NTT Security

GTIC Monthly Threat Report

January 2019

A Global Threat Intelligence Center
publication from NTT Security

Contents

HHS Releases New Cybersecurity Practices

Lead Analyst: Aaron Perkins

The U.S. Department of Health and Human Services (HHS) has released what is arguably one of the most comprehensive cybersecurity preparedness documents for the health care sector in recent history.

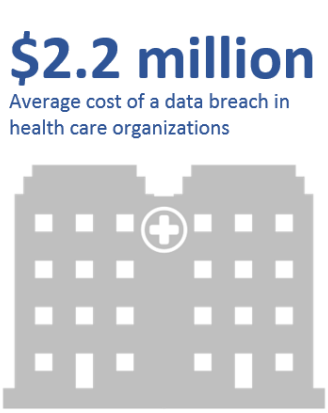
Titled "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients", the *Practices* document aims to help health care organizations both large and small defend against some of the most common threats to these organizations' cybersecurity.

The publication is broken down into three sections, a main document and two technical volumes which detail threats and mitigations to protect against those threats. While this document is not regulatory guidance, following the recommendations outlined within will make it easier for health care organizations to obtain and maintain compliance standards.

The main document makes no qualms about its purpose – it is a call to action. By fostering awareness, providing best practices, and moving toward consistency within the health care sector, the HHS has a vested interest in seeing the entire industry mitigate the most impactful cybersecurity threats.

It is no secret that the health care industry is a lucrative target for attackers, given the sheer amount of sensitive data available, as well as the industry's operational requirements.

According to the document[1], four in five doctors have experienced some form of cyber-attack. And, while 80 percent of doctors experiencing a cyber-attack is frightening, when including internet-wide scanning in that number, physicians impacted by the threat of an attack grows much closer to 100 percent.



With the average cost of a data breach in health care organizations at $2.2 million, health care organizations around the globe would be wise to take heed to the recommendations provided by the HHS.

The HHS took great care in developing this publication, ensuring recommendations aligned with perhaps one of the most-referenced cybersecurity standards – the NIST framework[2].

The HHS readily admits that even a well-developed guide which outlines best practices is only a starting point. For the health care organization that doesn't know where to start when it comes to protecting against cybersecurity threats though, this is an excellent resource. The *Practices* document does an excellent job at providing

[1] https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf
[2] https://www.nist.gov/cyberframework

information and recommendations that are not only applicable to U.S. health care organizations but can also be applied in health care settings around the globe.

Many of the cybersecurity threats facing the health care industry are similar to threats organizations in every industry face – phishing attacks, ransomware attacks, loss or theft of equipment or data, and insider attacks – all common threats globally.

Where the health care industry is unique within the threat landscape is when it comes to the very real threat against connected medical devices, where attacks may adversely impact patients' safety.

The remainder of the document provides practical recommendations on mitigating some of the most common cybersecurity threats.

While there is not room in this NTT Security report to dive into the details of each recommendation, the below snapshot should help to provide an indicator as the the level of detail (and the practicality) of the recommendations from the HHS:

- E-mail protection systems
- Endpoint protection systems
- Access management
- Data protection and loss prevention
- Asset management
- Network management
- Vulnerability management
- Incident response
- Medical device security
- Cybersecurity policies

The bottom line is that, for an industry with such a diverse threat landscape, protecting against cybersecurity threats is an incredible challenge, and it is important to have not only the right protections in place, but also to have the right organization partnering with yours so you can focus on what's most important – providing excellent care to patients.

5G: A Blessing or a Curse?

Lead Analyst: Danika Blessman

Set to roll out at some point during 2019 – depending on device and provider – 5G technology[3] promises to provide much better connectivity, flexibility, and speed for the user.

Unfortunately, these same benefits could also be security risks, as new technologies almost always mean new vulnerabilities and new targets for cybercriminals and threat actors.

So, is 5G a blessing or a curse?

The easy answer is "yes" to both; though it's not necessarily an *easy* answer. A *better* answer is "it depends" – and it depends on who you ask and what the application will be.

Sure, 5G promises incredibly low latency, blazingly fast download speeds, and an increase in signal reliability, but many organizations haven't secured their 4G and older smart devices. So, the question remains, will the 5G roll-out or security implementations of the technology be any different?

Ironically, the perks associated with 5G technology could also be considered security risks. New technologies typically mean new vulnerabilities – these will almost always be targeted by attackers – some just to "see if they can crack it" while others see a potential gain in line with their goals.

In addition, there is also the very real state-sponsored threat[4], with popular smartphone manufacturers in the spotlight regarding this technology.

5G will also see an increase in the use of cloud and virtualization technologies, further increasing connectivity, capacity, and cost-effectiveness.

With increasingly more data stored in the cloud, along with an overwhelming increase in the number of connected IoT devices, 5G technology on these devices will offer up a wealth of potential entry points, becoming more enticing for cyber criminals and state-sponsored actors, alike.

Those devices and technologies not currently secured will not be magically fixed by 5G technology.

Privacy will also continue to be a key concern, highlighted recently by a combination of what seems to be an endless series of high-profile data breaches, as well as the introduction of new regulations such as the GDPR. The implementation of 5G technology could enable a higher volume of sensitive data to cross networks at greater speed than ever before, and as with any technology which does not have security details firmly in place, a breach could be potentially devastating to an organization.

Long story, short: those devices and technologies not currently secured will not be magically fixed by 5G technology.

In fact, the additional speed and flexibility may simply expose more attack avenues – or increase the speed with which these attacks can take place.

[3] https://www.nytimes.com/2018/12/31/technology/personaltech/5g-what-you-need-to-know.html
[4] https://www.theglobeandmail.com/politics/article-canadas-spy-chief-warns-about-state-sponsored-espionage-through/

So, with the enormous undertaking of securing IoT and BYOD policies, what can your organization do to prepare the network environment for 5G technology?

NTT Security recommends that, as with any new technology, approach it with caution, ensuring that potential security risks are considered and mitigated from the start of the transition. Secure deployment may not be achievable immediately on your network environment, despite its convenience or appeal. In addition, ensure users and your organization purchase and use equipment only from vetted vendors which employ strict supply chain security, and enforce your organizations' security policies across the incoming 5G supply chain.

Worldwide: Unprecedented DNS Hijacking Campaign

Lead Analyst: Danika Blessman

Researchers[5] recently uncovered unknown threat actors, possibly with a nexus to Iran, using sophisticated methods to manipulate dozens of domain name server (DNS) records, rerouting traffic meant for these legitimate websites through malicious servers.

DNS hijacking campaigns have been targeting organizations in EMEA, North Africa, and the Americas.

This results in users who navigate to the targeted, legitimate domain, not accessing the intended website; rather, they access an attacker-controlled server which is collecting usernames and passwords. Users of these targeted websites won't typically notice any difference in their visit, other than a possible delay in website response.

These highly successful campaigns have occurred in "clusters" between January 2017 and January 2019, targeting organizations in EMEA, North Africa, and the Americas. They have spanned multiple industries including government, telecommunications, internet service providers and sensitive commercial organizations.

Researchers believe attackers leveraged DNS hijacking to gain an initial foothold into the targeted servers, though the report suggests various methods could have been used, including conducting phishing attacks to steal credentials for access or compromising a victim's domain registrar account. The attackers then use certificates which appear legitimate on the malicious servers to avoid detection.

Based on indicators of compromise used in previous campaigns by known Iranian actors, security researchers assert with moderate confidence the group is likely an Iranian state-sponsored threat actor. In addition, it appears that data gleaned from targeted domains would benefit Iranian interests, even though the data is not necessarily financially lucrative.

While DNS hijacking at this scale shows a continued growth and sophistication in Iranian-based threat actors, it is unclear as to if each campaign is conducted by the same group.

The Department of Homeland Security also issued an alert[6] regarding the attacks to reiterate the threat, releasing recommendations via the National Cybersecurity and Communications Integration Center (NCCIC), urging network administrators to take precautions such as implementing two-factor authentication, revoking malicious certificates, and verifying their DNS systems are pointing to the right IP addresses.

NTT Security echoes the recommendations of the NCCIC in addition to best practices, as a root cause for this type of attack is an improperly secured – or already compromised – DNS configuration control.

[5] https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
[6] https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign

NTT Security Observations: Apache Struts and RCE

Lead Analyst: Terrance DeJesus

GTIC security researchers analyzed all attacks targeting Apache products occurring throughout January 2019. Apache products, such as Struts, HTTP Server and Tomcat are popular products used as servers, web application frameworks, and more, and have become a vital part of the enterprise ecosystem.

In 2017, Apache Struts become rather infamous due to CVE-2017-5638, a remote code execution (RCE) vulnerability which attackers targeted heavily following disclosure. Over time, vulnerability researchers continued to discover similar vulnerabilities to that of CVE-2017-5638, and these newly discovered vulnerabilities were effective against newer versions of the Apache Struts product.

Since 2017, NTT Security researchers have seen Apache remain in the top ten most-attacked products, with attackers continuously targeting Apache products such as Struts and Tomcat.

Attack Analysis

Most attacks on Apache products in January 2019 sourced from the United States, Hong Kong, and China. The finance sector was easily the number one most-attacked industry at 77 percent. Technology came in as the second-most-attacked sector at 14 percent, and all other industries comprised the remaining nine percent of attacks.

Industry	Percentage
Finance	77%
Technology	14%
Health Care	3%
Education	3%
Oil, Gas & Electric	2%
All Others	1%

Figure 1. Attacks Against Apache Products by Industry

Source Country	Percentage
United States	49%
Hong Kong	32%
China	15%
Other	2%
Vietnam	1%
India	1%

Figure 2. Attacks Against Apache Products by Source

GTIC security researchers took special note of the high number of attacks on the finance industry and discovered continuous attempts to exploit Apache Tomcat RCE vulnerability CVE-2017-12617. This vulnerability relies on *HTTP PUT* being enabled. If *HTTP PUT* is enabled, it is possible to upload a JSP file to the server via a specially crafted request. One important note is that security experts have been recommending that organizations disable HTTP in their environments for quite some time, further recommending HTTPS as the default.

This led GTIC researchers to further analyze a specific campaign where attackers attempted to upload a custom JSP shell after exploiting this vulnerability, a very simple task for even a novice attacker. The code for the JSP shell is included in the HTTP body of the PUT request to a file named *FxCodeShell.jsp*. Analysis indicates the JSP is a webshell for Tomcat systems with a hardcoded password 'FxxkMyLie1836710Aa' embedded in the code.

Once the webshell is installed, an attacker can continue to download additional binaries or penetrate further within the network.

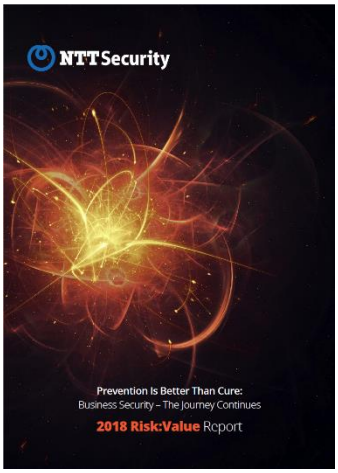
Finally, researchers analyzed the most attacked vulnerabilities which targeted Apache products. The most-attacked Apache product was Struts, with attackers attempting to exploit CVE-2017-9805[7], a vulnerability in the REST plugin which can lead to RCE in some versions of Apache Struts. Additionally, 92 percent of the targeted Apache vulnerabilities allow remote code execution if successfully exploited.

Conclusion

Apache is an integral part of many enterprises across a variety of industries, and as such, it comes as no surprise that attackers continue targeting Apache products. As a result, it is imperative that your organization keep patches on your Apache products up-to-date to strengthen your defenses against this attack vector.

[7] https://nvd.nist.gov/vuln/detail/CVE-2017-9805

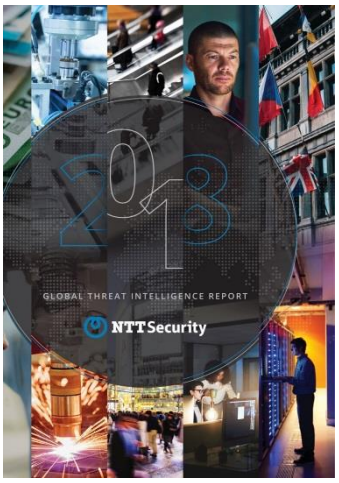
NTT Security Annual Reports



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!

About GTIC

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.

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.