NTT LTD. GLOBAL THREAT INTELLIGENCE CENTER

Monthly Threat Report

March 2020

Contents

Focus on Web Attacks

Lead Analyst: Jon Heimerl — Global Threat Intelligence Center

All organizations are at risk of a cyberattack. Attacks may take the form of ransomware, denial of service, brute forcing, social engineering and more. The types of cyberattacks an organization can face are widely varied and while realistically not endless, certainly seem so.

Throughout 2019, the most common attack type NTT Ltd.'s security monitoring services detected was application-specific attacks, with web-application attacks the second most common. Combined, these two types of attacks accounted for 55% of all attacks detected during 2019. For the previous few years, the total of these attacks ranged from 29-33% of all attacks. Both types of attacks have continued to increase in frequency.

These attacks often focus on the web-presence of an organization. This does not mean just the 'website' but any internet-accessible system, as well as supporting applications or tools. For instance, about 20% of all attacks NTT Inc. observed in 2019 targeted some form of content management system (CMS). This includes WordPress, Joomla!, Drupal, noneCMS and other similar tools. There were periods throughout the year where Joomla! or Apache Struts was the single most attacked technology for a week or more at a time.

Additional supporting technology like Apache Tomcat, Adobe ColdFusion, XWork, JBoss and Oracle products were all highly targeted in 2019.

Unfortunately, there is no one control an organization can put in place to secure their entire web-facing environment. The best solution to combat web-application and application-specific attacks is to architect security into the very fabric of the organization – to build a layered defense which considers security as a fundamental business requirement. But what do you do until you get there?

Organizations should consider the following recommendations to reduce their exposure to these attacks. While there is a natural progression in the recommendations, even improving a single area has the potential to reduce an organization's attackable footprint.

1. **Know what you have**. Make a full inventory of the systems involved with your web presence. That's not just the webserver or the storefront server. It's the servers, their operating systems, the middleware and other code which runs on the server. It's the content management system which supports the site, and the backend database which supplies the data. Think of it as an ingredient list, of everything you would need to rebuild your web presence. If you can't name it, you can't manage it. Better yet, add how critical each piece is to the environment and you just jumpstarted your business continuity planning.
2. **Harden everything.** Harden the operating systems, stripping or disabling functions you don't need. Delete or disable default accounts. Change all passwords. Run applications at their lowest practical privilege levels. Use resources to properly configure the software you are using – for instance, Oracle has dedicated manuals devoted to the secure installation of WebLogic. Most tools and supporting software have such documentation. Unfortunately, there is a difference in 'making it work' and 'making it work well', including proper security configurations. Make sure responsible staff have formal training (not just 'the manual') to help ensure they can maximize the effectiveness of the tools and systems available.

   Much of the software and tools used in these environments are vulnerable because they are improperly installed and configured.

	2016	2017	2018	2019
Application-specific	11%	13%	21%	33%
Web application	22%	16%	11%	22%
Total	**33%**	**29%**	**32%**	**55%**

Table 1: Common attack types and year-on-year growth

Focus on Web Attacks, continued

3. **Patch everything.** On 14 December 2015, Joomla! issued a patch for CVE-2015-8562 – a vulnerability in Joomla! which could allow remote attackers to run code on the targeted system. Attacks targeting this vulnerability were some of the most common attacks of 2019 – more than four years after the patch was made available. Of the 15 most-targeted vulnerabilities NTT Ltd. observed in 2019, only one of them was less than two years old. Those 15 vulnerabilities covered over 88% of all attacks. If an organization had fully patched those 15 vulnerabilities across its operating systems, tools and applications, it could potentially make 88% of all exploit attempts ineffective. Prioritize patching for the systems which are most critical and most attacked; for example, since attackers are targeting CMS suites, if you are using one, making sure it is on the latest revision level is important. Then, that inventory you made in step 1? Use that to help monitor for new patches and updates, and apply those as soon as practical after release. Patching is boring, but necessary.
4. **Code securely.** Make sure your developers are using secure coding techniques. That probably means training them in secure coding principles and techniques, then equipping them with tools to help. Build core components with inherent trust and maximize their use. Improve error handling (fail securely), input field sanitization (never trust user input), and logging. Learn the OWASP Top 10[1] and how to avoid exposure. Be rigorous with your source code repository and bug-tracking system. Test your code and perform application security testing against code in a near-production environment before it goes live. Always know exactly what you have migrated to production.
5. **Protect your data.** If you don't need to store sensitive data, don't. At least don't store it in that backend database which supports your web presence if you don't need to. If you do store it, encrypt it while stored, and encrypt it while it moves between the application server and the database. And, isolate that data from the external systems – don't store it on the webserver or on the DMZ – and truly segregate it.
6. **Segregate systems.** Segregate systems to the extent practical. Put front end, web-facing systems on different segments from backend systems. And segregate backend systems from other core segments within the organization. Protect communications between the segregated systems with ACLs and firewalls as appropriate – making conscious decisions on exactly which communications are explicitly allowed. Everything else should be denied. Avoid repeating credentials on segregated systems unless required by the specific software being used. Protect internal systems from compromises in other internal systems.
7. **Manage your vulnerabilities.** Test your entire web presence for vulnerabilities. Identify and track them. Assign resources to fix them. Provide those resources with the training and tools necessary to fix them. Actively track open vulnerabilities and report on progress. Verify patches, verify installation, verify implementations, verify redeployment and test again. Repeat. If you can find the vulnerability, an attacker can. Find and fix everything, then keep coming back to test again as new vulnerabilities or exploits are developed. Remember that vulnerability management is a truly dynamic practice.
8. **Implement a WAF.** A web application firewall (WAF) can help identify attacks attempting to abuse your web-enabled applications and protect you from them. The whole purpose of a WAF is to analyse web traffic and decide what is legitimate traffic and what is fraudulent or malicious activity. Some vulnerabilities cannot be easily patched or closed, especially if they are in commonly used utilities. A WAF can help plug some of those holes while other patches are prioritized and pass through the organization's evaluation and testing phases.
9. **Ensure your web presence is part of your Incident Response Plan.** In step 1 you made an inventory of systems, applications, tools and data which supported your web presence. Prioritize how critical the elements of your web presence are to your business operations and integrate them into incident response and management planning. Be realistic about the impact your web presence has on your organization. If the online store for a top five retail company is down, it's a big deal. If your site is more for informational use only, like company history or directions to your office, it's probably not a critical priority in incident planning.
10. **Train and practice.** Train administrators in the use of the technology they are using. Place emphasis on the secure use of technology which supports resilient operations. Train employees on the importance of security policies and controls, and train managers, including executives, on that security as well as the need to support security initiatives. If the people involved with building and supporting your operational web presence are not properly trained in the technology they are using and the security decisions of the organization, the probability that they will make mistakes goes up. And, your attacker will take advantage of those mistakes.

This list is more of a summary of how to protect your web presence than it is a comprehensive checklist. Realistically, it will be hard for many organizations to implement everything here if they haven't already started. The best way to implement a secure web presence would be via a secure-by-design process, built with security as a foundational control. But if you are not in the position to do that, any progress you can make on this list will make you more secure.

> The best solution is to **architect security** into the very fabric of the organization.

[1] https://owasp.org/www-project-top-ten/

#Spotlight 1

A look at the CTA Threat Assessment on the 2020 Olympics

Lead analyst: Jeremy Bender — Global Threat Intelligence Center

Since the 2008 Olympic Games, cyberthreat activity targeting the Games has consistently increased. For each subsequent Olympics, researchers found activity targeting the Games and associated organizations has grown in frequency and sophistication. In general, researchers have found disruptive attacks to be the most common attack type and have observed sustained campaigns lasting for months.

Due to this potential for cyberthreat activity, the Cyber Threat Alliance (CTA) recently released its 2020 Summer Olympics Threat Assessment[2]. The CTA is a security consortium comprised of members of various cybersecurity industry partners – including NTT Ltd. (known as NTT Security at the time of the report). Researchers and analysts at NTT Ltd. participated in the creation of CTA's assessment.

The CTA is focused on protecting the security, integrity and availability of IT systems by improving defenses and advancing critical infrastructure security. To achieve this, CTA focuses on protecting end-users, disrupting malicious actors and elevating the overall security posture.

The Olympics Threat Assessment is intended to provide security recommendations to the Tokyo Organizing Committee, as well as to help share industry knowledge and prepare for potential incidents which may impact those associated with the Games. This includes sponsors, supply chain organizations, infrastructure providers, participants and attendees.

The CTA Assessment found that anti-doping agencies and services supporting the Olympics' operations and logistics are at the highest risk of attack – based on historical targeting and the current threat environment. Still, potential cybersecurity risks exist across the spectrum, from tourists and spectators to partner governments. As the report outlines, the risks vary depending on the target; however, the CTA assesses the most prominent threats are likely disruptive cyberattacks and disinformation campaigns launched by nation-states.

Cybercriminals are also likely to go after targets of opportunity and attempt to profit off potentially lax cybersecurity standards among tourists and associated organizations through various actions, such as phishing emails, compromise of public WiFi systems and ticket scams. While some targets are more likely to be targeted than others, the report outlines potential security concerns for a variety of groups.

Although the Threat Assessment is written particularly for the Olympics, its recommendation section is applicable for all major events in which third parties, ranging from government organizations to corporate sponsors, are involved.

You can read CTA's full Threat Assessment at the CTA website[2].

CTA's Threat Assessment provides **recommendations applicable for all major events**, not just the 2020 Olympics.

[2] https://www.cyberthreatalliance.org/wp-content/uploads/2020/02/CTA-2020-Olympics-Threat-Assessment-Report_Final-1.pdf

Reality check: That update on the coronavirus in your city is *not* real

Lead analyst: Danika Blessman —

Global Threat Intelligence Center

Let's face it: cybercriminals often take advantage of major events to send out phishing emails in attempts to capitalize on the potential curiosity or panic or any given event. The content of these phishing or malware campaigns could even create additional panic. Pretending to be a source of news about a current crisis or news story has become a common technique, whether the subject is a crashed jetliner, an earthquake, a hurricane or a potential pandemic. This holds especially true in cases like the new coronavirus (COVID-19), particularly as global concerns rise about the potential spread of the disease.

The World Health Organization (WHO) has issued warnings[3] to the public of potential malware and phishing campaigns disguised to make it look as if they are coming from WHO officials, containing subjects and content such as safety measures concerning the coronavirus.

Many phishing emails are easily identifiable, with glaring errors like incorrect spelling or grammar, and overly sensationalistic language.

However, some phishing emails are more realistic, like the images in Figure 1 using the WHO logo or website, with an overlaid frame prompting for login information. In some cases, once the attackers have acquired your information, you are simply redirected to the actual WHO website.

So far, we have observed fake coronavirus campaigns attempting to deliver malware, redirect users to hostile sites and steal email credentials.

Be wary, too, of emails relaying information (possibly misinformation) about how the virus was initially released, is transmitted, that numbers are being inaccurately reported, etc.

These emails will likely be more effective for those in regions with a higher incidence of coronavirus.

In addition, new information from the Centers for Disease Control (CDC) in the U.S.A suggests[4] that the coronavirus is expected to hit epidemic proportions in the U.S.A. as well, giving further fodder for phishing campaigns.

Many of these campaigns are currently leveraging Emotet, a highly used and effective banking Trojan. While Emotet is often disguised as an invoice, receipt or coupon, NTT Ltd. J-CERT reported in January that they had already observed emails using Emotet to leverage the coronavirus theme.

NTT Ltd. recommends that users do not click on links in emails, rather manually enter the website, such as the World Health Organization (www.who.int) or the United States Centers for Disease Control (www.cdc.gov) to obtain the most up-to-date information.

In addition to their warnings, the WHO has set up their own page for users to report suspected scams.[5]

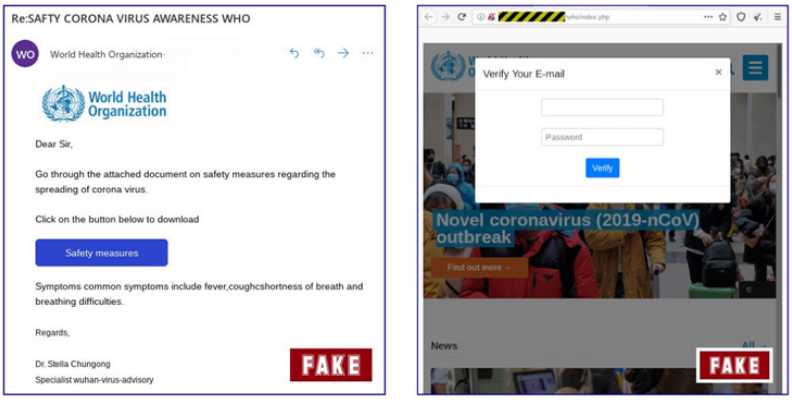

Figure 1: Sample phishing email and website impersonating WHO

[3] https://www.bleepingcomputer.com/news/security/world-health-organization-warns-of-coronavirus-phishing-attacks/
[4] https://www.cdc.gov/media/dpk/diseases-and-conditions/coronavirus/coronavirus-2020.html
[5] https://www.who.int/about/report_scam/en/

NTT Ltd.'s Global Threat Intelligence Center

The NTT Ltd. Global Threat Intelligence Center (GTIC) protects, informs and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT Ltd. to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT Ltd.'s threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT Ltd.'s security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

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 report

Risk:Value 2019

In 2019, 33 percent of organizations around the world would consider paying a ransom to a hacker rather than investing more in cybersecurity because paying the ransom is cheaper. Read more about this and other trends in the 2019 Risk:Value report.

Download report


NTT