ivanti

IT Security State of the Union: Three Short Security Essays

WHITE PAPER

Contents

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”) and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.Ivanti.com.

State of the Union on Security, Part I: The Rise of Nation-State Activities

Without question, hackers today can have a major impact on critical infrastructure worldwide. Hospitals, banking systems, power grids, and many other areas are regularly prone to and affected by cyber threats. The uptick is in no small part due to the widespread availability today of sophisticated attack tools.

As you may know, for example, the base architecture for 2017’s NotPetya attack used exploits that were developed by a nation-state entity—in this case, the U.S. National Security Agency (NSA). The tools and vulnerabilities that were being exploited were disclosed through the activities of a hacking group who got their hands on these NSA tools.

In this case, the attack that used nation-state tools was orchestrated by nation-state hackers as well. NotPetya masqueraded as ransomware but was in fact not motivated by money at all. Most ransomware campaigns provide a variety of mechanisms to allow for payment to occur because they want to make sure that the authorities can't shut them down and limit their ability to get a payout. Well, a lot of those characteristics were lightly implemented or near nonexistent in the NotPetya attack. The attackers also provided no means for those impacted to recover files even if they paid the ransom

What we really saw was ransomware used as a *social and economic disrupter* rather than a direct impact to try to get a payout—a new evolution in cyber-attacks. It was a deliberate, malicious act designed to destroy, not to extort—in this case, to destabilize a country. The NotPetya attack targeted Ukrainian infrastructure by compromising Ukrainian accounting and tax software from the financial tech company MeDoc and using that to launch the attack on those who would likely download that software—Ukrainian businesses.

It proved very successful, too, at destroying all records on targeted systems, rendering them unusable. Entire organizations in Ukraine found themselves unable to operate for days on end. NotPetya impacted hospitals—leading to canceled surgeries—and other major organizations like airlines, banks, the Chernobyl nuclear power plant, pharmaceutical company Merck, FedEx, and global shipping company Maersk, which was forced to shut down container terminals in ports from Los Angeles to Mumbai. It managed to take down multi-national companies whose internal networks were large enough that the infection could travel quite far from ground zero. It infected more than 2,000 organizations worldwide.

The question is, then: How do we as security and IT professionals strategize and make ourselves more effective at defending against this type of attack?

The Threat Landscape of Software Vulnerabilities

We have to prioritize risk.

To this day, for example, software vulnerabilities play a significant part in the overall threat landscape—the total attack surface that we're exposed to.

The Forrester Wave: Vulnerability Risk Management, Q1 2018 cites that 58 percent of enterprise organizations suffered a breach at least once in the past year. Now, not every breach among that 58 percent was headline-grabbing where millions of accounts were exposed. But the scary part of all of this is that more than half of the companies out there suffered at least one breach in the past year.

The good news is there’s a solid takeaway here. Of those breaches, 41 percent exploited a software vulnerability. One very significant breach during that time period—the Equifax breach that exposed the personal data (Social Security numbers, addresses, driver’s license numbers, credit card numbers, and more) of 147.9 million consumers—can be traced to software vulnerabilities in the Apache Struts web framework.

There were likely other stepping stones employed to get to that Apache web server and access sensitive data. But, again, software vulnerability was the way that the data was actually accessed and extracted. Notably, this was also a software vulnerability for which a patch existed.

Returning to our exploration of nation-state attacks, let’s look now at WannaCry. It was a nation state–developed software exploit and ransomware incident that affected more than 230,000 endpoints in over 150 countries worldwide in a short period of time.

As with NotPetya, attackers used the EternalBlue exploit, developed by the NSA, and leaked by the Shadow Brokers hacker group on April 14, 2017. EternalBlue exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol.

Microsoft issued a security bulletin that detailed the flaw and released a patch update. But, as with the Equifax breach and NotPetya (which struck after WannaCry), despite the availability of a patch, attackers were later able to launch the WannaCry attack using the EternalBlue exploit.

Another tool employed in the attack was DoublePulsar, a backdoor utility also developed by the NSA and leaked by the Shadow Brokers that allowed the WannaCry infections to get into environments where there wasn't a public-facing SMB port. DoublePulsar was previously installed on tens of thousands of systems globally, leaving control of those systems in the attackers' hands and enabling them to use DoublePulsar to easily execute the WannaCry ransomware. Because DoublePulsar runs in kernel mode, it grants hackers a high level of control over the compromised computer system.

So, a combination of SMB protocols being public facing and exposed, plus DoublePulsar being a backdoor that allowed exploit, enabled WannaCry to become very successful. And once inside many of these environments—because the update had not been rolled out—the exploit spread very quickly.

As WannaCry and NotPetya each show, comprehensive, timely patch management must be a priority in any organization today—all the more so given the havoc nation states are now wreaking.

A Sophisticated, Layered Approach to Attack Requires a Sophisticated, Layered Approach to Defense

Once inside an environment, additional capabilities were used to spread NotPetya further.

A tool called Mimikatz was employed to find admin credentials. Those credentials were then utilized to employ other existing tools like PsExec and WMIC, and to access other systems remotely using those tools and compromised credentials, allowing the exploit to spread even to where the SMB exploit was not available.

Finally, in the second wave of attacks, phishing was another method NotPetya used to introduce malware onto a machine. Did you know that phishing is actually the number one threat vector for ransomware and other malware?

All of this is to say that this was a very sophisticated, layered approach to attack—requiring an equally sophisticated layered approach to defense. As we've seen, properly executed patch management is critical, but so is privilege management to reduce the spread of malware through an organization. And, so is security awareness training for employees to reduce the effectiveness of phishing campaigns.

In our final essay, we'll take a closer look at the risks you should prioritize and the security controls you should have in place to mitigate them..

State of the Union on Security, Part II: SamSam Attacks and the Need to Prioritize Risks

The SamSam Ransomware Family

SamSam is another fairly recent evolution in ransomware. It emerged onto the market only a couple years ago and has quickly become very effective.

The SamSam ransomware family—and the threat group by the same name behind the scenes—is definitely focused in its targets. These hackers are not out for mass-scale ransomware-as-a-service for a random payout. They single out their targets and are actively involved during an attack. They'll break into and survey a victim's network before deploying and running any ransomware. They also change their tactics during the attacks. If one approach doesn't seem to be working, they'll shift gears and employ other approaches to be able to maximize their effectiveness. And if security software stops the malware from running, they'll look for ways to disable that software.

Edge Servers or Infecting Servers

This threat group has a history of infecting internet-facing servers. In a few cases that have been detected so far, the attacks focused on JBoss, the Red Hat–based Java development environment, and open Remote Desktop Protocol (RDP) ports that are often public facing in healthcare companies where they let partners or clients into their RDP service.

Cyber-criminals will brute-force attack RDP, or they'll take advantage of a public-facing software exploit on a platform like JBoss. Traditionally, as you know, RDP sessions are often configured with weak passwords, so strengthening your password policies is one way to help mitigate how these guys are getting in.

But once they do get in, the level of sophistication is alarming. They're using tools like Mimikatz, PsExec, and WMIC to find admin credentials and access other systems. They've got a list of about 10 to 12 different tools either malicious in nature or existing in your environment that just need a certain level of privilege to use in the different ways.

And, as noted earlier, it’s not just automated software trying to exploit things based on certain algorithms. They will be active in an environment, change up tactics, and develop new ways around obstacles they encounter.

Not Looking for Individual System Payouts

What’s more, these guys aren’t looking to get individual system payouts. They’ll usually offer a per-machine-level payout, but they quickly get up into a site-wide decryption option, typically hitting around $50,000.

What they're really aiming for is six to eight attacks per month with payouts of $50,000 each. Since they surfaced a few years ago, they've made about $6 million in bitcoin payouts and are averaging around $330,000 a month in successful ransoms paid out. Again, they'll get into an environment and they'll sneak around and distribute themselves very effectively across an environment before they actually launch the attack.

One event that happened not too long ago was an attack on a healthcare company. In the first 15 minutes before the attack was contained, ransomware infected and executed on nearly 9,000 systems. This is how they operate.

Attack on the City of Atlanta

Now, this particular SamSam ransomware family is what hit five departments in the City of Atlanta in March of 2018. It was a very disruptive attack and relegated city officials to sharing old laptops that were pulled out of closets to try to get their work done.

Almost 30 percent of the systems that were impacted were vital, including court systems and police. The city department lost all but six of its computers and 10 years’ worth of documents. The police lost their dash cam recordings. Around 8,000 city employees weren’t able to use their PCs for several days.

The cost to the City of Atlanta was roughly $17 million and rising. This number factors in the hard costs of cleaning up that attack—around $2.6 million—which included bringing in external security services and online Emergency Services to replace disrupted services like police and 911, respectively.

But, again, looking beyond cost, more than a third of the city’s necessary services were knocked offline or partially disabled, and almost 30 percent of those were vital.

Similarly, while NotPetya cost companies like FedEx, Maersk, and Merck an estimated $200 to 300$ million each, it’s vital to remember that surgeries were canceled, the Chernobyl nuclear plant was targeted, and more. In addition to costs due to damaged or lost data, business disruption and lost productivity, forensic investigations, restoration of operations, stock prices, and possible fines, the potential loss of life and other public safety concerns must be heavily weighed.

How Do We Start Prioritizing Risks?

How can security and IT pros protect their organizations from these kinds of sophisticated attacks designed to have such a critical impact?

You must prioritize risk. Obviously, we can't protect against every potential exploit; there is no 100-percent security. So, how do we focus on the right things to maximize our effectiveness?

Known Vulnerabilities

First, known vulnerabilities are still *the root cause* of a lot of security breaches. **Gartner predicts** that 99 percent of the vulnerabilities exploited by the end of 2020 will continue to be the ones known by security and IT professionals at the time of the incident. Zero days happen, but they're not extremely common occurrences. Hackers are relying on security-penetration skills. They're developing the same skill sets as your own security teams and penetration testers. Their luxury is the fact that they can move faster than we can.

People: Your Weakest Link

In connection with these known vulnerabilities, it's *people* that will still be the No. 1 vector for attack. People are the weakest link in your environment.

According to the *Verizon 2017 Data Breach Investigations Report* (DBIR), 90-plus percent of security incidents and breaches involve some level of phishing attempt. It's still the number one threat vector for ransomware and other malware. While more people are being educated, and fewer and fewer are clicking on things without first thinking, four percent of the recipients of any phishing campaign will still click.

Similarly, in 2018 the DBIR Risk team found that email continues to be the most common vector for breaches—walking away with a staggering 96 percent of the blame. And 49 percent of malware gets installed via email!

All it takes is one person and one link or attachment. Given that, is it any wonder phishing plays such a prominent role in attacks? In fact, there is evidence phishing was used in a second wave of NotPetya attacks: a user logged in as an admin or domain admin could be tricked into running a booby-trapped email attachment that installed and ran the malware with high privileges.

And right there is yet another piece of the people equation: admin privileges. As we discussed in part I, they can be hijacked to help modern cyber attacks spread through an organization.

State of the Union on Security Part III: The Framework of CIS Critical Security Controls

CIS Controls—A Proven Security Framework

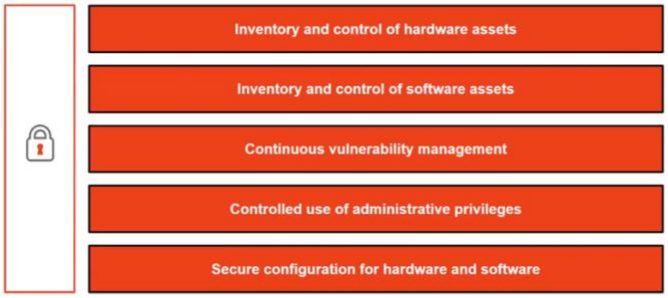
There's a reason we're examining the major attack vectors for modern cyber attacks in these essays. We have a goal of helping you direct potentially scarce resources to actions with an immediate and high-value payoff.

One of the ways we help customers prioritize risk is through adherence to the Center for Internet Security (CIS) Critical Security Controls framework. The CIS Controls are recognized as best practices for securing IT systems and data against the most pervasive attacks. Derived from actual experiences at the U.S. National Security Agency (NSA), the CIS Controls both support and reflect many of the other leading sources of cybersecurity guidance, including the Australian Signals Directorate (ASD), the National Institute for Standards and Technology (NIST), the National Cyber Security Centre (NCSC), and more.

The CIS framework consists of 20 security controls, and research and case studies from the CIS show that the top 5 controls are an effective defense against the most common cyber attacks, which amount to about 85 percent of the cyber threats we face today. Being able to focus on and eliminate the majority of that security exposure by applying a small subset of the overall framework makes you more effective. Again, this is about *prioritizing effectiveness*.

Much of what we need to do in securing our environments is evaluating things based on an 80/20 rule. How do you gain 80 percent of the value with 20 percent of the effort? You can actually realize upwards of 85 percent effectiveness in the security program by implementing the first five of the 20 controls. So, 25 percent of the work, 85 percent of the benefit. That's a pretty good payout for prioritizing your effectiveness.

So, what are those five critical security controls?


Inventory and control of hardware assets
Inventory and control of software assets
Continuous vulnerability management
Controlled use of administrative privileges
Secure configuration for hardware and software

Inventory and Control of Hardware *and* Software Assets

We'll start with the first two critical security controls. Without a complete picture of the organization's assets, you can't protect or defend against all that's in your environment. Are all systems running business critical applications reducing admin privileges? Are all kiosks and other systems exposed to the public locked down from an application and device control standpoint? Similarly, if you know you've got devices running on an older operating system or running on hardware that will not receive firmware updates to defend against hardware vulnerabilities like Meltdown and Spectre, you can start to identify what's exposed to older vulnerabilities and replace them.

As alluded to above, CIS Critical Security Control 2 is where you bring in application whitelisting. Regardless of how or where a user accesses their desktop, it's essential they receive only the authorized apps they need to be productive, and that they can't introduce unauthorized apps that could reduce desktop stability, impact security, breach licensing compliance, lead to user downtime, and increase desktop management costs.

Continuous Vulnerability Management

The third of the five controls entails assessing and taking action continuously on known vulnerabilities in your environment. So, for this one to be effective, you will have already identified the software in your environment. By the same token, for the second control to be effective, you will have established a good inventory of hardware in your environment. So, the controls here are prioritized in a way where each of them becomes more effective because the first one was done.

To assess and manage vulnerabilities continuously, we're really talking two different sets of technologies here. You have your security team and your vulnerability management software—your Qualys, Nessus, Tenable, Rapid7, whichever vulnerability vendor you're using—and then you've got your patch management solution from Ivanti, Microsoft, or another vendor.

These two groups and sets of capabilities need to work together to close those vulnerability gaps. Again, software vulnerabilities make up the largest part of the attack surface. Limiting how much of that surface is exposed helps close and lock the doors and windows.

Controlled Use of Administrative Privileges

Concerning some of the attacks we discussed before, many times a software vulnerability is exploited by attackers first getting on one system and then launching untrusted tools that shouldn't belong in the environment. And with those tools, they will compromise valid administrative credentials in the environment.

By using a valid credential from your environment and readily available tools that you yourself utilize, attackers can use capabilities and methods that are harder to detect. How do you filter through and scrutinize behavioral patterns when it's a user that you've created and it's the tools that you've given access to?

Gone are the days when we could literally lock down the user experience and call it a day. There are still companies that can enforce a policy of total lockdown of user permissions, but generally users require some ability that inevitably requires us to grant them administrative privileges on their system. Microsoft provides just two levels of control: user or a full admin. There's some variation in between, but not enough to make it a good experience for the user or administrator.

By removing full admin rights from users and providing them with elevated privileges for just the tasks they need for their job, you can simplify endpoint security, reduce support calls, and lower TCO. Take a full admin back down to a regular user, and provide escalation of privileges where and when needed, from access to install applications, install a printer, use PowerShell, or whatever the user may need, but nothing more than what user should have.

Or you could take that full administrator and strip away the things they should not have access to. Take PowerShell away, for example, or access to other specific capabilities. Limit administrative privilege to specific consoles, applications, services, and commands, reducing the risk of admins introducing malware, halting essential services, or affecting performance of mission-critical services.

Secure Configuration for Hardware and Software

The default configurations for operating systems and apps are geared to ease-of-deployment and ease-of-use – not security. At the end of the day, then, with CIS control 5 what you are looking to do is to maintain a set of minimum standards for your configs.

You can pore through the checklists to give you ideas, but let's tie this to what we've discussed in these essays. For example, a weak RDP password is like a server room door that's propped open, inviting any passing snooper to look inside. Once hackers have your RDP password, they'll log on and create new administrative accounts. That gives them backup accounts they can use to sneak back in later and perhaps upload and deploy devastating ransomware.

In addition to timely patching that addresses vulnerabilities like these, to help stave off attacks like SamSam you can turn off RDP if you don't need it. You can also set a lockout policy to limit password guessing attacks.

After WannaCry hit, it was also recommended that IT disable the SMB v1 service. In general, the fifth control is about making sure you've got good firewall rules and password complexity. It's also about locking down vulnerable cipher suites, protocols, and applications running in your environment with hardened configurations. This extends to your IIS servers, SQL servers, etc.

Again, with these top 5 controls working together, you can mitigate or eliminate 85 percent of the threat right there.

Staying Vigilant

It's critical for IT security professionals to stay informed about threats, vulnerabilities, and trends in the industry. Ivanti is committed to helping organizations achieve this through the following resources:

- **Weekly security blog updates** – Our researchers publish a post every Friday in addition to urgent updates in the event of a widespread malware attack. Click here or visit us at Ivanti.com/blog.
- **Patch Tuesday webinar series** – Join us LIVE every month as we break down updates, threats, and more in our award-winning Patch Tuesday webinar series.
- **IT security resources** – Let us help you increase your organization's security posture. Get insights from Ivanti experts, our customers, and industry analysts like Gartner and Forrester. Browse our re-designed security site for content you can use!

Learn More

ivanti.com

☎ **1 800 982 2130**

✉ **sales@ivanti.com**