View this article on online

Activity Summary -- Week Ending June 30, 2017

After the breakout of WannaCry in May, it was just a matter of time before the next big cyber threat would hit. And like clockwork, there it is: Petya, also called NotPetya (or even Nyetya) is a new malware variant that Fortinet has named a ransomworm. It has the attention of the world's press, and is creating havoc all over the world.

The primary victims of this attack seem to be large companies in Europe and in the United States, with the highest number of infections, including critical infrastructure, happening in Ukraine.

If you are interested in a more technical analysis of this new strain of malware, you can find more information in the *Threat Research & Insights* section and the *Malware Activity* section.

Malware Activity

Rank	Name	Volume
1	*JS/Nemucod.DDR!tr.dldr*	*560,099*
2	*W32/Frauder.VA!tr.bdr*	*406,608*
3	*W32/Farfli.BGG!tr*	*377,886*
4	*W32/BackDoor.Prosiak.65*	*126,857*
5	*W32/Genome.XJN!tr*	*68,613*

Petya Ransomware outbreaks- Petya is a family of encrypting ransomware that was first discovered in 2016 that propagated via infected e-mail attachments. Last week, a new variant of Petya, also known as NotPetya, Petna, Petrwrap, and even Nyetya, was used for a global cyberattack, which was the second major global ransomware attack in the past two months. The new variant combines ransomware with the behaviors of a worm by propagating via the NSA's EternalBlue exploit. This same exploit was used last month by the WannaCry ransomware, which also had worm characteristics. As a result, Fortinet has designated these new malware hybrids as ransomworms.

Petya encrypted and locked thousands of computers running Microsoft Windows-based systems. Petya resembles a previous malware strain that utilized a payload to infect the computer's master boot record overwriting the Windows bootloader, and then triggering a restart. On the next startup, Petya's payload, which encrypts the Master File Table of the NTFS file system, is executed and then displays a ransom message demanding a payment made in Bitcoin. In addition, although it operates like ransomware, the encryption routine was modified so that users may never be able to recover their files. This characteristic, along with other unusual signs such as generating a random infection ID rather than a unique ID for each specific

infection, reinforces the theory that the main goal of this attack was not intended to be profit, but to damage devices.

FortiGuard Labs has been monitoring this malware carefully since the earliest version of this family was discovered. There is reason to believe that Wannacry and Petya were trial attacks allowing cybercriminals to refine the scale and effectiveness of this new hybrid attack system. We will continue to track the family of ransomworm malware and share our findings with readers as new details come to light.

Application Vulnerabilities / IPS

Rank	Name	Volume
1	Backdoor.DoublePulsar	81,979,562
2	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	55,339,152
3	MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure	49,479,556
4	TCP.Split.Handshake	35,465,702
5	HTTP.URI.SQL.Injection	11,793,268

Up until today's report, we have always listed the signatures that generated the highest volume of hits on our FortiGate devices. As a result, however, the results have always been highly skewed towards signatures linked to DDoS attacks. By the very nature of DDoS threats, these signatures create a huge volume of traffic even if used in a relatively low number of attacks.

For this reason, beginning this week, we will display the Top 5 IPS signatures with DDoS signatures filtered for more accuracy.

SMB attacks again -- The signature **MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure** once again made an appearance on our top 10 list. The vulnerability exists due to insufficient input validation in the Microsoft Windows SMBv1 server when handling a crafted SMB request. As a result, a remote attacker can exploit a crafted SMB request to gain unauthorized access to sensitive information. Exploits targeting this vulnerability have been incorporated into a variety of tools and malware, including the infamous WannaCry, and this week's Petya, ransomworms. This vulnerability was fixed by Microsoft in April, so be sure to update your machines to the latest security patch.

Web Filtering

api dash restlet dot com - Xavier Malware is a simple Adware that silently installs other APKs on targeted devices. FortiGuard Labs identified the C2 server, and the reverse whois of the domain revealed that the threat actor owns domains with similar names. All URLs have been added as Malicious Websites.

173212223124 colon 8080 backslash downloads backslash VideoPlay dot apk - FortiGuard Labs has discovered that this URL is associated with

the malicious payload delivered through MMS that tricks victims into installing the spyware OmniRAT. OmniRAT is a multi-platform remote administration tool that is commonly being used to attack Android users. The URL has been added to our blacklist.

Threat Research & Insights

The new global Threat: Petya - After WannaCry, another ransomware/worm hybrid is spreading rapidly around the globe. This research article provides an overview of this new "ransomworm" called Petya. Read More

Petya Technical Analysis - Fortinet has also provided a technical analysis of the new Petya ransomworm. Read More

Google CTF, Part 2 - In this blog, another Google CTF 2017 challenge is solved by the FortiGuard Labs team. Read More

The Fortinet Security Research Brief -- The edition for the month of May is now available. Have a look. Read More

---

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