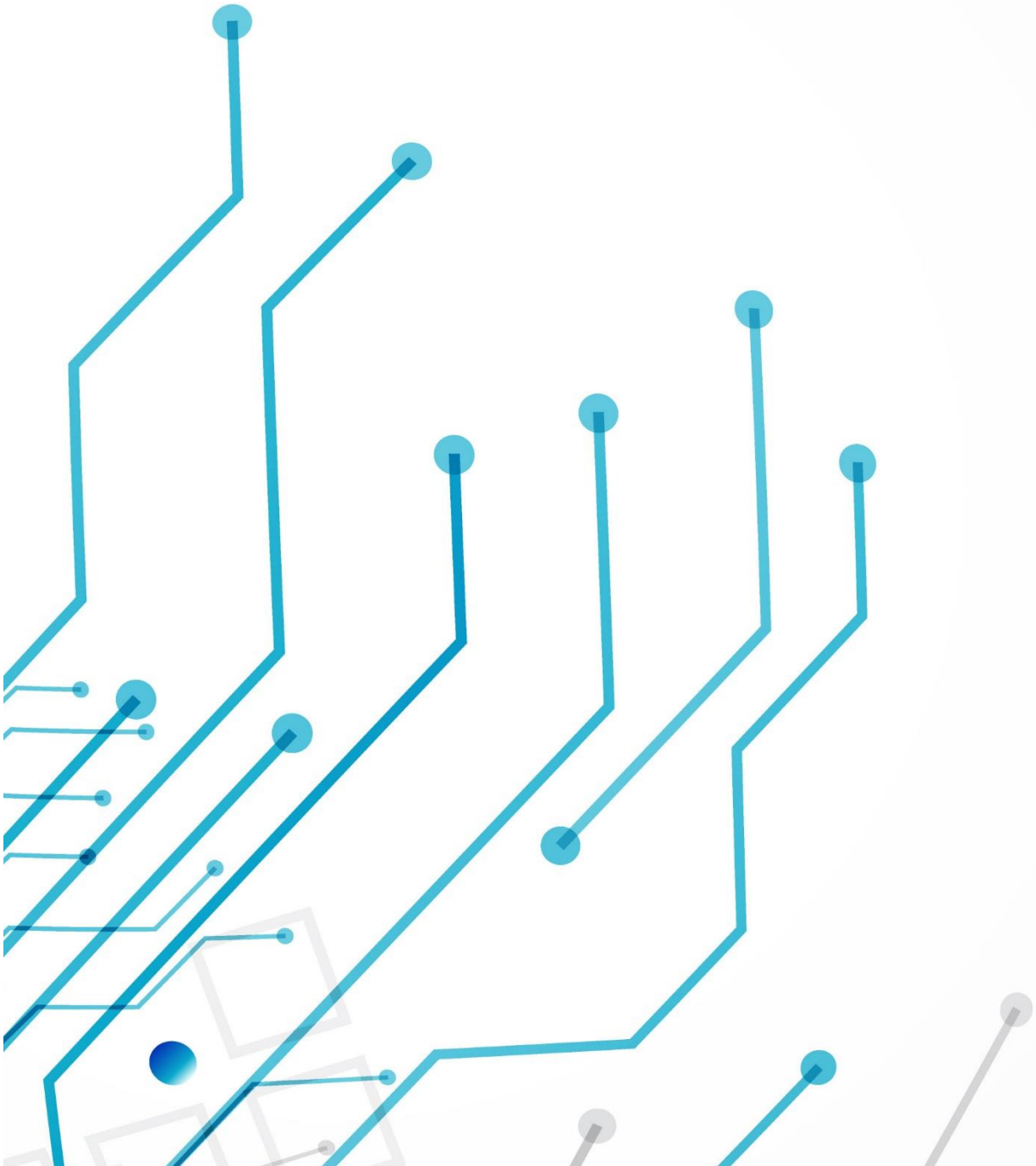
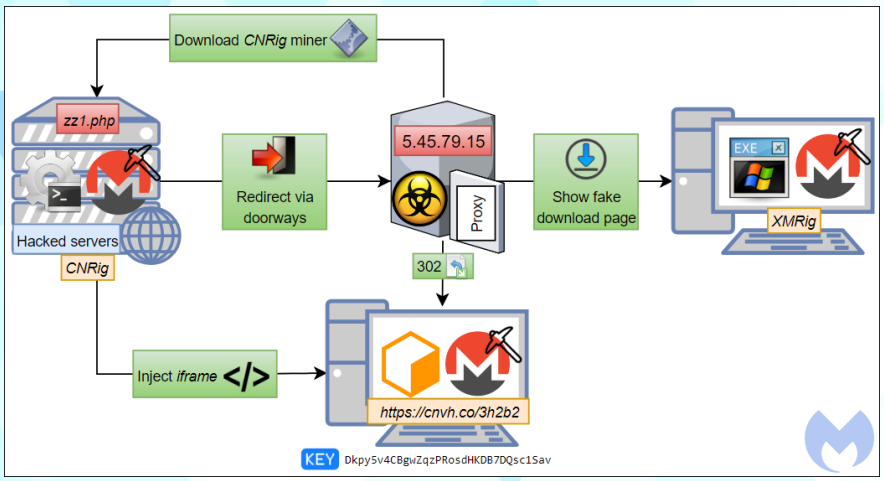
INFOSEC NEWSLETTER

JULY, 2018



1. Secretly Mining Cryptocurrency using CoinHive URL Shortener

CoinHive has become one of the most popular browser based mining service allows owners to embed JavaScript code into their website and user visitor's CPU's power to mine cryptocurrency for monetization. Cybercriminals have been secretly using this service to illegally mine cryptocurrency to make money by injecting their own CoinHive JavaScript code to the hacked website in a large scale.



Malwarebytes security researchers, said that a large number of legitimate website has been hacked to load CoinHive URL hidden inside the HTML Iframe forcing visitors to mine cryptocurrency for the attackers.

To read more about this Click Here.

2. LokiBot : The "Hijacked" Version of Original Malware

Security researcher goes by alias "droot" found that someone made changes in the original LokiBot sample, without having access to its original source code, which allows hacker to define its own custom domain for receiving the stolen data from its victim. The researcher also found the location of the C&C server location of the malware stored at five places in the program – four of them are encrypted using Triple DES algorithm and one using simple XOR cipher.

```
lpMema = (LPVOID)wCheckTokenMebership();
qmemcpy(&v9, &unk_418810, 0x31u);
v3 = get_size(&v9);
registryKey = Decrypt3DESstring(&v9, v3, (int)&unk_418868, (int)&unk_41885C,
v5 = registryKey;
if ( registryKey )
{
  v6 = ge
  v7 = v6;
  if ( v6 )
  {
    wRegSetValue((lpMema != 0) - 0x7FFFFFFF, (int)v6, a2, (int)v2, 0);
    wHeapFree(v7);
  }
```

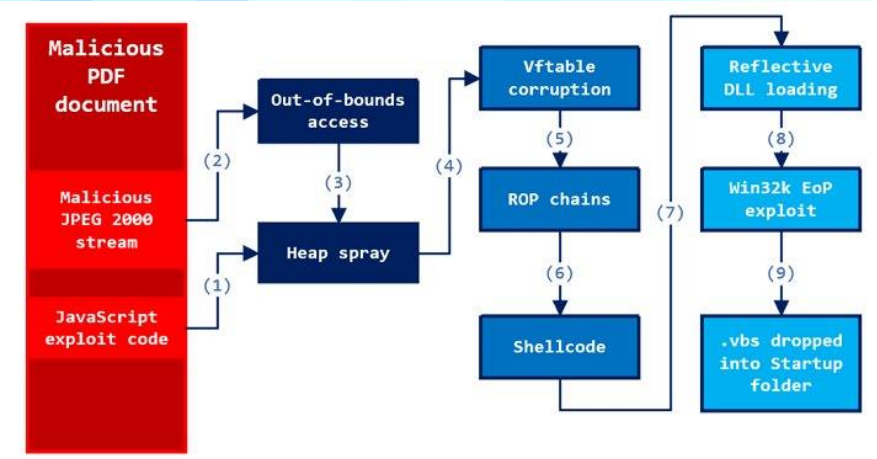
```
char *registryKey; // eax
0x609D48:"http://ipvhosted.duckdns.org:6060/newmarch/fre.php"
```

The malware is has a function "Decrypt3DESstring" to decrypt the encrypted strings and get URL of the C&C server. By using the hex editor anyone with the sample can modify and add their own custom URL for receiving the stolen data.

To read more about this Click Here.

3. Two Zero-Day Exploits Found after "Unarmed" POC Uploaded to VirusTotal

Security researchers at Microsoft discovered that two zero-day where discovered after someone uploaded malicious PDF file to VirusTotal. After analyzing the malicious PDF file, the Microsoft team found that it includes two different zero-day exploits which targeting Adobe Acrobat and Reader and other targeting Microsoft Windows. The team has also said that the malicious PDF was in the early stage of development, could not deliver the malicious payload and appeared to be a proof-of-concept (poc) code. Someone has combined both the zero-days exploit to build an extremely powerful cyber weapon and mistakenly uploading his/her development to VirusTotal.



The zero-day vulnerabilities in question are a remote code execution flaw in Adobe Acrobat and Reader (CVE-2018-4990) and a privilege escalation bug in Microsoft Windows (CVE-2018-8120).

To read more about this Click Here.

4. Facebook Quiz App Exposed Data of 120 Million Users

Facebook was again in controversies when a third-party quiz app called NameTests, found exposing data of 120 million Facebook users to anyone who finds it. NameTests.com, the website popular social quizzes like "Which Disney Princess are You?" having 120 million monthly users, which uses facebook's platform to signup fast into the website. A bug bounty hunter by the name "Inti De Ceukelaire" found that the popular qui website is leaking logged-in user data to other websites opened in the same website.

As a proof of concept, Ceukelaire developed a malicious website that would connect to NameTests to mine the data of visitors using the app. Using a simple bit of code, he was able to harvest the names, photos, posts, pictures, and friends lists of anyone taking part in the quiz.

To Read More about this: Click Here.

5. Microsoft Tuesday Patch July 2018

This month's update covers vulnerabilities in:-

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office and Microsoft Office
- Services and Web Apps
- ChakraCore
- Adobe Flash Player
- .NET Framework
- ASP.NET
- Microsoft Research JavaScript Cryptography Library
- Skype for Business and Microsoft Lync
- Visual Studio
- Microsoft Wireless Display Adapter V2 Software
- PowerShell Editor Services
- PowerShell Extension for Visual Studio Code
- Web Customizations for Active Directory Federation Services

Software Patches Download List:-

- ADV170017
- ADV180002
- ADV180012
- ADV180016
- ADV180017
- CVE-2018-8260
- CVE-2018-8281
- CVE-2018-8282
- CVE-2018-8289
- CVE-2018-8297
- CVE-2018-8299
- CVE-2018-8300
- CVE-2018-8305
- CVE-2018-8306
- CVE-2018-8310
- CVE-2018-8312
- CVE-2018-8323
- CVE-2018-8324
- CVE-2018-8325
- CVE-2018-8326
- CVE-2018-8327

Known Issues:-

- 4338825
- 4338818

To Know More: Click Here

6. Ticketmaster Suffers Security Breach

Global entertainment ticketing service Ticketmaster has admitted that the company has suffered a security breach, warning customers that their personal and payment information may have been accessed by unknown third-party. The company has accused the third-party support customer service chat application for the data breach affecting thousands of its customers.

The third-party which provides chat customer chat supported application, made by Inbenta Technologies – a third party artificial intelligence tech supplier used to help major website to interact with their customers. Ticketmaster has disabled the Inbenta products across all of its websites after the discovery of malicious software on the customer support application hosted on its UK website allows to extract the personal and payment information from its customers.

Ticketmaster said that it has emailed all affected customers, and is offering 12 months of free identity monitoring service for those who have been impacted.

7. Unpatched WordPress flaw Gives Attacker Full Access

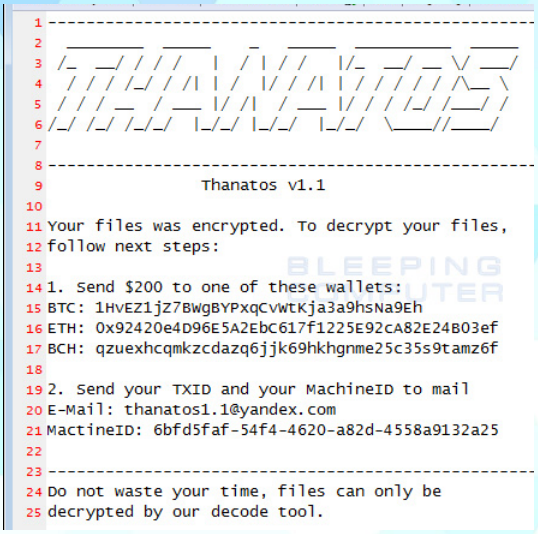
WordPress has released new version 4.9.7, to patch this vulnerability that could allow remote attackers to gain full control over the affected website. Researchers at RIPS Technologies GmbH, the authenticated arbitrary file deletion was reported 7 months ago to WordPress but remains unpatched and affected all versions of WordPress, including the current 4.9.6. The vulnerability resides in one of the code functions of WordPress that runs in the background when and user permanently deletes thumbnail of the uploaded image.

The delete function accepts unsanitized user input, which if tempered, could allow users to delete any file from the web hosting. If the attackers deletes the “wp-config.php” file from the server, which contains important configuration related to WordPress installation, forcing the website back to installation screen and attacker can reconfigure the website to take full control.

Video PoC: YouTube.

8. Thanatos Ransomware Decryption Tool Released

Security Researcher at Cisco Talos have discovered a weakness in the Thanatos ransomware code that makes it possible for the victim to unlock or decrypt their files for free without paying any ransom in cryptocurrency.



If the computer is infected, all the encrypted filename extensions on the affected computer are changed to ".THANATOS" and then a ransom note pop up to the logged in user with the instructions to send ransom money to a cryptocurrency wallet address in order to decrypt the files. The tool has been dubbed as **ThanatosDecrypter**, the open source, free ransomware decryption tool which can be downloaded from the GitHub website.

To protect from such ransomware, you should be always suspicious of uninvited documents send in an email and never click on links inside the documents unless you have verified the sources. Block macros from running in MS Office files from internet. Always keep a backup of the important documents on a routine basics to an external storage which is not always connected to the computer. Keep the anti-virus updated and run an active scan of the entire system on routine basics.

9. Timehop Hacked – 21 Million Users Data Stolen

Timehop is a social media app that has been hit by data breach on July 4th that lead to compromise of personal data for more than 21 million users. It is an app that collects old photos from iPhone, Facebook, Instagram and Twitter and helps you to find what you were doing on that very day a year ago.

Hackers had also stolen authorization token keys provided by the respective social media sites allowing them to access social media posts and images without your permission. The company also said that the stolen token has been made invalid and deauthorized as soon as the company has detected the breach on its network.

Timehop was not using two-factor authentication, the attacker were able to gain access to its servers using the compromised credentials.

Timehop after the data breach logged out all its users of the app as the company invalidated the API credentials, users have to re-authenticate and generate a new token for their social media accounts.