View this article on online

Activity Summary -- Week Ending September 1, 2017

The advent of the WannaCry ransomware caused immense problems around the world. One of the most famous victims of this malware was the NHS (National Health Service) in the UK. Its compromise served to elevate a concern that has been highlighted over the past year or so by the growth in ransomware attacks targeting the healthcare industry. In our ultra-connected world, this has become an issue that didn't even exist just a few decades ago. How do we protect data that needs to be freely accessed and shared by a variety of people? The information held by healthcare organizations is obviously of extreme importance and must be defended thoroughly. However, it also needs to be accessed and shared among healthcare providers, often in different locations, as well as with patients and even healthcare administrators. To address this issue, Fortinet recently posted a blog where we identify the biggest challenges that today's healthcare organizations face, along with a list of possible solutions to consider.

On a related topic, we also made an estimate of how much monetary damage a ransomware attack like WannaCry can generate in another article. If you are interested in the details, you can read them here.

Malware Activity

Rank	Name	Volume
1	VBS/Agent.PDB!tr.dldr	4,167,174
2	W32/BackDoor.Prosiak.65	718,435
3	JS/Nemucod.DGY!tr	186,061
4	Riskware/NetFilter	54,065
5	Riskware/Asparnet	41,603

Script malware continues to deliver ransomware -- Nemucod is a javascript Trojan that downloads potentially malicious files to an infected computer. It is commonly spread through spam or phishing emails that contain malicious attachments. These emails are normally disguised as coming from an important sounding department or an organization, claiming that the attached file is vital information that requires opening to view. Over the past week, a variant of Nemucod (**JS/Nemucod.DGY!tr.dldr**) that does this very thing has reappeared at third place in our rankings.

Ransomware campaigns are usually distributed through malicious attachments via spam or phishing emails. When an unsuspecting user opens the attachment, malicious code is run, and often, additional malware is subsequently downloaded onto the affected machine. This is the reason we

have always strongly recommended that our customers think twice before opening any unexpected Microsoft Office file or script attachments in any email, especially from any unsolicited senders, and that they create an active training program for employees and others to educate them on this and other cyber risks triggered by end users.

VBS/Agent is another notorious script malware that has been observed to download and execute ransomware. Last week, **VBS/Agent.PDB!tr.dldr** was at the top of the most prevalent malware chart. We have detected approximately 4 million additional hits in just the last 3 days. 31.8% of these were detected from the United States, and 17.9% were from Japan. 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	231,957,776
2	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	37,711,488
3	MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure	19,916,619
4	TCP.Split.Handshake	9,638,900
5	Web.Server.Password.Files.Access	4,570,271

Old Bugs are the Best Bugs -- This week, FortiGuard Labs saw an increase in the detections of signature **FlashChat.Arbitrary.File.Upload**, which indicates an attack attempt against an arbitrary file upload vulnerability in FlashChat. This vulnerability, discovered in 2013, affects FlashChat 6.0.8 and earlier versions, down to 6.0.2. The vulnerability is caused by insufficient sanitizing of user-supplied inputs when handling an unauthenticated file upload. It allows a remote attacker to upload an arbitrary file onto vulnerable systems.

At the moment, FortiGuard Labs is not aware of any patch released by the vendor. Given that the vulnerability is from 2013, it is unlikely that one will be released anytime soon, so we strongly recommend switching to more up to date and secure software.

NTP Vulnerability Holds Steady -- In terms of sheer volume, the signature **NTP.Monlist.Command.DoS** has been the most detected over the past year. Obviously, these numbers have to be evaluated while keeping in mind that this vulnerability is used to perform DoS attacks, so the number of detections cannot be the only metric used. Regardless, this vulnerability remains the favorite of attackers when it comes to DoS attacks. The vulnerability exists due to an error that occurs when the vulnerable software handles a maliciously crafted request. It affects NTP before 4.2.7p26 and allows attackers to generate a very large amount of data traffic by sending a very small amount.

FortiGuard Labs recommends upgrading to the NTP version 4.2.7, which removes the monlist command entirely. Otherwise, it is possible to start the

removes the monlist command entirely. Otherwise, it is possible to start the NTP daemon with noquery enabled in the NTP conf file. This will disable access to mode 6 and 7 query packets.

Web Filtering

Filecoin dot online - FortiGuard Labs discovered this phishing site targeting Filecoin. The domain was newly created on 22nd August 2017. Reverse whois reveals that the threat actor, **juliahealdsburg95448 at india dot com** also owns 3 other domains created for a similar purpose. We have added all of these domains to our blacklist.

Web dash appleiid dash applle dot com - FortiGuard Labs has identified this domain as a phishing site targeting Apple users. Reverse Whois revealed the Threat Actor as **michelleknox15 at outlook dot com,** who owns another 107 phishing domains which were also recently created in 2017, and that target Apple, Paypal and BitCoin users. Fortiguard Labs has blacklisted all of these domains

---

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