NTT Security

GTIC Monthly Threat Report

October 2018

Contents

Hacking the U.S. Elections

Lead Analyst: Jon Heimerl

Are voting machines hackable?

Technically, they are, but how badly seems to be based on a high amount of opinion. Based on everything we know, some devices have shown to be vulnerable to hacking via Wi-Fi, some are vulnerable via an active USB port, and others if the attacker has physical access to the device. Machines use different technologies, and are generally physically isolated from the internet, so a single attack which would affect a wide range of many machines remotely may very well be impractical.

One of the catches is that those voting machines are built using components from a variety of sources, including sources which, in the past, have been alleged to insert their own malicious chips into motherboards destined for overseas markets. Realistically, we probably need to worry more about that supply chain than we need worry about voting machines being hacked on a global scale.

Another catch is that even if the voting machine is well architected and is a secure device, if an administrator does not continue good security hygiene, there can still be challenges to face. As an example, what if an authorized systems administrator installs remote access software the night before an election so he could work from home? Probably not a problem, but it definitely opened up remote access, and potentially other vulnerabilities, which would not have otherwise been there.

But the problem is not “hacking a machine” as much as it is “hacking a sufficient number of voting machines that someone could affect enough votes to sway the results of an election without making it obvious.” If say, a state uses 2000 voting machines, and the bad guys want candidate A to beat candidate B, they can’t just change all the votes on all machines to candidate A. They can’t just change all the votes in a single district. The results could not possibly be a 100% sweep in a key area. To be less than obvious, this would have to be many small changes over many devices. This “impact of volume” is what makes machine tampering more difficult.

Are counts vulnerable?

State websites which gather and report election results are probably more vulnerable. At DefCon 2018, it took an 11-year old girl 10 minutes to compromise the first simulated state site. Most sites tested were broken in less than 15 minutes. If an 11-year-old can make state election results report that Kim Jong-un won that state’s election with a quadrillion votes, that sounds problematic.

That bad news is that a significant amount of this information runs through a smaller number of systems within each state than the actual number of voting machines. So, an attacker would find it much easier to attack a single state site with a single state database to edit just enough votes to change election results. Realistically, this is a much bigger area of risk than “hacking machines.”

The good part is that local machines keep audits and paper trails to show what votes were originally cast, right? So, if candidate A surprisingly achieves a victory over candidate B, we can go back and look at the original voting results from the machines and verify the votes cast were accurately represented in the votes counted.

The catch is that there are as many as 14 states which have questionable audit trails, so authenticity of those votes cannot be validated with good confidence. (Auditable voting results are in flux in Louisiana, Georgia, South Carolina, New Jersey, Pennsylvania, Texas, Kansas, Florida, Tennessee, Arkansas, Indiana, Kentucky and Mississippi).

That said, based on what we know, there are very few incidents of confirmed attacks against election websites which would enable access to such voting results. That does not mean it is not happening, but if it was happening on a wide scale, we would most likely be hearing about more such incidents.

Voter registration details

After the 2016 federal elections, the Department of Homeland Security disclosed that foreign actors had targeted voter registration information in 21 states[1].

Most of these were sites which were targeted and included no site compromise. Still, some attacks over the past few years have potentially led to the release of information about registered voters, including name, address, date of birth, gender, driver's license number, partial Social Security Numbers, elections in which you voted (though not your actual votes), phone number, and email address. In many states, most of this information is a matter of public record and can be found with no hack whatsoever.

So, if it's public information, what is the value?

Social media campaigns

The value is identifying people to target in social media and social engineering campaigns. USA Today[2] identified 3,517 ads bought by Russian sources before and after the 2016 presidential election in the United States. The ads were dominated by divisive subjects, designed to increase hostilities between liberals and conservatives. This included messages designed to exaggerate issues and spread disinformation, increasing or suppressing voter turnout, depending on the goal of that particular messaging. Most of the known activity is from Russia, China, and Iran, and some of it is designed to soften the image of each country in the eyes of the voting citizens. Facebook[3], Twitter, and other online social media platforms have removed significant numbers of users who have continued to be active in such campaigns, so these are not isolated, limited incidents, but long-term, continued campaigns.

For a simple example, let's say you feel strongly that left-handed people are being unfairly discriminated against. If someone wants you to vote for candidate A over candidate B, they might send you targeted emails or ads, or social media posts which either says or suggests that candidate A is left-handed, and that candidate B has in the past made derogatory comments about "wrong-handers." Might that help increase the chances you will vote for candidate A? Or at least decrease the chances you will vote for candidate B? The statements don't even have to be true – how many of us go verify every claim we see in political ads?

[1] https://www.nytimes.com/2017/09/22/us/politics/us-tells-21-states-that-hackers-targeted-their-voting-systems.html
[2] https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/
[3] https://www.cbsnews.com/news/how-to-hack-the-midterm-election-with-social-media/

A campaign like this might not help you decide for candidate A, but it also might. Now, what happens if the attacker repeats this tactic 200,000 times, or 2 million times, or 60 million times (about half the voters in the United States)? If only 10% of victims respond the way the attacker wants, that is potentially a shift of 20,000, 200,000, or 6 million votes.

It should not be news that countries[4] other than the United States are being subjected to such tactics. Finland, Sweden, Denmark, Netherlands, United Kingdom, Germany, Spain, Italy, and France have all been targeted with such social media campaigns over the past few years, with varying degrees of success. Some of these campaigns, such as Russian initiatives against President Macron in France, are known to have been accompanied by hostile activity from APT28, the hacking group previously linked to the Russian government. As part of Russia's pro-Brexit campaign, Russia used nearly 150,000 social media bots to help spread misinformation. The United Kingdom leaving the EU makes for a weaker EU – clearly an outcome desired by Russia. How would a shift of 10 percent of voters have affected results of an international issue like Brexit (which passed by less than four percent) for instance?

What can we do about it?

Standards associated with voting machines and the reporting/management of voting data are evolving. The United States Election Assistance Commission released updated voluntary standards in September 2016[5], but some states follow federal initiatives, and some states follow their own initiatives. The result is that there is currently no universal standard on how to protect voting machines and the entire voting process.

The best guidelines are to enforce standards of good practice in the design of the entire voting system, including security controls as basic requirements. Fundamental security controls such as physical isolation, tamper-proof construction, an active patch management program, and robust security monitoring and auditing. These controls cannot simply be implemented on voting machines, but must be integral to any supporting system in every state, as well as at the national level.

But technical controls are only part of the solution. The influence dictated by aggressive social media campaigns has had national and international impacts. Social media sites have made progress cracking down on fake accounts used only for such campaigns, but the process must rely on the personal discipline of an informed public.

In an era in which information is power, and social media is the greatest path to that information for a significant number of users in modern countries, effective control and manipulation of that social media may very well have a bigger impact on our elections than the limited hacking we have so far observed, and if it can be done subtly, we may not even realize we are being had.

[4] https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf
[5] https://www.eac.gov/assets/1/28/VVSG.1.1.VOL.2.FINAL.pdf

Cryptojacking on the rise – now featuring EternalBlue

Lead Analyst: Danika Blessman

We've written quite a bit in the past on the upward trend of cybercriminals implementing cryptojacking malware[6] versus ransomware for financial gain.

Until recently, reporting has been geared more toward the threat to home users or single-system targets. The threat is now growing on enterprise networks, with cryptojacking malware getting increasingly difficult to detect.

Security industry leaders, including NTT Security, provide insight into this threat in a recently released Cyber Threat Alliance (CTA) white paper[7]. Of note, CTA members have seen miner detections increase nearly 460 percent from 2017 through 2018, and there's no sign the rate of infection is slowing. Unsurprisingly, cryptojackers often infiltrate a system or network through social engineering or vulnerabilities in the targeted organization's defensive perimeter.

One of the newest worrisome trends is that WannaMine cryptojacking malware is leveraging the leaked NSA tool called EternalBlue. EternalBlue tool has the capability to remotely access any computer running the Windows operating system, regardless of the system's location. This capability can enable additional malware to spread more quickly across a network. The clincher? These are *unpatched* instances; neither WannaMine nor EternalBlue exploits are new, but attackers are still successfully taking advantage of unpatched server message block (SMB) services.

As we've mentioned in previous reports, cryptomining malware, while not "malicious" in and of itself, may indicate that there are bigger problems on your network. You've already been breached and are likely vulnerable to other types of malware, possibly already present in your network. Additionally, 'simple' cryptojacking attacks are becoming more sophisticated, as the malware can monitor CPU usage, automatically pausing operations when the processing power goes lower than a designated threshold. This makes it even more difficult to detect this malware's presence, allowing the attacker potentially indefinite persistence to the victim system or network, along with greater financial gains.

Cybercriminals are essentially exploiting bad practices. Patching is the best way to defend against these known threats. It is also essential to train end-users against phishing emails and ingrain good security hygiene habits using best practices. In addition, look to the CTA's approach to not only protect and train end-users, but to disrupt cybercriminals and elevate an organization's overall security posture. Part of this is in CTA's overall mission and approach of bringing industry leaders together to form a united front against cyber threats, a mission NTT Security is proud to stand behind as a CTA partner.

[6] https://www.darkreading.com/vulnerabilities---threats/cryptojackers-grow-dramatically-on-enterprise-networks/d/d-id/1332852
[7] https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf

Router Attacks in October

Lead Analyst: Terrance DeJesus

In October 2018, GTIC researchers tracked and analyzed router-based attacks as internet-of-things (IoT) targeting continues to grow. In Figure 1, you can see the routers, displayed from the most targeted to the least targeted.

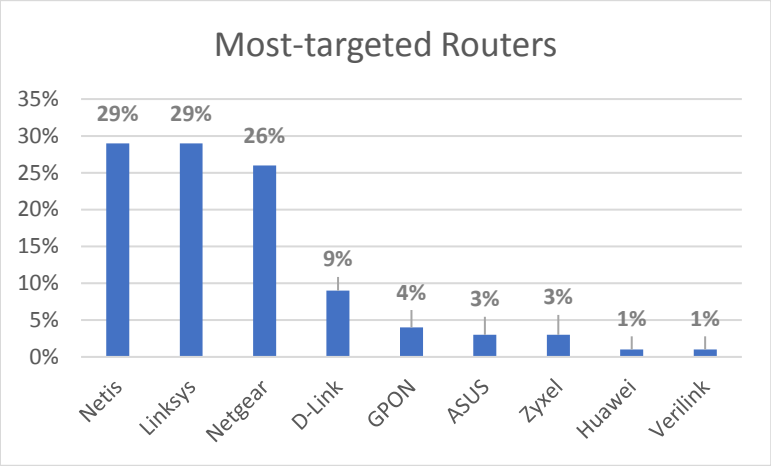


Figure 1. Most-targeted routers

Attackers Still Targeting Netis Hard-Coded Backdoor

According to Netis, more than 200 million people around the world use Netis products. Therefore, it comes as no surprise that threat actors are still targeting a hard-coded vulnerability in China-made Netis and Netcore routers. Security researchers disclosed the hard-coded backdoor in 2016 after researchers found Netcore and Netis routers listening on UDP port 53413 in which the password was hardcoded in the router's firmware. As of October 2018, attackers are still targeting these devices, with retail and business services sectors comprising 29 percent of all router-based attacks.

Mirai Compromising Zyxel via Command Injection Vulnerability

In 2017, security researchers disclosed a command injection vulnerability for Zyxel EMG2926 home routers (CVE-2017-6884[8]). Since April 2018, GTIC researchers have observed Mirai variants targeting this vulnerability to install a shell script, which then installs a *MIPS* or *x86* version of Mirai. Attackers have previously targeted Zyxel devices as part of IoT botnets, made possible using a previous backdoor vulnerability in Zyxel devices, CVE-2016-10401[9].

[8] https://nvd.nist.gov/vuln/detail/CVE-2017-6884
[9] https://nvd.nist.gov/vuln/detail/CVE-2016-10401

GPON Exploits from Egypt and Bangladesh

Although only accounting for four percent of all router-based attacks, GPON routers are now primarily being targeted from what GTIC researchers assess to be compromised hosts in Egypt and Bangladesh. In May 2018, security researchers disclosed CVE-2018-10561[10] and CVE-2018-10562[11], both of which affect GPON routers. These vulnerabilities, if successfully exploited, would allow remote code execution (RCE) on GPON routers, and analysis indicates the sources of these exploit attempts are related to the Hajime botnet. While security researchers first discovered Hajime in 2016, the botnet has never been used for any major DDoS. The popularity of the botnet died down for a short time before making a return in April 2018, exploiting MikroTik routers.

HNAP Vulnerabilities Popular Among Threat Actors

In October 2018, GTIC researchers analyzed vulnerabilities in the configuration of D-Link's home network administration protocol (HNAP) related to CVE-2016-6563[12], CVE-2014-3936[13], and CVE-2015-2051[14]. Although attacks were minimal, the sources were known for operating from compromised infrastructure for TheMoon[15] malware. In 2014, security researchers discovered and disclosed this malware for targeting vulnerable HNAP configurations in Linksys routers. While the most recent GTIC analysis did not immediately confirm if TheMoon malware variants are targeting HNAP in D-Link routers, GTIC researchers continue to analyze this trend. In September 2018, researchers discovered Hakai, a fairly new IoT botnet, targeting D-Link routers with vulnerable HNAP configurations as well.

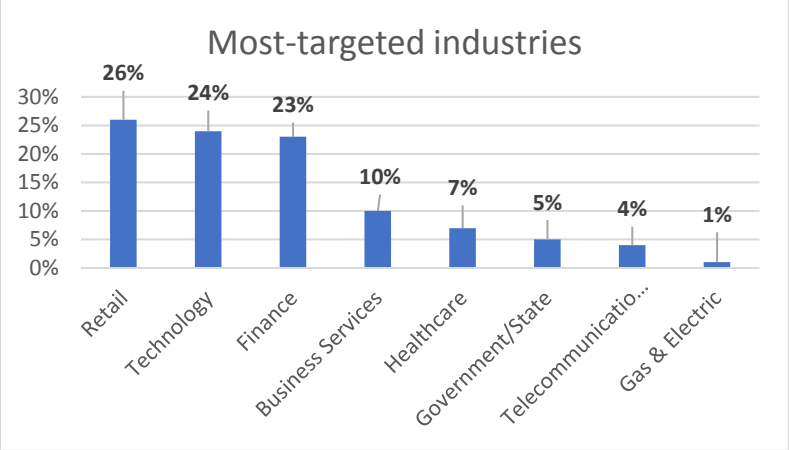
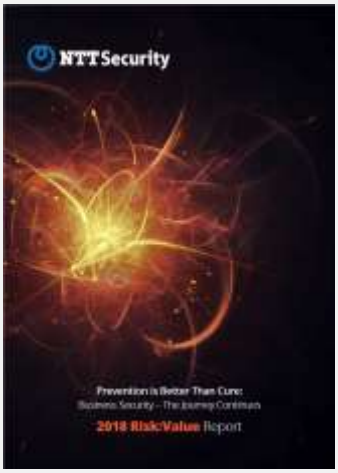


Figure 2. Most-targeted industries

[10] https://nvd.nist.gov/vuln/detail/CVE-2018-10561
[11] https://nvd.nist.gov/vuln/detail/CVE-2018-10562
[12] https://nvd.nist.gov/vuln/detail/CVE-2016-6563
[13] https://nvd.nist.gov/vuln/detail/CVE-2014-3936
[14] https://nvd.nist.gov/vuln/detail/CVE-2015-2051
[15] https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Summary+What+we+know+so+far/17633/

NTT Security Annual Reports



Risk:Value 2018

Many organizations are stuck in a reactive mindset when it comes to information security and would opt to pay a hacker's ransom rather than proactively invest in security. That's a key finding in this year's Risk:Value 2018 Report.

Download your copy today!

2018 Global Threat Intelligence Report

This year's report summarizes activity we detected in over 6.1 trillion+ logs and more than 150 million+ attacks, along with vulnerability scans, incident response engagements, and diverse findings from threat research and threat intelligence teams across NTT Security.

Download your copy today!

The NTT Security GTIC protects and informs NTT Group clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including vulnerability disclosures, threat reports and white papers, visit the resource page on www.nttsecurity.com or our blog.