Weekly Threat Briefs

FortiGuard Threat Intelligence Brief - November 03, 2017

View this article on online

Activity Summary -- Week Ending November 3, 2017

After a few months of apparent inactivity, the Sage ransomware family resurfaced this past week with a new variant. While the encryption routine did not change (meaning it still belongs to the v2.2 release that first appeared in March 2017) this new campaign sports new evasion and obfuscation techniques to make it harder to detect and stop. These include anti-VM, anti-sandbox, anti-analysis, and privilege escalation. If you want to know more about this new campaign, head down to the *Threat Research & Insights Sectio*n to find a link to our recent blog that digs into this new variant in detail.

Malware Activity

Rank	Name	Volume
1	*LNK/Agent.AG!tr.dldr*	*237,546*
2	*W32/GenKryptik.ARNZ!tr*	*225,859*
3	*LNK/Agent.7346!tr.dldr*	*150,329*
4	*MSWord/DDE.7E29!tr*	*90,700*
5	*Riskware/NetFilter*	*88,081*

Pushdo botnet continues -- Also known as the Cutwail or Pandex botnet, Pushdo is the name given to the botnet's main malware binaries, and was first issued ten years ago. Pushdo is essentially an advanced downloader that first infects a targeted system and then downloads the Cutwail spam module (also owned by the same criminal gang). The bots connect directly to their command and control server to receive instructions about the emails they should collect and send.

After they have completed their task, the bots report exact statistics on the number of emails that were delivered back to the spammer, as well as which and how many errors were reported. This campaign also functions as a DDoS botnet that can be used to launch attacks on SSL encrypted websites. The botnet thread sends thousands of malformed SSL connections to SSL port 443 on the victim's website in a very short time. The server responds with SSL negotiation errors and eventually gets exhausted.

FortiGuard Labs has been tracking Pushdo since it was first discovered. This botnet campaign is once again climbing our malware list. During our tracking late last week, it triggered approximately 5,000 sensor triggers with 1.3 million hits. The United States leads in the number of detections, but we've also seen some surprising activity in Taiwan and Japan. 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*	*64,166,853*
2	*Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass*	*43,949,609*
3	*MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure*	*32,327,000*
4	*Backdoor.DoublePulsar*	*30,096,993*
5	*Apache.Struts.Jakarta.Multipart.Parser.Code.Execution*	*7,519,182*

Drop your masq -- This week we saw an increase in the detection frequency of the signature **Dnsmasq.add_resource_record.Heap.Overflow**, which identifies attempts to exploit a vulnerability in dnsmasq, an open source software that provides DNS forwarding, DHCP server router advertisement, and network boot features for small networks. It is included in most Linux distributions and Android systems, in addition to multiple IoT devices. The vulnerability (CVE-2017-14491), which affects Dnsmasq versions prior to 2.78, is due to an error that occurs when the software receives a malformed DNS response. A remote attacker may be able to exploit this to execute arbitrary code within the context of the application. The developer released a fix for this vulnerability, which can be downloaded from the official site. We strongly recommend that users running Dnsmasq versions prior to 2.78 upgrade to a patched version of the software

2010: A Microsoft Odyssey - This week we also registered a high number of detections for **MS.Communicator.SIP.Invite.DoS**. This signature detects an attack attempt to exploit a Denial of Service vulnerability in Microsoft Office 2010 beta. The vulnerability is a result of the application's failure to properly sanitize user-supplied inputs, which then allows remote attackers to cause a denial of service (memory consumption) via a large number of SIP INVITE requests. The signature detects for 100 requests within 5 seconds. It is an old vulnerability that affects old products, but as always, you should be sure that your systems are running the latest security patch.

Web Filtering

Mymyetherwallet dot com - FortiGuard Labs has identified this domain as a phishing site targeting MyEtherWallet that attempts to steal a victim's digital wallet. The site tries to appear legitimate by having a secure certificate issued by Let's Encrypt Authority X3, a free and open certificate. We have added the

domain to our blacklist.

95 dot 46 dot 8 dot 51 - FortiGuard Labs has discovered that this URL performs malicious activities. Reviewed from the content, it also includes a number of drive-by-downloads files. We also discovered that some of those malicious files are a Trojan related to cryptocurrency. FortiGuard has blacklisted all the URLs/IPs in our database.

Threat Research & Insights

A Sage once said... - Ransomware Sage 2.2 has resurfaced after being dormant for about 6 months, now adding tricks focused on anti-analysis and privilege escalation. Read More

Follow the Apache - Apache Struts 1 is a popularly used JAVA EE web application framework. We decided to analyze the code behind two vulnerabilities that affect it (CVE-2015-0899 and CVE-2016-1182).

- (https://www.facebook.com/FortiGuard.Labs)