NTT Security

GTIC Monthly Threat Report

April 2019

A Global Threat Intelligence Center
publication from NTT Security

Contents

Web Attacks: By the Numbers

Lead Analyst: Jon Heimerl

The media has been full of stories about coin mining attacks, ransomware, social engineering, and phishing attacks. While most security professionals know those narratives are not the whole story, many seem to forget that information security is not just about the most newsworthy activity.

The Harsh Reality

The reality is that the last two years have seen an explosion in the number of new vulnerabilities defined each year. In 2016, 6,447 new vulnerabilities were assigned Common Vulnerabilities and Exposures (CVEs) numbers – indicating that a new vulnerability was discovered and defined. In 2017, that number exploded to 14,714 new CVEs. 2018 saw that record climb even higher, with 16,555 vulnerabilities. That's an average rate of 45 new vulnerabilities each day, and 2.6 times the number of new CVEs as defined in 2016.

The Increasing Challenge

It has always been hard for organizations to keep up with the flow of vulnerabilities. The web-based vulnerability most exploited during 2018 was originally discovered in 2014, and all the top 10 were from 2017 or earlier. Maybe your patching process was running at capacity in 2016, and you were able to keep up with the release of patches designed to address the 6,447 vulnerabilities defined that year. If nothing else has changed, and your organization is still fully functioning at 2016 levels, that means you may not be addressing about 61 percent of the vulnerabilities defined during 2019.

The Attacks

Web attacks tend to focus on technologies which organizations implement in their web presence. These technologies (e.g., Apache Struts, Samba) are used frequently and, unfortunately, have many vulnerabilities associated with them.

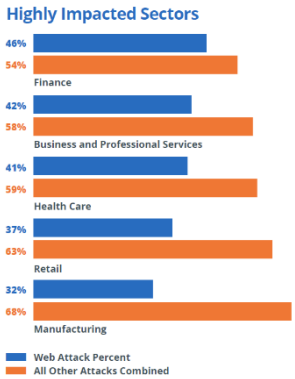
That's why attacks which focus on exposed vulnerabilities – web-based attacks, which take advantage of vulnerabilities in an organization's internet presence – made up 32 percent of all attacks during 2018. This is up from 29 percent in 2017. That three percent does not sound huge, unless you understand that three percent represents millions of attacks – and "millions" is a real, and significant, number, to any of those targets.

Nearly one out of every three attacks detected by NTT Security monitoring services targeted the applications or systems available on the target's web presence. This includes technologies like Java, Joomla, Adobe, Oracle, and WordPress (among others). In fact, there were periods of time during which well over half of all hostile activity NTT Security detected was directed at one or more of these applications. Unfortunately for the victims, these attacks can often be readily weaponized and can often be easily automated so their execution can be simplified, and consequently, their use more widespread.

The Most Attacked Sector

And these attacks also mattered where they showed up most. During 2018, the single most attacked sector according to data gathered for the 2019 Global Threat Intelligence Report was Finance, with 17 percent of all attacks globally. And what was the single most common attack type directed at financial organizations during 2018?

Web-based attacks made up nearly half of the attacks against Finance globally, accounting for 46 percent of all such attacks. While every sector was targeted by such attacks in 2018, the five industry sectors most targeted by web attacks were Finance, Business and Professional Services, Health Care, Retail, and Manufacturing. In each case, these industries experienced web attack levels above the global average. These industries tend to have a strong internet presence, which means more applications are exposed to the public web, creating a wider threat landscape. Organizations in these sectors are using applications, services, and tools which are experiencing the surge in highly exploited vulnerabilities.



The Attack Pattern

The attacks take on a different perspective at the regional levels. Attackers took advantage of regional differences to target specific sectors. In EMEA, 85 percent of all attacks against the Retail sector, and 73 percent of all attacks against the Business and Professional Services sector were web attacks. In APAC, 71 percent of all attacks against Health Care were web attacks.

Advanced attackers and nation-state actors develop and weaponize exploits for new vulnerabilities, including vulnerabilities discovered by those same actors. Mature, high quality and reliable exploits are implemented into exploit toolkits. These kits are sold to any hostile actor with the funds and inclination to buy the tools. Once included in a toolkit, these attacks can be performed with little to no skill. As a result of this automation, attacks which may have in the past focused on a single target, sector, or geographic area can now rapidly spread around the globe.

Organizations are experiencing higher numbers of attacks against the technologies they use to support their internet presence. The rising number of vulnerabilities in those technologies only makes this problem worse. It has become even more important that organizations take actions to minimize their exposures.

The Solution

- Prioritize patching on your critical and exposed systems.
- Segment your networked environment to add layers of protection around your critical systems and data.
- Perform regular vulnerability scanning to improve the chances that you find and patch vulnerabilities before a cybercriminal can use them to compromise your company.

For more information about web application attacks, including more recommendations, please read the 2019 Global Threat Intelligence Report.

U.S. Declares IRGC a Terrorist Organization – Why That Matters for Cybersecurity

Lead Analyst: Danika Blessman

On April 8, 2019, the United States labelled[1] Iran's Islamic Revolutionary Guard Corps (IRGC) as a foreign terrorist organization. This new designation comes with additional economic sanctions and travel restrictions for approximately 100,000 Iranian individuals affiliated with the IRGC. This is the first time the U.S. has taken this step against a foreign government entity and comes on the heels of the European Union levying new sanctions on Iran. Security experts expect both actions could spark an increase in the cybersecurity threat from the country.

Iran has already issued warnings of "dangerous consequences," as the U.S. designation was also backed by Middle East allies Israel and Saudi Arabia.

Since at least 2009, Iran has regularly responded to sanctions or perceived injustices against the nation by conducting offensive cyber campaigns. One such example is the 2012 denial-of-service attacks on U.S. financial organizations dubbed Operation Ababil[2], believed to be an immediate response to U.S. imposed sanctions. And it is not only U.S. organizations at risk. Based on analysis of monitoring data gathered for the 2019 Global Threat Intelligence Report, 48 percent of all Iranian activity was directed towards organizations in EMEA during 2018.

As observed historically, organizations in the financial, oil, gas, and energy sectors, and military contractors are the most likely targets of Iranian attacks; however, Iranian threat actors could easily shift focus to global targets as well as affect those in the supply chain or third-party affiliates of targeted organizations. Also, since Iran's cyber capabilities continue to expand and become more sophisticated, attacks could be more severe.

Iran's cyber capabilities have grown significantly over the past decade. The country's nation-state-sponsored threat actors have gone from essentially script kiddie status to conducting sophisticated attacks such as Operation Cleaver, along with other large attacks. The country's overall goals also seem to have shifted from more destructive operations to supply chain attacks, credential theft, as well as maintaining persistence in targeted networks.

Experts predict that Iran could compete with China and Russia as the most capable and most active state-sponsored cyber threat. Organizations should maintain awareness of the geo-political landscape, which plays a huge role, albeit highly nuanced, in targets of sophisticated threat actors.

They key takeaway here is that the cyber threat from Iran is an increasing threat which could directly impact organizations worldwide. If your organization does business with companies which could potentially be targeted by Iran, NTT Security recommends that you proceed with extreme caution in your business dealings, as your risk is potentially increased. Even if you feel Iran may not target your organization directly, it is wise to ensure your vendors, contractors, and others in your supply chain hold their own organizations to the highest of security standards.

[1] https://www.washingtontimes.com/news/2019/apr/8/iran-retaliates-after-revolutionary-guard-terror-d/
[2] https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

Operation ShadowHammer: Another Attack on the Supply Chain

Lead Analyst: Danika Blessman

Researchers recently discovered[3] another sophisticated supply chain attack similar to CCleaner[4], this time leveraging the ASUS Live Update Utility, which comes pre-installed on the majority of ASUS computers and is used to automatically update components such as BIOS, UEFI, drivers and applications.

In Operation ShadowHammer, which took place between June and November 2018, researchers estimated as many as one million machines worldwide may have been at risk. But this is likely a specially targeted campaign, as the attackers appeared to be interested in only about 600 computers, with specific MAC addresses. If one of the targets was found to have one of the selected MAC addresses, the malware downloaded the next payload – a backdoor used to maintain persistence; if the victim machine didn't match up with one of the specific MAC addresses, the malware went dormant.

A big concern here, though, is that attackers were able to deliver Trojanized updates signed with legitimate ASUS certificates *and* hosted from ASUS live update servers, which helped disguise the malicious activity for at least six months. Additionally, these factors make it nearly impossible to tell, based solely on the researchers' data, how many users were actually infected.

It is unknown, at this time, as to the success of the operation. And, while exact attribution is also unknown, an advanced persistent threat (APT) actor, BARIUM, is thought to be culpable. BARIUM is a suspected Chinese APT, part of the Winnti Umbrella, a collective of previously unconnected Chinese threat groups known to have leveraged the Winnti backdoor since at least 2009.

While exact targeted victims are unknown, many of the campaigns using Winnti have previously targeted political personnel and organizations as well as those in technology, software and gaming. Additionally, Winnt groups have targeted smaller organizations in efforts to garner valid code-signing certificates, which are then used to sign malware directed against higher-value targets.

Of note, ASUS was one of the primary targets in the CCleaner attack. It may be that attackers gained access to ASUS via the CCleaner attack and we are just now seeing the fallout.

In this campaign, the highest numbers of victim machines were in Russia, Germany, France, Italy, and the United States.

Affected ASUS users should assume that the backdoor remains on their machine. Although it may lie dormant, it's unclear whether the group will conduct further attacks. Both Kaspersky and ASUS released diagnostic tools with which you can check your own system for infection. Links to each tool can be found at the corresponding references below. In addition, ASUS issued a statement[5] regarding the attack, along with patches for the Live Update Tool.

NTT Security encourages ASUS computer users to run the ASUS and Kaspersky diagnostic tools and apply patches, where appropriate, after testing in your environment

[3] https://securelist.com/operation-shadowhammer/89992/
[4] https://technical.nttsecurity.com/post/102ev92/ccleaner-hack-what-weve-learned
[5] https://www.asus.com/News/hqfgVUyZ6uyAyJe1

New North Korean Malware: HOPLIGHT Is Worth a Second Look

Lead Analyst: Danika Blessman

U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) officials are warning the private sector about new Trojan malware variants which suspected North Korean state-affiliated attackers have deployed as part of their global operations.

A 10 April joint DHS-FBI Malware Analysis Report (MAR) [6] stated, nine different executable files are being used to spread a new malware called HOPLIGHT, suspected to be affiliated with the North Korean government's Hidden Cobra Advanced Persistent Threat (APT) group (a.k.a., Lazarus Group). The variants in HOPLIGHT employ proxy applications to disguise command and control (C2) communications between the malware and Lazarus Group. When successfully executed, the malware collects data on victim hosts.

While the malware itself is not a significant leap in capability for the group, the files are signed with valid certificates by Naver, the largest search engine in South Korea, enabling the malware to evade basic anti-virus measures. The signed certificate also enables HOPLIGHT to leverage encrypted connections to communicate with their command-and-control (C2) servers.

HOPLIGHT is a custom malware with spyware functionality; it gathers system information and has the ability to exfiltrate files and sensitive data. The malware can also inject code into various processes, which downloads additional malware, allowing the disruption of an organization's daily operations by disabling systems and files.

Although the MAR doesn't specify how the malware is disseminated, phishing is a likely vehicle, as Lazarus Group has been known to use this method in past campaigns. Targets, to date, include companies and government organizations in the U.S. for this particular campaign, although the Lazarus Group has historically targeted financial organizations worldwide.

Hidden Cobra/The Lazarus Group continuously updates its malware strategy. Last year, for example, security researchers observed the state-sponsored group using two custom families of malware against U.S. assets to include a remote access tool (RAT) called Joanap and a worm known as Brambul – both previously used but updated to more effectively target victims' proprietary data.

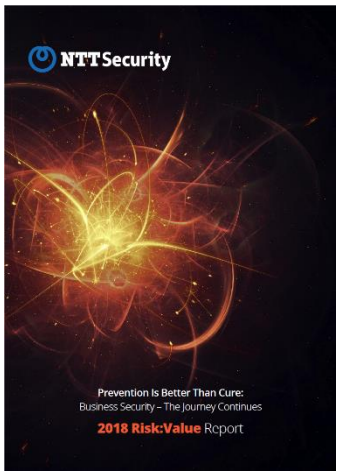
It does not appear that this new malware gives North Korean threat actors any *added* capability. In fact, some of the malware files show that these programs are over two years old. However, the clincher here is that they are using new malware with new indicators. As always, NTT Security strongly recommends prioritizing critical patches and keeping systems up-to-date.

Another point is this: Lazarus Group continues to target its victims – primarily in the financial and cryptocurrency sectors, enabling North Korea to circumvent sanctions and provide additional funding for other state-sponsored activities.

Organizations are encouraged to follow best practices, especially maintaining up-to-date patching and anti-virus, enabling workstation firewalls, and restricting user permissions for software installations.

[6] https://www.us-cert.gov/ncas/analysis-reports/AR19-100A

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!

2019 Global Threat Intelligence Report

This year's report focuses on several security challenges we have observed in organizations over the past year. Our analysis shows an escalation in coin mining, web-based attacks and credential theft, along with changes in the sectors most targeted.

Download your copy today!

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more about NTT Security or visit www.ntt.co.jp/index_e.html to learn more about NTT Group.