Hunting Like Indiana Jones

*S.Dharshan*

*185001044*

1. Fitting through the MITRE template for the given link: -

**Description:** CollectorGoomba(Collector Project) steals sensitive data from the infected computer. It reads sensitive data from the user’s web browser including their web cookies, personal information, and even login details. It targets the data files of Google Chrome, Firefox, and Internet Explorer.

**Type:** spyware

**Target geolocations:** Any (mostly originated from Germany,

Russia)

**Target data:** login details and personal information

**Target businesses:** Any

**Initial access:** Executable file by user, social engineering attacks

**Exploits:** CVE-2018-14560

**Persistence:** Registry Run Keys

**Evasion:** Biweekly changes in the spyware destination host

**Collection:** web cookies, login details, saved passwords.

**Exfiltration:** Exfiltration over Command and Control channel

2. The patterns and connections between the file hashes and the domain sites are as follows: -

The most common pattern was that all these hashes were mostly from a single ip address 185.22.155.62

Or the file hashes were from IP addresses which were having the firs 3 numbers as 185.22.155 and this family of IP addresses usually generates from Russia (Russian Federation)

When one of the active sha 256 values which was:

49a56e067a73bb6f553b8df8a354d3b3328b8fffb64a459a1e719d86df89a322

The following threats appeared: -

* Checks disk space, network adapters
* Direct CPU Clock access
* invalid rich pe linker version
* invalid signature
* overlay, peexe, runtime modules, signed
* The md5 value was 70e863fb5753b95b4bb7d8c746ae4b94.virus which contains the word “virus” itself.

Found in C2 Infrastructure checking:

|  |  |
| --- | --- |
| Domain Name | Remarks |
| raw[.]githubusercontent[.]com/fkarelli/fjrusbftnf/maste r/nyun[.]txt | 151.101.128. 133 ==> 404 not found |
| u7320947p3[.]ha0004[.]t[.]justns[.]ru/collect[.]php | Detected as **phishing and malware repository** |
| u667503srd[.]ha004[.]t[.]justns[.]ru/collect[.]php |  |
| u667503gif[.]ha004[.]t[.]justns[.]ru/collect[.]php | not found |
| u640763aha[.]ha004[.]t[.]justns[.]ru/collect[.]php | **Phishing and malware** |
| 185[.]22[.]155[.]51 (observed hosting collect.php,  April 2020 - June 2020) | 200 status |

The common IP address of 185.22.155.62 is observed in 2 collect.php files.

And 2 of the domains act as the repository to collect the phishing data.

3. Connection among the given connections: -

File Names:

1. => ajtDr.exe
2. => COPY.rar
3. => content.27640.2501.28169.6540.28790
4. =>a55d1c36f3d5ba85a951e75b6a5de7a350d133ad49a44ddce349d5d181e64ae8
5. => Swift copy.exe
6. => tlBHy.exe
7. => confirm.exe

The Files connecting to the given domains

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Domain Name | A | B | C | D | E | F | G |
| www[.]paintwithdrink[.]com | Y | Y |  | Y |  | Y | Y |  |
| www[.]technicalworld[.]online | Y | Y | Y | Y |  |  |  |  |
| www[.]yilingshenghuo[.]net |  |  | Y | Y |  | Y | Y |  |
| www[.]media0702[.]com |  |  |  |  |  | Y |  |  |
| www[.]focusopgeld[.]com | Y |  |  |  |  | Y |  |  |
| www[.]cjnexgift[.]com | Y | Y | Y |  |  |  |  |  |
| www[.]qduola[.]com | Y | Y | Y |  |  |  |  |  |
| www[.]dytt889[.]com | Y |  |  |  | Y | Y |  |  |
| www[.]truckingtag[.]com |  |  |  | Y | Y | Y |  |  |
| www[.]officialbetterbeardclub[.]com |  | Y |  |  | Y | Y |  |  |
| www[.]njssnt[.]com |  |  |  | Y | Y |  |  |  |
| www[.]bitechanalytics[.]com | Y |  |  | Y |  |  |  |  |
| www[.]starbuckranchtx[.]com | Y |  |  |  |  | Y | Y |  |
| www[.]thelifewaykefir[.]com | Y |  | Y |  | Y |  |  |  |
| www[.]hillsidesunshine[.]com |  | Y |  |  | Y |  |  |  |
| www[.]regulars6.com |  |  |  | Y |  |  | Y |  |

After analysis of each of these files in the legend the following conclusion was drawn: -

* All these files which maybe executable or zip files when checked with virus total and scanners are found to be not a safe file.
* The most common file is “ajtDr.exe” --> This is found in 9 of the domains mentioned.
* The files are detected as Trojan or malware in most of the virus scanners
* The domain www[.]regulars6[.]com has many visible malwares that it has more than 5 virus scanners depicting as an unsafe domain.
* Consider the file ajtDr.exe it as the following signature detected: - o Classification: mal100.troj.evad.winEXE@9/1@3/1 o Threat Name: FormBook
* These files are classified as the following genre in the scanner: - o Detect-debug environment o Assembly level o Direct CPU-clock access o Self-delete o Peexe