability.

While a laundromat might seem innocuous, the key point is that the IoT device threat is real. These devices could be cameras, in-home routers, televisions, or millions of other things. Security patching requires ongoing investment from both the vendor and the device owner. If left unpatched, attackers will discover and exploit these design flaws.

Figure 5 shows one example of how hackers are still trying to exploit older vulnerabilities in Dahua DVRs. Equipment that should have been patched or removed from the internet remains in place without remediation.

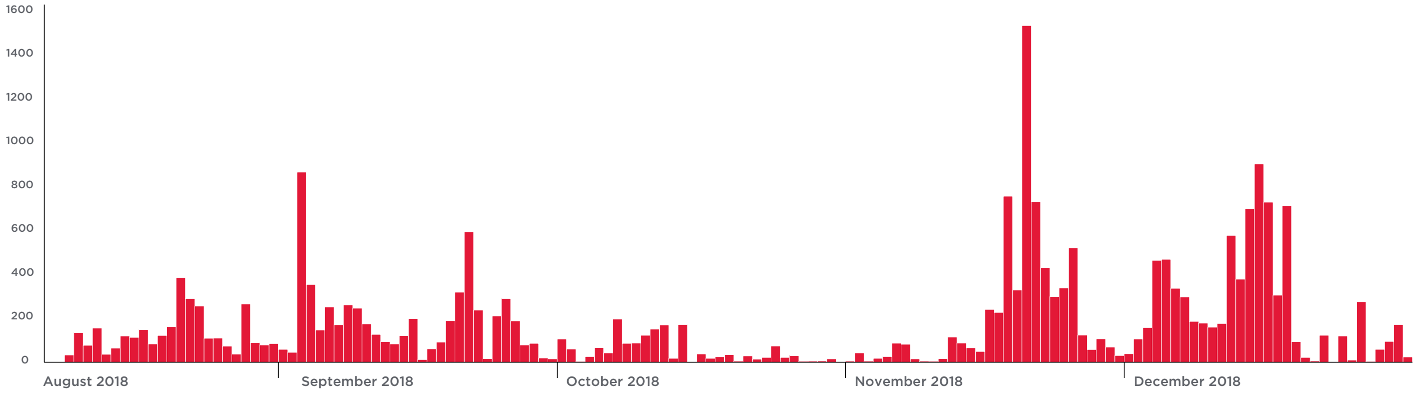


Figure 5. Attackers still target Dahua DVR (CVE-2013-6117) exploit from 2013

Additional research shows that many hackers are simply opportunists. They try to find as many vulnerable older systems as they can. One example is CVE-2009-4140, which demonstrates that opportunists will look through the archive of vulnerabilities to try to find exploitable systems running ancient software on the internet. Old equipment may still be in use or redeployed as a backup. Older software is less likely to receive patch updates or intrusion-detection and -prevention signatures for security threats, increasing risk for organizations that deploy it.

The CVE-2009-4140 vulnerability allows complete access to a system. Remote authenticated users can execute arbitrary code by uploading a file to the system. Activity targeting this old vulnerability for web applications reappeared in Ixia honeypots in 2018, as shown in Figure 6.

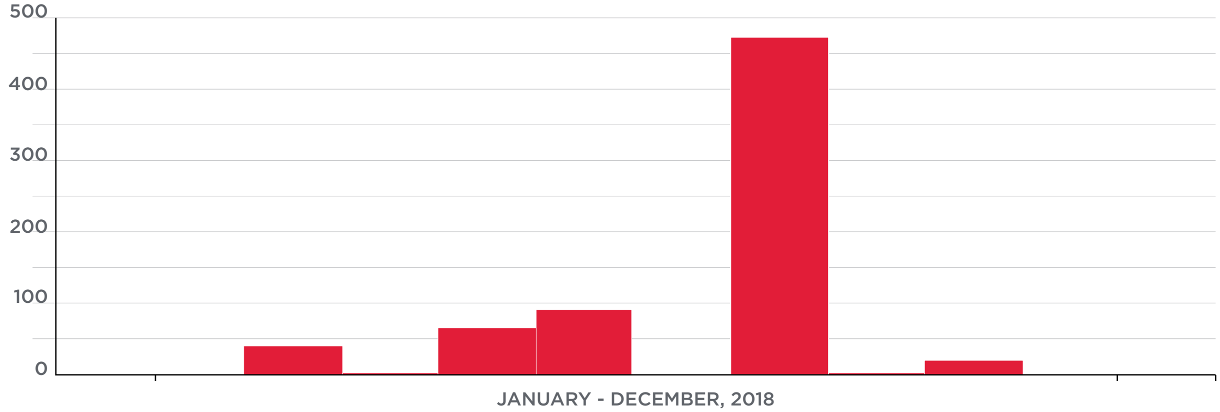
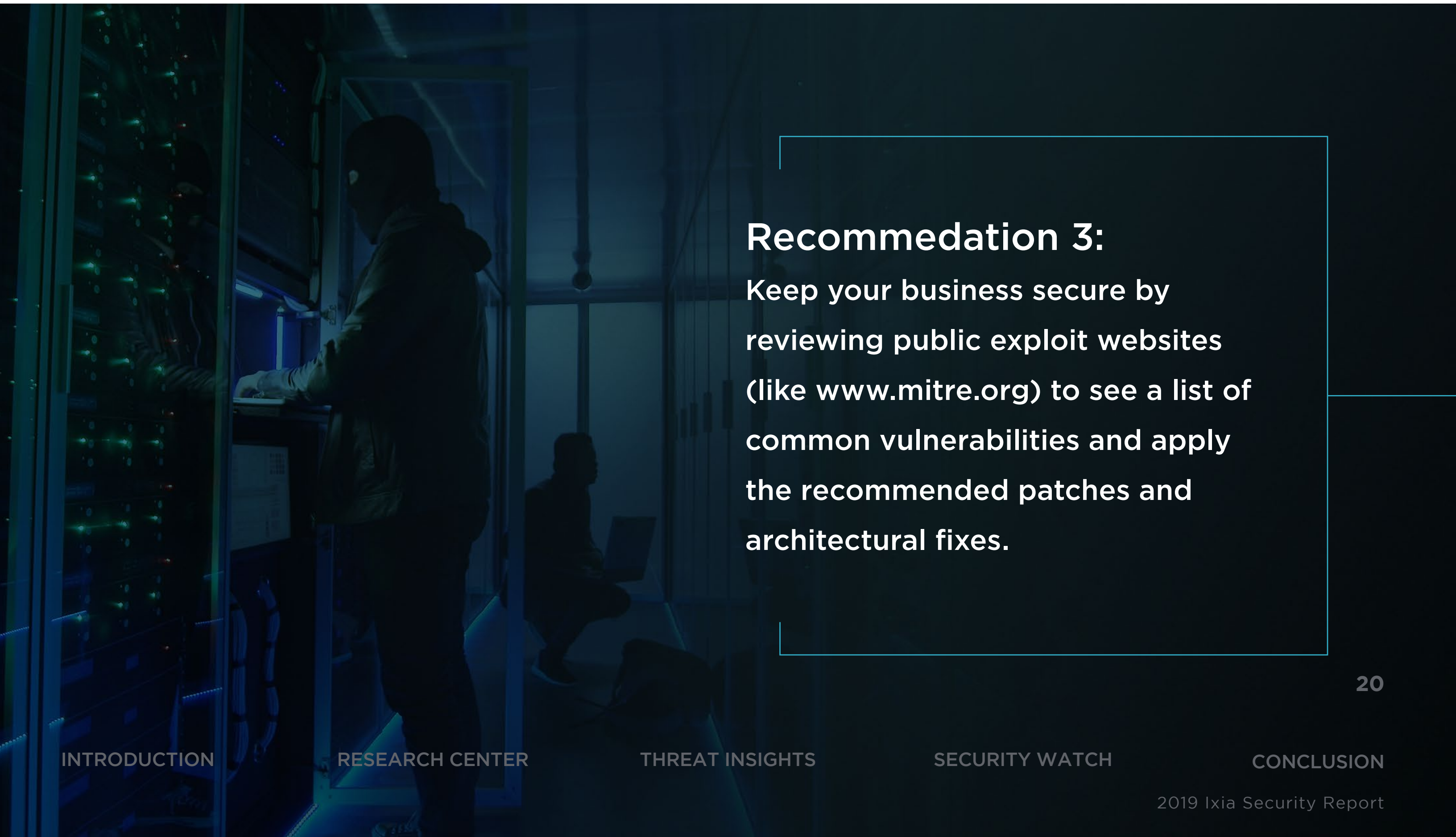
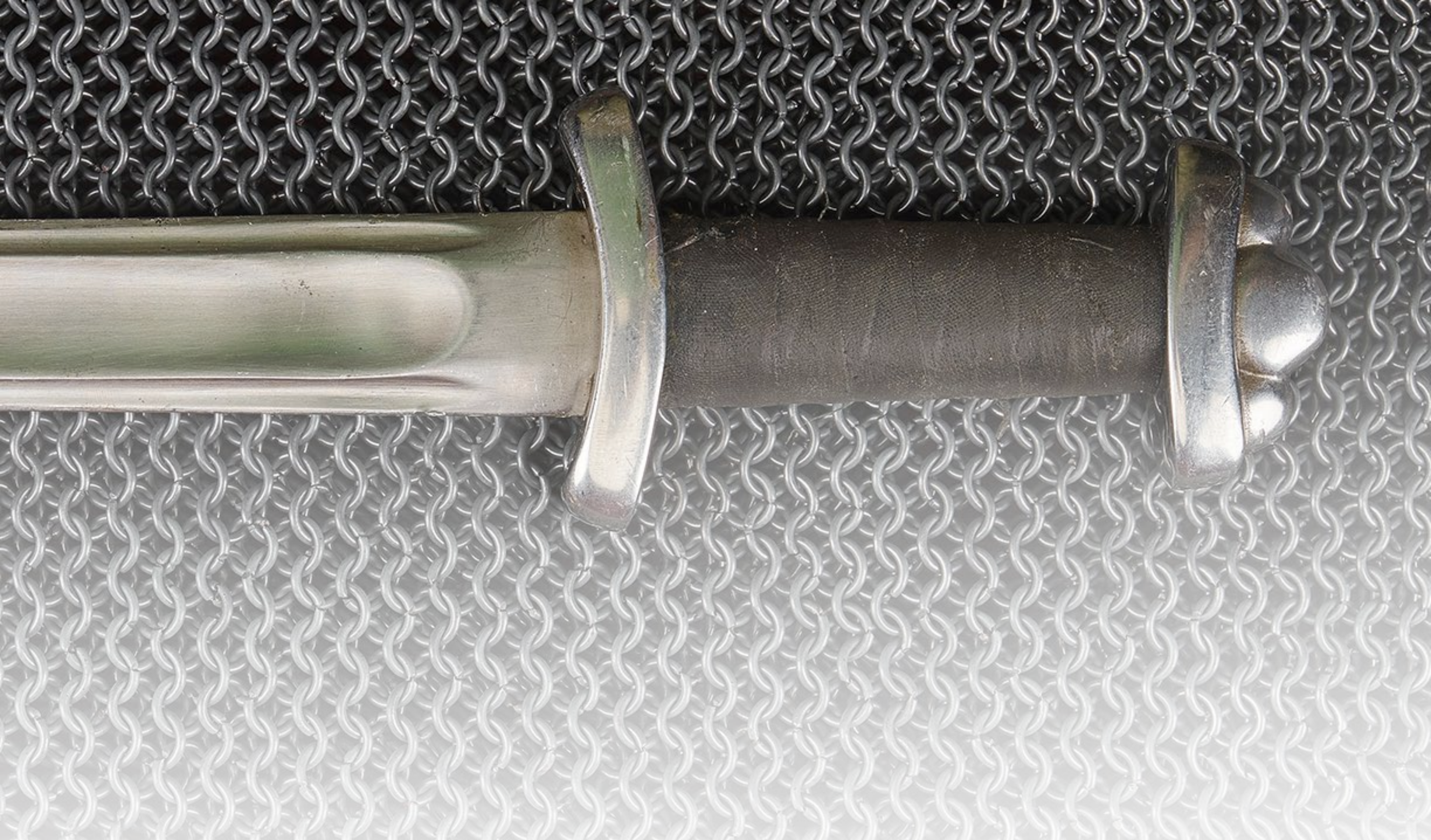


Figure 6. CVE-2009-4140 exploitation continues



Recommendation 3:

Keep your business secure by reviewing public exploit websites (like www.mitre.org) to see a list of common vulnerabilities and apply the recommended patches and architectural fixes.



4. Security Vulnerability Disclosures are a Double-edged Sword

Vulnerability reporting helps vendors and consumers identify security flaws. When security engineers find a zero-day vulnerability, security threat, or other exploit, sharing information quickly is a common practice, so that vendors can fix their code and IT teams can secure their networks. But vulnerability reporting also informs hackers, who often can move faster than vendors or enterprise IT. Ixia has observed more successful security attacks following the disclosure of new vulnerabilities.

Here are examples of exploits where hackers were able to move faster than vendors and IT teams:

- Mirai
- Drupalgeddon
- D-Link DSL-2750B remote code execution vulnerability

Mirai, the botnet that hit the internet in 2016, originally used brute force to target embedded devices listening on Telnet. Mirai source code was released to open source communities, spawning many copycat versions that use brute-force SSH attacks and incorporate multiple other embedded device vulnerabilities to increase the rate of compromise. Mirai derivatives remain high on the list of active botnets on the Internet and remain a persistent and evolving threat to embedded Linux systems. Figure 7 illustrates the ongoing risk from this attack.

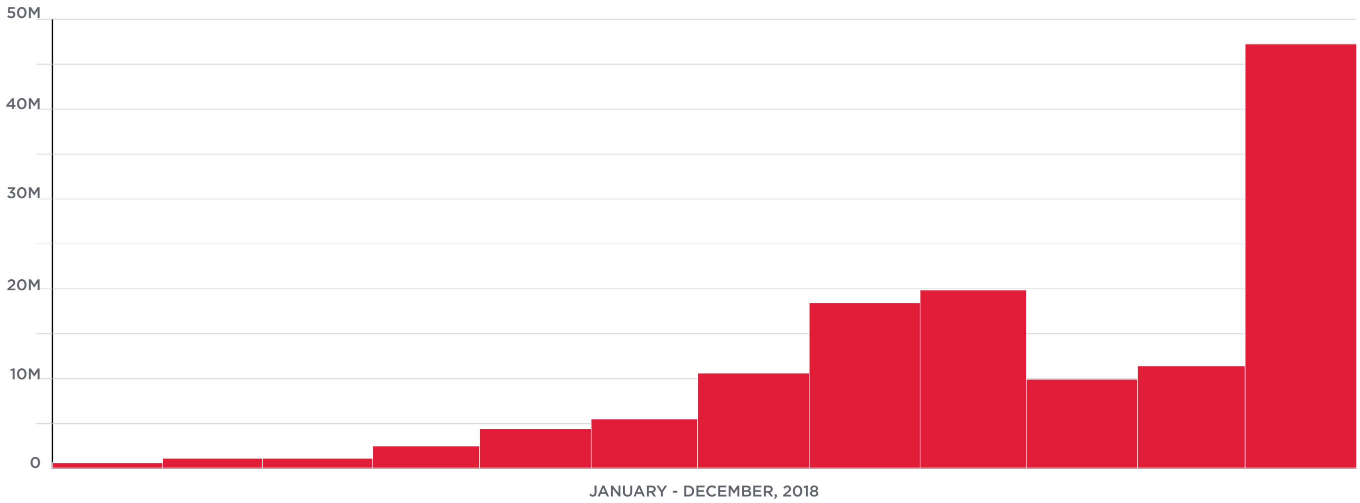


Figure 7. Mirai resurgence in late 2018

Drupalgeddon, originally referred to as CVE-2014-3704, is a SQL injection vulnerability that targets the Drupal web framework. Last year, researchers uncovered and responsibly disclosed similarly dangerous flaws that they dubbed Drupalgeddon 2 and 3. Drupalgeddon 2 (CVE-2018-7600) was responsibly disclosed. The researcher warned the development team, giving the team time to create and issue a patch before the exploit details became public. After private notification, the researcher released information necessary to exploit each vulnerability on April 12 and April 25, 2018, respectively. As shown in Figure 8, exploit attempts quickly followed.

Interest in these two vulnerabilities then waned, mainly because the fast patching process quickly reduced the number of available targets.

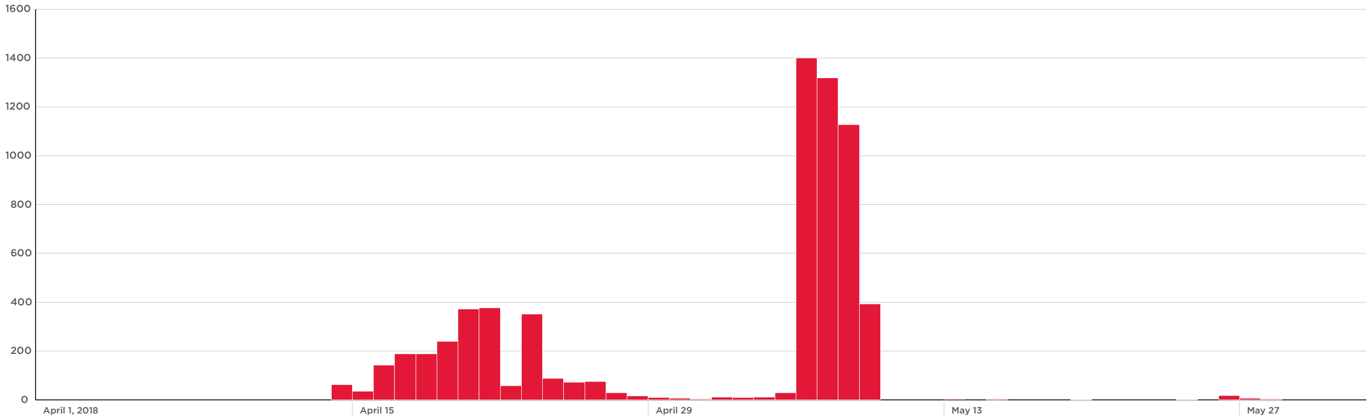


Figure 8. Drupalgeddon 2 and 3 attack waves start in April

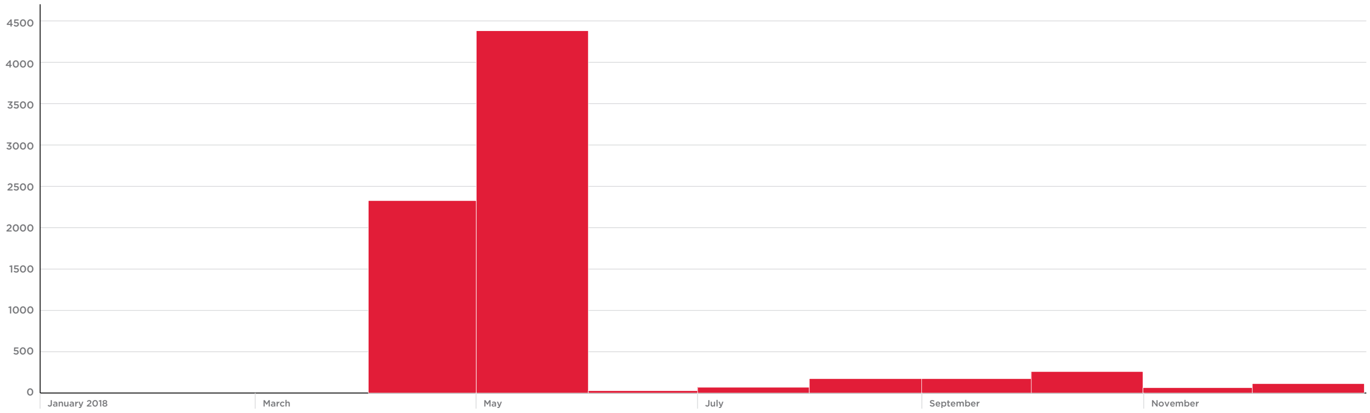


Figure 9. Drupalgeddon 2 and 3 attacks wane after May 2018

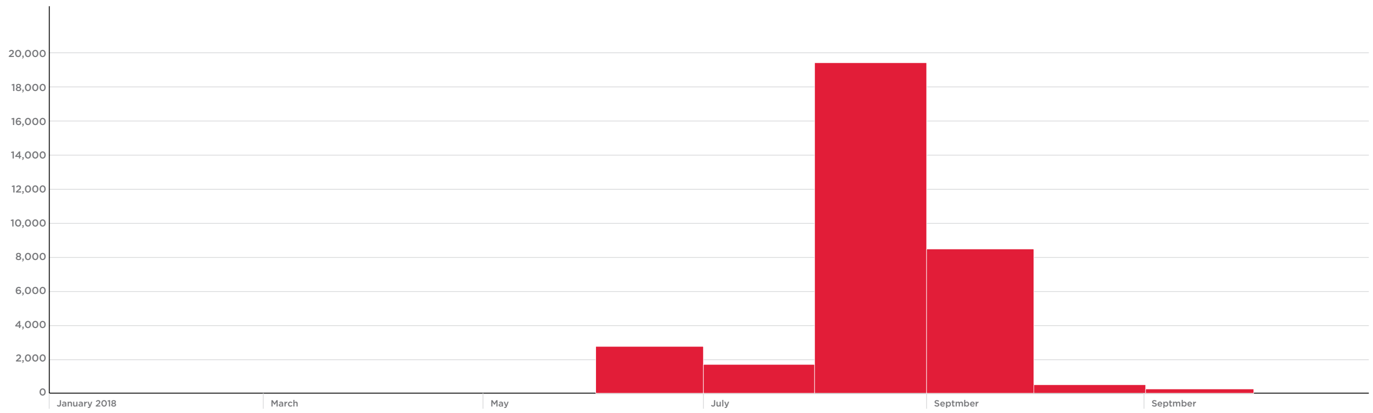
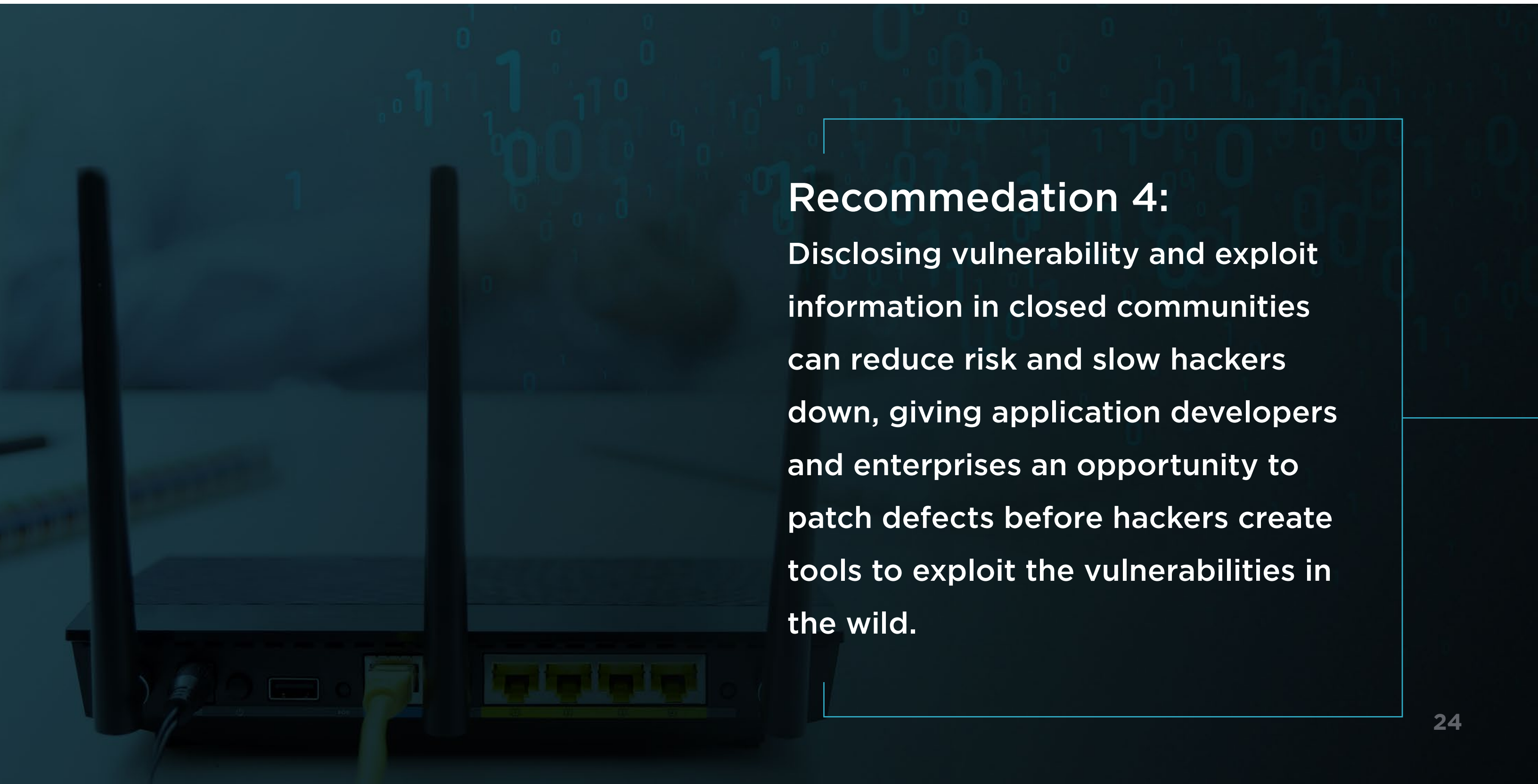


Figure 10. D-Link DSL-2750B exploit

On May 25, 2018, a new tool emerged that exploited a vulnerability in D-Link DSL-2750B routers. Attackers quickly seized the new tool and attempted to exploit the vulnerability. Interest peaked in August and September when newer versions of Mirai clones attempted to exploit this vulnerability.



Recommendation 4:

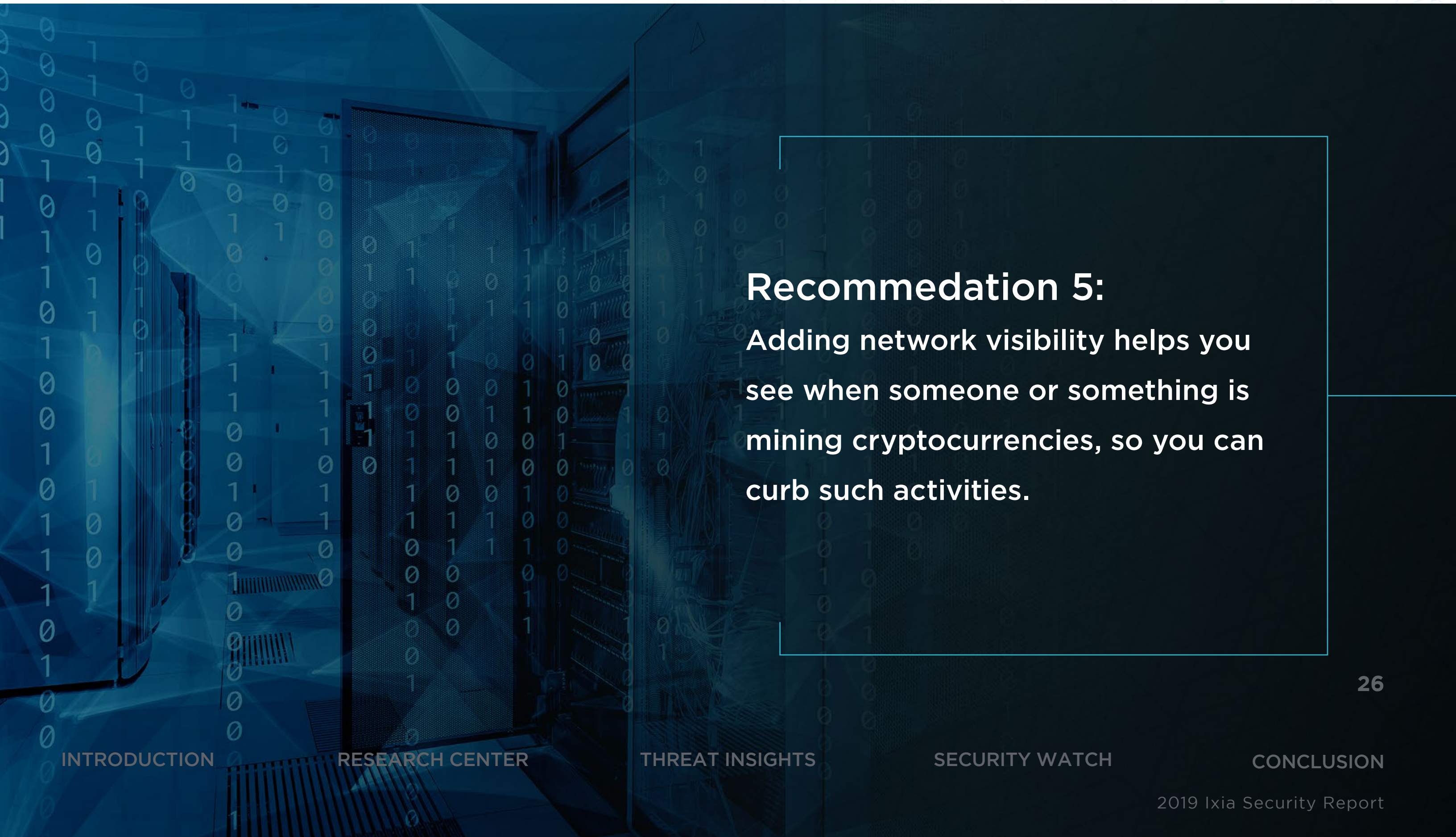
Disclosing vulnerability and exploit information in closed communities can reduce risk and slow hackers down, giving application developers and enterprises an opportunity to patch defects before hackers create tools to exploit the vulnerabilities in the wild.

5. Crypto-jacking Activity Reached New Peaks in 2018

Ixia predicted the rise of crypto-miners in its 2017 annual security report. Not only did this trend emerge, but hackers combined multiple classic attacks to deliver nearly autonomous malware, capable of spreading internally and building massive shadow networks dedicated to crypto mining. Ixia honeypots captured several new exploits that run an EternalBlue scan and, when successful, deposit a crypto miner onto the network.

The meteoric rise of cryptocurrency value in 2018 drove a new form of compute resource monetization. Classic malware tried to find something of value on a compromised system, often ransoming the data. With crypto-mining, the compromised system itself provides value through the mining of cryptocurrencies. It is easier for bad actors to mine for cryptocurrency than to ransom or steal something else of value. Detection poses little risk to the hacker using an anonymous cryptocurrency. This low-risk, high-reward environment means that ransomware is no longer the exploit of choice. Instead, many new exploits now focus on automating the installation and distribution of miner malware to as many hosts as possible.

Cloud misconfigurations caused many data breaches in 2018. In many cases, organizations stored personally identifiable information (PII) in the clear in Amazon S3 databases. Plain-text storage, combined with human errors that exposed the database to hackers, caused many costly data breaches in 2018. While human error causes some of these incidents, others clearly stem from a lack of understanding of security best practices. Cloud security teams could benefit from working more closely with their on-premises IT security teams, leveraging best practices learned from years of on-premises IT application deployments. Cloud technology works differently, but that is no excuse for breach of PII. Your choice of technology platform will not reduce the fine levied for breach of personally identifiable data.



Recommendation 5:

Adding network visibility helps you see when someone or something is mining cryptocurrencies, so you can curb such activities.

SECTION 04

SECURITY WATCH LIST FOR 2019

Based upon Ixia-collected data and historical activity, the Ixia ATI team predicts the following six trends for 2019:

- Abuse of low-value endpoints will escalate
- Brute-force attacks on public-facing systems and resources will increase
- Cloud architectures create complexity that increases attack surfaces
- Phishing will continue to evolve. As more companies begin using similar enterprise email systems (Office 365, G Suite), better phishes will help hackers get around defenses
- Multiphase attacks that use lateral movement and internal traffic will increase
- Crypto mining/cryptojacking attacks will increase

Trend 1:

Abuse of Low-value Endpoints will Escalate

Until basic security hygiene improves, hacks like Mirai and cryptojacking will continue unabated. With more devices connecting to the internet every day, the number of targets continues to increase — and so will the number of victims.

Trend 2:

Brute-force Attacks on Public-facing Systems and Resources Will Increase

This attack vector has existed for close to 20 years. While solutions exist to eliminate this attack vector, we continue to see the same mistakes made repeatedly by vendors and IT practitioners. It appears there will always be a server out there with the username “root” and the password “password” that a hacker can exploit. Individuals can prevent attacks on their systems by changing default credentials, but only adoption of two-factor and public/private key authentication will provide a permanent solution.

Brute-force exploits will also increase significantly for enterprises and carriers with the proliferation of IoT devices. Many forget, or do not understand, that these devices ship with default credentials. In addition, the devices are actively broadcasting — so they can connect to an internet router and relay data. Attackers can exploit this mechanism to connect to the IoT device and take it over.

Trend 3:

Cloud Architectures Create Complexity That Increases Attack Surfaces

On-premises architectures gave security personnel complete control of their equipment and architecture. Public cloud-based solutions give no control over server and network architecture. Attacks like Spectre (CVE-2017-5753) and CVE-2019-6260 are just the beginning of the new types of attacks aimed at cloud users and their data. The speed and dynamic capabilities of public clouds have unfortunately exposed a new attack vector: service misconfiguration. Misconfigured services provide an open gate that hackers and bad actors can walk through, often with disastrous results.

Trend 4:

Phishing Attacks Will Become More Focused During the Next Two Years

Enterprises invest thousands to train employees to recognize phishing attacks. In response, hackers create better phishes that are less obvious to victims, and more targeted. Growing Office 365 and Google G Suite adoption will help slow down phishing momentum. Both tools provide some phishing indicators. However, well planned attempts will get past these newer defenses. Hackers will relentlessly attack any system that provides a larger potential payoff.

Trend 5:

Multiphase Attacks That Use Lateral Movement and Internal Traffic Will Increase

Malware dwell times can exceed 100 days. Malware often goes undetected because command and control traffic is sporadic, hidden like a needle in a haystack and disguised to look like normal HTTPS traffic. Many organizations only monitor at ingress and egress points in their network. As attacks grow more sophisticated, we expect detection times will continue to grow longer. We also expect attackers to utilize more LAN-to-LAN attacks, hoping to avoid detection by abusing the trust of internal traffic. Micro-segmentation can increase visibility, helping detect and catch lateral movements.

Trend 6:

Crypto Mining and Cryptojacking Attacks will Increase

For decades, hackers sought to compromise systems, steal data, and more recently ransom computers. A shift has occurred, where new attacks target the systems themselves. Rather than stealing data at rest, attacker use compromised systems for crypto mining. Old unpatched vulnerabilities previously used for ransomware or DDoS networks are easily exploited to deliver crypto mining software. Advanced crypto miners do not depend on classic command and control architectures, making them harder to detect and prevent fluctuating cryptocurrency values may slow the growth of mining networks, but mining will continue to offer financially attractive incentives to hackers looking to make some quick money.

SECTION

05

CONCLUSION

In 2018, we observed important shifts in the threat landscape. We observed new malware variants, and new versions of well-known legacy exploits. We observed many security breaches due to misconfiguration errors, and we saw this trend extend further into cloud-hosted software and services. Cloud services offer nearly instant access to a wide variety of scalable platforms and services, but with that speed comes a rapidly expanding attack surface, and more opportunities for human error.

Network complexity continues to rise and attack complexity mirrors the network landscape. Some attacks die off, while others are reborn as new variants year to year. The ever-changing landscape requires vigilance and quick responses from your security team.

Our research also uncovered data that indicates that the following six items will pose the most threat to enterprises over the coming one to two years. We suggest that you review your security architecture for the following threats:

1. Abuse of low value endpoints will increase this year
2. Brute force attacks will increase on your public facing assets
3. Cloud networks are increasing complexity, which is increasing attack surfaces
4. Phishing attacks will become more focused over the next two years
5. Multiphase attacks that use lateral movements and internal traffic will increase
6. Crypto mining attacks will increase

IT teams can make many improvements to enhance their security architecture. We recommend that you implement these activities now:

- Perform a security patch analysis versus your security control protections
- Analyze your public cloud security architecture, and audit application access policies
- Review password security practices for your IT systems and equipment

Our research shows that basic security hygiene practices could prevent or minimize the impact of many breaches. Security teams that ignore these practices are more likely to suffer a breach.

Patch analysis may sound boring, but too often, a single engineer is responsible for patch maintenance of an application or piece of equipment. If that engineer leaves the company, responsibility for patch maintenance may fall through the cracks. Our data shows that in many cases, year-old unpatched vulnerabilities allowed exploits to happen.

If you have vulnerable systems that you cannot immediately patch, do you know whether your security controls will protect you?

Another basic hygiene practice is default password security. IT professionals should remove factory default or well-known passwords before devices are deployed. This mitigates nearly all brute-force attacks and exploits. Brute-force attacks continue to work, because IT continues to deploy equipment with default passwords.   Eliminating these passwords would eliminate this attack vector.

Cloud architectures continue to grow in popularity. However, security personnel are often not involved in all aspects of cloud implementations. Enterprises learned long ago that stateful inspection firewalls and logs were insufficient to protect against application level attacks, but many cloud providers offer these features as standard defenses.

Additional lines of defense are crucial to protect applications in the cloud.

As noted earlier, the number of data breach incidents rose in 2018, with more incidents attributed to misconfigured cloud applications and resources. Some common cloud security mistakes include failure to encrypt personally identifiable data, incorrect data access permissions, and unpatched code creating vulnerabilities in the application stack. Cloud technology works differently, but data breach laws and fines don’t discriminate. We here at Ixia, and the ATI team, understand these complexities and are here to help you safely navigate the ever evolving cyber world.

Ixia can help you secure your network, data, and applications. To learn how network packet brokers and taps can augment your security infrastructure to give you the visibility you need to act fast — ask for a demo, and we would be happy to show you what is possible.

Contact us at ixiacom.com

ixia
A Keysight Business

Find us at www.ixiacom.com

915-9331-01-4091 Rev A | © Keysight Technologies, 2019