View this article on online

Activity Summary -- Week Ending June 2, 2017

This week the threat actor(s) known as TheShadowBrokers released a cryptographically signed post, in which they announced the start of their "TheShadowBrokers Monthly Dump Service". This is a monthly release of 0-Days that will be sent to whomever is willing to pay them an amount of 100 ZEC (ZCash, an anonymous cryptocurrency), with no distinction between black hats, white hats, corporations or individuals. Right now, 100 ZEC is worth around 21.000, but cryptocurrencies have been increasing in value in the past few months, so the price could be subject to fluctuation.

This situation is creating a big debate within the InfoSec community. What is the right thing to do? On one hand, it is wrong to support criminals like TheShadowBrokers, and there is no way to know if they are going to deliver

TheShadowBrokers, and there is no way to know if they are going to deliver what they are promising. On the other hand, paying a little amount of money could potentially prevent a large scale crisis like WannaCry. The question is not trivial, and the community is torn. The deadline for the payments is the June 6th. Until then, there is no real way to know.

Malware Activity

Rank	Name	Volume
1	*WM/TrojanDownloader.7A51!tr*	*842,415*
2	*WM/Agent.BRC!tr.dldr*	*707,440*
3	*W32/Genome.XJN!tr*	*592,387*
4	*JS/Kryptik.BEN!tr*	*357,984*
5	*Riskware/Asparnet*	*169,834*

Malware spread by macro -- A macro virus is a virus family that is written in a macro language: a programming language that is embedded inside a software application (e.g., a word processor). Some applications, such as Microsoft Office, Excel, and PowerPoint allow macro programs to be embedded within documents. In this way the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread.

Ransomware campaigns are usually distributed through malicious attachments via email that come with a compressed attachment. Inside the attachment, there is a Microsoft Word file. When the victim opens the document, it executes a hidden PowerShell script and attempts to download ransomware. This is the reason we have always suggested our customers to think twice before opening any unexpected Microsoft Office file or script attachments in an email from any unsolicited senders.

FortiGuard Labs has seen a rise in the detection of Microsoft Word macro malware. Two of the top 5 detections this week were Word macro malware. **WM/TrojanDownloader.7A51!tr** had approximately 12,000 sensor triggers this week of which 37.3% were detected from Japan and 34.8% were from the United States. This variant first appeared in 2016 and peaked in the month of April 2017 with 1.7 million hits. **WM/Agent.BRC!tr.dldr** logged close to 11,800 triggers and 707,000 hits. 35.6% were detected from Japan and 31.1% from the United States. The signature was first released on Aug 29.

2016, and did not have too much activity in the recent months until this week. As previously discussed, both of these malicious macros have been observed to download and execute Cerber ransomware.

Application Vulnerabilities / IPS

Rank	Name	Volume
1	NTP.Monlist.Command.DoS	6,733,039,725
2	DNS.Invalid.Opcode	2,463,138,068
3	SNMP.v1.Spec.Violation	2,367,133,827
4	SIPVicious.SIP.Scanner	664,003,494
5	IP.Land	540,524,554

Dahua cameras - In the past few months, IoT security was all the media could talk about. Recently, with the explosion in popularity of ransomware, it seems like IoT threats have ceased completely. However, criminals did not stop trying to obtain access to IoT devices within our homes. This week we saw an increase in the number of triggers for **Dahua.IP.Camera.UnAuthorized.Access**. This signature detects a vulnerability in the web interface of affected Dahua recorders and IP cameras that allows remote attackers to obtain login access by leveraging knowledge of the MD5 admin hash without knowledge of the corresponding password. This vulnerability was discovered in March 2017 and Dahua has released updated firmware to mitigate these vulnerabilities. If you own a Dahua device, we encourage you to check if it is subject to this vulnerability and in case it is, download the updated software from Dahua technical support or an authorized Dahua distributor.

Another SMNP vulnerability attacked - Another vulnerability that was very popular this week was the one detected by the signature **SNMP.v1.Spec.Violation.** This signature indicates an SNMP version 1 protocol anomaly. It indicates detection of 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 a malformed SNMP version 1 packet. If your systems are repeatedly detecting this signature, it could be a

packet. If your systems are repeatedly detecting this signature, it could be a sign of suspicious activity.

Web Filtering

instagram dash security dot net - FortiGuard Labs has discovered a new phishing domain targeting Instagram. The domain was newly created on April 30, 2017. Further investigation shows that the threat actor **alondra dot qeli at outlook dot com** also owns several other social media phishing domains related to Facebook and Snapchat. FortiGuard has blacklisted all of the domains.

thenathedtset dot com and **parutdownbo dot com** - FortiGuard Labs has identified these two sites as Zloader CNC domains in a malspam campaign. Traffic to thenathedtsetcom was first seen on April 17, 2017 and FortiGuard blocked it on the same day. We are still observing an increase in visit traffic to the domain.

Threat Research & Insights

A Spear Phishing fileless attack - *CVE-2017-0199* allows a criminal to attack a system through Microsoft Office and WordPad to take control. We recently detected a suspicious RTF file abusing this vulnerability. Read More

---