Weekly Threat Briefs

FortiGuard Threat Intelligence Brief - August 18, 2017

View this article on online

Activity Summary -- Week Ending August 18, 2017

Last week FortiGuard Labs identified a new campaign of the Locky ransomware, identified as "Diablo6", and described in detail how it propagates. For this reason, we decided to also release an in-depth technical analysis of the samples we found. You can find more about this in the *Threat Research & Insights* section below. This seems to be the beginning of a Locky resurgence, because, in breaking news, we just detected another new variant known as "Lukitus" that hit the streets in just the past couple of days. Details about this latest variant are now available on our Fortinet blog site, and we will describe this latest Locky variant in more detail in next week's threat intelligence brief.

In last week's brief, we reported that the FBI was investigating Marcus

In last week's brief, we reported that the FBI was investigating Marcus Hutchins, aka @MalwareTech, for the creation and distribution of the banking malware Kronos. Earlier this week Hutchins pleaded innocent to all accusations in court. His trial is set to take place in October 2017.

Malware Activity

Rank	Name	Volume
1	WM/Agent.AP!tr.dldr	330,978
2	Riskware/NetFilter	44,201
3	W32/Farfli.BGG!tr	37,725
4	PHP/WebShell.AS!tr	32,772
5	Riskware/Asparnet	26,482

TrickBot on the rise - Banking Trojans are dangerous for the victim because they provide cyber criminals with the credentials they need to access banking accounts.

After being downloaded by WM/Agent.AP!tr.dldr via a malicious macro, Trickbot uses an advanced technique to seamlessly display its own login page, hosted on a separate server, to the victim rather than the login page they were intending to use. It does this through a technique known as web injection. The tricky part is that it still displays the genuine URL and certificate of the banking site page to the user, making it very difficult to determine that he/she could be the victim of an attack.

WM/Agent.AP!tr.dldr was at the top of our most prevalent malware chart this week. It had approximately 850 FGT triggers yesterday, of which 69% were detected from Japan and close to 24% were from the United States. This variant first appeared on July 20th, 2017 embedded in a Word document file(.doc). The past weekend there was a large spike in activity, almost double the last time this malware was active, but that activity has now leveled off.

FortiGuard Labs has been monitoring this malware carefully since the earliest version of this family was discovered in 2016. We will continue to track this malware family and share our findings with readers as new details come to light.

Application Vulnerabilities / IPS

Rank	Name	Volume
1	SNMP.v1.Spec.Violation	300,109,411
2	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	53,993,981
3	MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure	22,035,927
4	TCP.Split.Handshake	12,748,080
5	Web.Server.Password.Files.Access	5,637,338

Not the MVP(ower) - This past Tuesday we saw an unusual increase in the number of triggers for signature **MVPower.DVR.Shell.Unauthenticated.Command.Execution**. The affected product with this vulnerability is a digital video recorder, MVPower model TV-7104HE, running firmware older than version 1.8.4. The 'shell' file on the web interface of the digital video recorder performs insufficient validation of user-supplied inputs when processing HTTP requests. This allows remote attackers to execute arbitrary commands without any authentication. Non-PC appliances, such as home routers, provide ideal targets for malware due to their combination of enhanced processing power and lack of security. FortiGuard is currently unaware of any vendor-supplied patch for this vulnerability. In case you own one of these devices, FortiGuard Labs strongly recommends switching to a more secure product.

Web Filtering

eltracom dash gr dot com - This domain contains phishing kits that are downloaded in zip format when an unsuspecting user clicks on links on that site. FortiGuard Labs discovered the threat actor *kckalu15 at yahoo dot* com, who owns a total of 14 domains. We also observed that similar free phishing kit samples are hosted on all of these domains. FortiGuard had previously blocked 3 of these domains, and we have now added the other 11 domains to our blacklist.

unlock dash appleidcloud dot com - We have identified a list of phishing

URLs targeting Apple users. Reverse whois from http://unlock-appleidcloud.com reveals the threat actor to be *hemz underscore 0585 at yahoo dot com,* who also owns 12 other domains created for the same purposes. FortiGuard has blacklisted all of these domains.

Threat Research & Insights

Wild RATs - FortiGuard Labs found a new variant of KONNI, a RAT first discovered in May of 2017, but which has probably been active for a longer time. Read More

Back to Locky - FortiGuard Labs found a new strain of the infamous Locky ransomware in the wild during the past week. Read More

---

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