Weekly Threat Briefs

FortiGuard Threat Intelligence Brief - July 28, 2017

View this article on online

Activity Summary -- Week Ending July 28, 2017

This week has been a bad week for the bad guys and good news for everyone else. Let's begin.

First, a British man, named by authorities as "Daniel K.", pled guilty in a German court last Friday to infecting 1.25 million German routers with the Mirai botnet and causing $2.33 million in damages. Second, police in Beijing arrested 11 members of the gang that operated Fireball, a massive adware campaign that has infected around 250 million computers, including both Windows and Mac OS systems. Fireball is an adware program that is downloaded off the Internet bundled with other free, legitimate software. It is designed to persist on an infected machine and has the ability to spy on its victim's web traffic, execute malicious code, install plugins, and even drop victim's web traffic, execute malicious code, install plugins, and even drop malware. And third, Taylor Huddleston pled guilty on Tuesday to US federal charges of aiding and abetting computer intrusions for intentionally selling his NanoCore RAT tool to hackers. NanoCore RAT is a remote access tool that allows attackers to steal sensitive information from victim's computers, including passwords, email, and instant messages, and can even secretly activate the camera on a targeted computer.

In other news, Adobe has announced the end of life for their widely distributed Flash Media Player. Adobe plans to stop supporting it by 2020. Flash has been plagued with security bugs over its lifetime, and as a result has been a favorite target of cybercriminals. Adobe says that open standards like HTML5, WebGL, and WebAssembly have matured over the past several years and can now be used as a viable alternative to replace the capabilities and functionalities that its Flash plugins had provided.

Malware Activity

Rank	Name	Volume
1	*Android/Qysly.S!tr*	*86,234*
2	*VBS/Agent.PCC!tr.dldr*	*80,684*
3	*Riskware/Asparnet*	*59,477*
4	*JS/Agent.QMG!tr*	*51,058*
5	*Riskware/NetFilter*	*36,931*

Android Qysly on the top -- Qysly, also known as Ztorg, is a large family of Android malware that was first discovered in April 2015. It is a malicious Android app used to interrupt the normal operations of Android devices and gain access to the private information stored on them. This malicious app can seize control of a user's SMS messaging system either through exploits or by tricking users to provide permissions through seemingly unrelated requests. Like most Android malware, initial Qysly trojans leveraged Adware to generate money for the bad guys through legitimate advertising networks.

Once the initial app is installed, it utilizes a wide range of advanced techniques to evade detection, collects information about the system, and communicates with a Command and Control server. The server responds with files that enable the malware to gain root access to the device, after with files that enable the malware to gain root access to the device, after which criminals have the freedom to do whatever they want. It also kills running processes on the device and is capable of creating shortcuts on the infected phone. The campaign downloads, installs, and launches Android application from that remote server.

Ztorg also spreads through ads. Clicking on an infected banner can result in the app being automatically downloaded and installed. Most malvertising banners do not link directly to the app download page, but rather take users to a page that redirects to another page, which redirects to another page, and then to another page. To avoid detection, the app can delay downloading malicious files from the C&C server for up to 90 minutes, which is long enough for many testers to decide that the app isn't doing anything malicious.

FortiGuard Labs has been monitoring this malware carefully since the earliest version of this family was discovered in 2015. Just this past week, this family climbed to the top place of our threat charts. 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	*NTP.Monlist.Command.DoS*	*6,238,430,213*
2	*BlackNurse.ICMP.Type.3.Code.3.Flood.DoS*	*1,830,493,788*
3	*DNS.Invalid.Opcode*	*1,226,169,745*
4	*SNMP.v1.Spec.Violation*	*357,097,950*
5	*IPv4.Invalid.Datagram.Size*	*168,442,411*

SMNP vulnerability continues -- the SMNP vulnerability that was the most popular this week was the one detected by the signature SNMP.v1.Spec.Violation. This signature indicates an SNMP version 1 protocol anomaly by detecting a malformed SNMP packet. SNMP uses Abstract Syntax Notation One (ASN.1) for message encoding. ASN.1 uses Basic Encoding Rules (BER) and Tag-Length-Value (TLV) streams to represent data. Only a portion of BER is used for SNMP packets, and each component can assume only a limited set of values. If any of these restrictions are violated, it is considered to be a malformed SNMP version 1 packet. If your systems are repeatedly detecting this signature, it could be a sign of suspicious activity, and we suggest that you switch to version 2c or 3 of that management protocol.

Web Filtering

besic dash cn dot com - FortiGuard Labs discovered several domains associated with the Pony Malware. These domains are used to host the Pony panel to deliver a malicious payload. This malicious payload is detected by Fortinet as **W32/Agent.NTM!tr**. We saw a spike in one of the domains, **besic dash cn dot com**, which had a visit count of 12.5K on 6th July 2017. The domain had been blacklisted before the spike occurred, and we have blacklisted all related domains.

security dash alert dot hihugxkfn dot bid - FortiGuard Labs has identified this domain as a fake alert scam site. Reverse whois reveals the Threat Actor as **certa at fartumas dot com,** which owns 907 other domains, all of which had been recently created in 2017. FortiGuard has blacklisted all the domains.