GTIC Monthly Threat Report

September 2017

Name	GTIC Monthly Threat Report – September 2017
Owner	**NTT Security GTIC**
Classification	UNCLASSIFIED-EXTERNAL
Status	APPROVED
Version	V1.0
Date	**29 September 2017**
Review	29 September 2017

Contents

1 Most Targeted Vulnerabilities

Overall in September, "Shellshock", Apache Struts, and IIS Server vulnerabilities were the primary targets of attacks against client networks, as analyzed by the Global Threat Intelligence Center (GTIC). **Figure 1** details the top 10 vulnerabilities of exploitation attempts. Please note, CVE-2014-6271 (Shellshock) was removed because detections resulted from excessive and continued scanning.

CVE	Company	Product	Percentage
CVE-2017-5638	Apache	Struts	22%
CVE-2014-0114	Apache	Struts	16%
CVE-2011-3230	Apple	Safari	13%
CVE-2000-0884	Microsoft	IIS	8%
CVE-2017-9805	Apache	Struts	6%
CVE-2017-7529	Nginx	Nginx	3%
CVE-2012-4167	Adobe	Air SDK	3%
CVE-2015-1635	Microsoft	Windows 7	< 3%
CVE-2011-0623	Adobe	Flash Player	< 3%
CVE-2016-3081	Apache	Struts	< 3%

Figure 1: Top 10 vulnerabilities with exploit attempts

As shown in this table, Apache Struts vulnerability CVE-2017-5638 was targeted the most, with 22 percent of all exploit attempts. It should also be noted that 4 out of 10 vulnerabilities listed were for Apache Struts, with the recent CVE-2017-9805 being listed as well. Analysis indicates 49 percent of all vulnerabilities targeted during September were for Apache Struts, highlighting the need to focus on updating and patching existing systems if Apache Struts is present in your environment.

1.1 Apache Struts Exploits

Apache Struts vulnerabilities which allow remote code execution (RCE) were popular targets in the month of September. Of these vulnerabilities, CVE-2017-5638 was the only target for which attackers attempted to download malware payloads post-exploitation. The primary focus for CVE-2017-9791 and CVE-2017-9805 were reconnaissance attempts, where threat actors were monitoring responses to determine if the exploit worked successfully. It should be noted that the GTIC has observed several CVE-

2017-5638 exploit attempts in which actors attempt to download a cryptocurrency miner (afe0135e0a63627447fc33020d9e19be) from 91.230.47[.]40.

2 Vulnerability of the Month

Apache Struts REST Plugin – Remote Code Execution

Threat Status: High

CVE-2017-9805

Severity: High (CVSS: 10)

Date: September 7, 2017

Remediation Details: Please update to the latest version of Struts. A patch was released in Apache Struts 2.5.13 and Struts 2.3.34.

Affected Versions: Apache Struts versions 2.5 through Struts 2.5.12

Analyst Note: Security researchers have discovered a critical remote code execution vulnerability in Apache Struts, a popular open-source framework for developing web applications in the Java programming language. All versions of Struts since 2008 are affected, and all web applications using the framework's popular REST plugin are vulnerable. Users are advised to upgrade their Apache Struts components as a matter of urgency. This vulnerability has been addressed in Struts version 2.5.13.

The REST plugin uses a vulnerable function called XStreamHandler which does not properly sanitize user input from a user's HTTP requests. The XStream library is commonly used to deserialize objects in Java applications. The attacker can create a Java object, send it through an HTTP request, and the XStream library will deserialize it, which can allow an attacker to remotely execute code on the victim's machine.

3 Equifax – What Can You Do?

143 million – that's the approximate number of people whose data was lost in the Equifax breach of May-July 2017.

If you use the population numbers from the U.S. Census Bureau and subtract people who don't have active credit, that leaves you with approximately 205 million people. If all Equifax victims were U.S. citizens (some were actually citizens of Canada or the United Kingdom), that would mean this specific breach touched nearly 70 percent of all U.S. adults.

This means *your* name, address, social security number and some credit cards – basically everything someone needs to create fake accounts and steal your identity, are more readily available than ever before.

Unfortunately, with the breach of Equifax of this magnitude, we must understand that all of our credit information has been compromised (if it wasn't previously). This puts people in a position which should make it clear that *people* are *personally accountable* for the security of their own information. NTT Security recommends the following:

1. Check your credit information regularly. Spreading out your free reports across the three main agencies can get you a free report every four months.
2. Monitor your own credit by actively checking transactions on a regular (i.e., frequent) basis.
3. Set alerts with your credit card providers.
4. Consider setting a credit freeze with the three reporting agencies.
5. Determine if a credit monitoring or identity theft protection service is required by your risk tolerance.

On the other hand, organizations have always been responsible for the protection of their own data – the data they use and maintain in their environment. As can be seen in this particular case, two basic security controls can drive a significant amount of improvement in any organization which actively implements them.

1. Clearly identify your most important data, along with the systems and infrastructure required to support that data. This might mean servers, operating systems, middleware or applications – in this case, it also means Adobe Struts.
2. Patch. Patch everything identified in the previous control. Make sure you are as up to date as possible in the systems which support your most critical data. If, for instance, your Adobe Struts or content management software (like WordPress or Joomla!) are out of date, you are exposing yourself, and your critical data, to unnecessary risk.

Protecting yourself is no easy task, but taking these actions can remove a significant amount of vulnerabilities from your environment, along with reducing the potential for exploitation and exposure those vulnerabilities bring with them.

4 Natural Disasters Set the Stage for Phishing

Natural disasters and high-level breaches continue to provide opportunities for scammers to capitalize on either the urgency of the situation or the collective fear, particularly on those wanting to assist.

The US-CERT recently issued a warning regarding phishing scams and other fraudulent activity related to Hurricane Harvey. This warning should serve just as well for the subsequent hurricanes: Irma, Jose, Katia and Maria, along with wildfires across much of the Western U.S., as well as the Equifax breach.

During and after natural disasters and breaches, phishing campaigns and other scams commonly take advantage of donors as well as victims. These scammers set up bogus "relief funds," request donations, and offer assistance in some capacity.

Phishing attacks will likely be persistent during and after these disasters, and clients are advised to be cautious of any emails and hyperlinks referencing the storm(s).

In addition, victims of the recent hurricanes or wildfires may receive falsified emails which claim to be from their homeowner, flood or fire insurance company, urging them to click on a link or document to file their claim. Others may see outright attempts to steal cash, saying that if their next insurance payment isn't made, their insurance claim won't be honored.

Attackers will use any means to gain access to your information, as scams aren't limited to cyber means. There are reports of would-be looters going door-to-door pretending to be emergency service providers or government officials, ordering homeowners to evacuate, then robbing their homes when they comply.

Of course, this isn't limited to recent hurricanes, or even to natural disasters. NTT Security analysts expect similar efforts for any event during which people are giving of their time and money.

Be vigilant, especially of emails or social media sites which solicit donations. As always, avoid clicking on links in unsolicited or untrusted emails. Those wishing to donate to relief funds are encouraged to go to an organization's website directly. In addition, those who may have been affected by the Equifax breach are encouraged to check their information here, as well as monitoring their credit card statements and credit reports.

References:
Potential Hurricane Harvey Phishing Scams

Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes

5 Dragonfly Campaign Returns, Targeting Energy Companies

Since 2014, in a campaign known as Dragonfly (a.k.a. Energetic Bear), suspected Russian actors have been targeting power and energy companies in the U.S. and Europe.

In a newly discovered campaign dubbed *Dragonfly 2.0*, the actors appear to have gained access to at least 20 targeted networks, including operational access to industrial control systems. In other words, these threat actors seized control of equipment which could stop the flow of electricity to U.S. homes and businesses.

Researchers have been unable to determine if the access is newly acquired or if these actors have been maintaining a foothold in these networks for the last few years.

Initial access is likely to have been gained via spear phishing emails, including a malicious attachment appearing to be an invitation to a New Year's Eve party. Once opened, the infected attachment leaks the

victims' network credentials to a server outside the company. The attackers also used other measures, including watering holes and fake Adobe Flash Player update alerts.

Researchers believe these same actors gained operational access to Ukrainian power companies twice in the last several years by leveraging the Black Energy malware family, affecting delivery of electricity to homes across a portion of that country.

It may be that these actors intended to maintain the ability to affect these networks at a specific time, rather than immediately impacting these networks.

This campaign has all the hallmarks of a Russian state-sponsored intrusion, though researchers believe it could simply be coming from inside Russia or from actors who hold Russian interests at heart. Perception management is a standard Russian tactic – hoping its victims will wonder at what point their attackers will exploit the access to its power grids.

IoCs are available, but one can assume an actor this sophisticated – and motivated – also has other cards up its sleeve. NTT Security expects more IoCs to surface in the future and will implement detection capabilities as necessary.

References:

Dragonfly: Western energy sector targeted by sophisticated attack group

Russia's Zapad-17 Has Already Succeeded