Weekly Threat Briefs

FortiGuard Threat Intelligence Brief - October 06, 2017

View this article on online

Activity Summary -- Week Ending October 6, 2017

In 2013, Yahoo suffered a huge data breach resulting in the leaking of sensitive information from about 1 billion accounts. It was considered to be the largest information breach in history. It was followed by another one - again suffered by Yahoo - in 2014, which affected another 500M accounts. However, this week Yahoo revealed that the numbers released from the 2013 hack were inaccurate. In fact, the number of accounts actually stolen was a staggering 3 billion, which represents all existing Yahoo accounts at the time.

Similarly, this week during a hearing on the facts surrounding the recent Equifax breach, the number of accounts that were lost was also tweaked, increasing the

total from 143 million to 145.5.

If you are among the customers of one of these two companies, and you are not sure if your data was stolen or not, your best option is to assume that you were and then act accordingly, starting with modifying your access credentials. If you're an organization with an Internet-facing application, the FortiGuard Credential Stuffing Defense service for FortiWeb can help ensure that your applications are protected against stolen credentials compromised in previous data breaches.

Malware Activity

Rank	Name	Volume
1	*VBS/Agent.PGE!tr.dldr*	*3,627,959*
2	*W32/PECompact*	*2,212,777*
3	*JS/Nemucod.3218!tr*	*1,595,752*
4	*VBS/Agent.9A6B!tr.dldr*	*945,159*
5	*W32/BackDoor.Prosiak.65*	*456,392*

VBScript again on the top -- Ransomware campaigns are usually distributed through malicious VBScript attachments via spam or phishing emails. A new wave of these emails loaded with malicious attachments was deployed this week.

Dealing with VBScripts is always hard for the average user. They are usually embedded in some document attached to an email from an address that looks like an authoritative department or figure. When the victim, compelled by this information, opens the document, it executes a hidden PowerShell script and attempts to download potentially malicious files such as ransomware to infect the computer. For this reason, it is always important to remember to educate your employees about cyber risks and threats, and in general be very careful when receiving and opening unsolicited emails.

Last week, our top detection was a VBScript (**VBS/Agent.PGE!tr.dldr**) that was observed to download the ykcol. variant of Locky. It set off nearly 19,000 sensor triggers this past week, of which 35% were detected from the United States and close to 35% were from Japan. This variant first appeared on September 26th,

2017. After peaking in activity last week, it slowed down considerably over the weekend. We will continue to track this family and share our findings with readers as new details come to light.

Application Vulnerabilities / IPS

Rank	Name	Volume
1	*SNMP.v1.Spec.Violation*	*160,193,333*
2	*Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass*	*149,028,733*
3	*MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure*	*67,787,773*
4	*TCP.Split.Handshake*	*29,083,848*
5	*Web.Server.Password.Files.Access*	*21,392,484*

WordPress Plugins at it again - This week we saw an increase in the signature **Wordpress.N-Media.Website.Contact.Form.Arbitrary.File.Upload**. This indicates an attack attempt against an Arbitrary File Upload vulnerability in the WordPress N-Media Website Contact Form plugin. The vulnerability is due to the insufficient sanitizing of user-supplied inputs when handling a crafted file upload. It allows a remote attacker to upload an arbitrary file onto vulnerable systems via a crafted HTTP request. The vulnerability affects WordPress N-Media Website Contact Form Plugin 1.3.4 and prior. To remove this vulnerability from your system it is sufficient to update the plugin to the latest version.

IoT, Internet of Threats - Another spike in popularity was observed for the signature **WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution.** This indicates an attack attempt to exploit a Command Injection vulnerability in WIFICAM. This vulnerability is the result of improper validation of user-supplied inputs in the application. A remote attacker can exploit this to inject malicious commands on the affected devices. Currently, we are unaware of any vendor-supplied patch or updates available for this issue. Therefore, FortiGuard Labs recommends switching to a more secure option.

Web Filtering

Banload - We have noticed an ongoing Banload campaign that uses Facebook's CDN to deliver the initial payload. Once the victim executes the initial payload (Banload file), it then attempts an HTTP GET request to download a second payload, which is a SpyBanker file. We have blocked the IOCs associated with this campaign.

Malware Detection:
W32/Trojandldr.DEBS!tr (Banload)
W32/Banker.AECD!tr.spy (SpyBanker)

IOCs:
manosunidas-online[.]org/biblioteca/templates/beez/html/com_search/search/search/my[.]zip (SpyBanker download link)
eletrodoria[.]com[.]br/aspnet_client/system_web/1_1_4322/folder/a1bc/index[.]php (C2)

Pandabanker - Recently, we discovered several URLs from Rig EK that deliver Pandabanker malware via Rulan gate. Pandabanker is a Zeus dubbed banking trojan used for targeted attacks via email attachments. FortiGuard Labs has blacklisted all associated URLs.

IOCs:
gordinka[.]xyz
kostinka[.]xyz
makabob[.]xyz
188[.]225[.]82[.]250

Threat Research & Insights

Ichitaro Vulnerability - OLE (Object linking and embedding) is a common technique used in macro-enabled documents for MS Word. FortiGuard Labs took a look at how this technique can be exploited on Ichitaro, a popular alternative to MS Word in Japan. Read More

- (https://www.facebook.com/FortiGuard.Labs)
- (https://plus.google.com/+fortinet)
- (https://twitter.com/FortiGuardLabs)
- (https://www.linkedin.com/showcase/3668640/)
-  (/rss-feeds)

- Contact Us (/contactus)
- Legal (https://www.fortinet.com/corporate/about-us/legal.html)
- Privacy (https://www.fortinet.com/corporate/about-us/privacy.html)
- FAQ (/faq)