NIIT UNIVERSITY, NEEMRANA
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
THREAT INTELLIGENCE LAB

THREAT INTELLIGENCE LAB (CS-5202)

Yara Rule for KPOT

2021-2022

Pradeesh Kumar.R
MT20ACS523

AREA DIRECTOR NAME
Dr. Debashish Sengupta

FACULTY NAME
Dr. Ashu Sharma

Table of Contents

KPOT Stealer

KPOT Stealer is a "stealer" malware written in C/C++ that focuses on exfiltrating account information and other data from web browsers, instant messengers, email, VPN, RDP, FTP, cryptocurrency, and gaming software. It is a high-risk trojan designed to steal various personal information. This malware is typically distributed using fake web browser updaters, however, this trojan was previously distributed using spam email campaigns. Its name is based on the command and control (C&C) panel used in earlier versions of the malware.

The main purpose of KPOT is to gather personal information. To be specific, it targets account credentials saved in various applications (e.g., Skype, Discord, Steam, FTP clients, etc.), web browsing data (cookies, passwords, autofill data), and even cryptowallets (cryptocurrency files). With access to this information, cyber criminals can cause significant issues. Firstly, hijacked accounts might be used to proliferate this malware even further by sending spam. Additionally, cryptocurrency wallets and other accounts might be misused through online purchases, money transfers, borrowing money from the victim's contacts, and so on. Therefore, having KPOT installed can lead to financial loss and even debt. Criminals also attempt to steal FTP credentials. They might gain access to various servers managed or owned by the victim. This can also cause various issues (e.g., data loss, permanently damaged/shutdown websites and servers, etc.). These problems are not only inconvenient, but could also result in financial loss, especially if the damaged website/server is used to generate revenue or serves as a communication/development tool in various companies. In summary, the presence of a high-risk trojan can lead to serious privacy issues (including identity theft), data/financial loss, and other problems.

KPOT Infiltration

KPOT is mostly proliferated using fake browser updaters and spam email campaigns. Fake updaters are promoted through deceptive websites that display pop-up messages. These falsely claim that the web browser is outdated and that the user should update it immediately. These pop-ups also contain an "Update" button, which downloads the malicious updater designed to inject KPOT into the system. Spam campaigns, on the other hand, are used to send hundreds of thousands of emails consisting of malicious attachments (typically, Microsoft Office documents or PDF files), and messages encouraging users to open them. Criminals are also likely to present malicious attachments as important documents (e.g., receipts, invoices, etc.). This is done to give the impression of legitimacy and increase the chance of tricking users into opening the files. Trojans are often proliferated using fake software 'cracks', third party software download sources (free file hosting websites, freeware download websites, Peer-to-Peer [P2P] networks, and similar), and other trojans (chain infections).

```
KPOT v2.0 update:
Soft:
1.1) Added the ability to grabbing files across the entire disk and over the network.
1.2) The storage structure in the grabber was revised. Now all the files are divided into folders as they were in the directory fro
m which the collection was.
2) Added to the RDP collection from the user folder for all users from which it is possible to collect.
3) Reworked collection from Windows storage (Credentials and Protected Storage). Now collects all the data pack without filtering
on any particular, i.e. if the software meets data of an unknown type without encryption, it will collect it in its pure form, if t
hey
will be encrypted, it will collect, but will not benefit from them.
4) Added collection of programs in the system information. Gathers the name and version of the installed program.
Both x64 and x86 programs are compiled.
5) Added Outlook collection from the registry for all users from which it is possible to collect.
6) Improved resolv .bit domains. All the workpieces I found at the time of adding dns for a resolver, as well as the dotbit proxy,
were added.
...
Current price: $ 85
Installation of the admin: $ 25 (the guide has been redone, now the installation is described much more clearly).
```

Figure 1: Portion of a Russian forum advertisement describing changes in KPOT v2.0 and its price

KPOT has been observed in a variety of email campaigns. For example, the following message shared tactics, techniques, and procedures (TTPs) with campaigns delivering another malware family, Agent Tesla, from similar documents and the same payload domain.

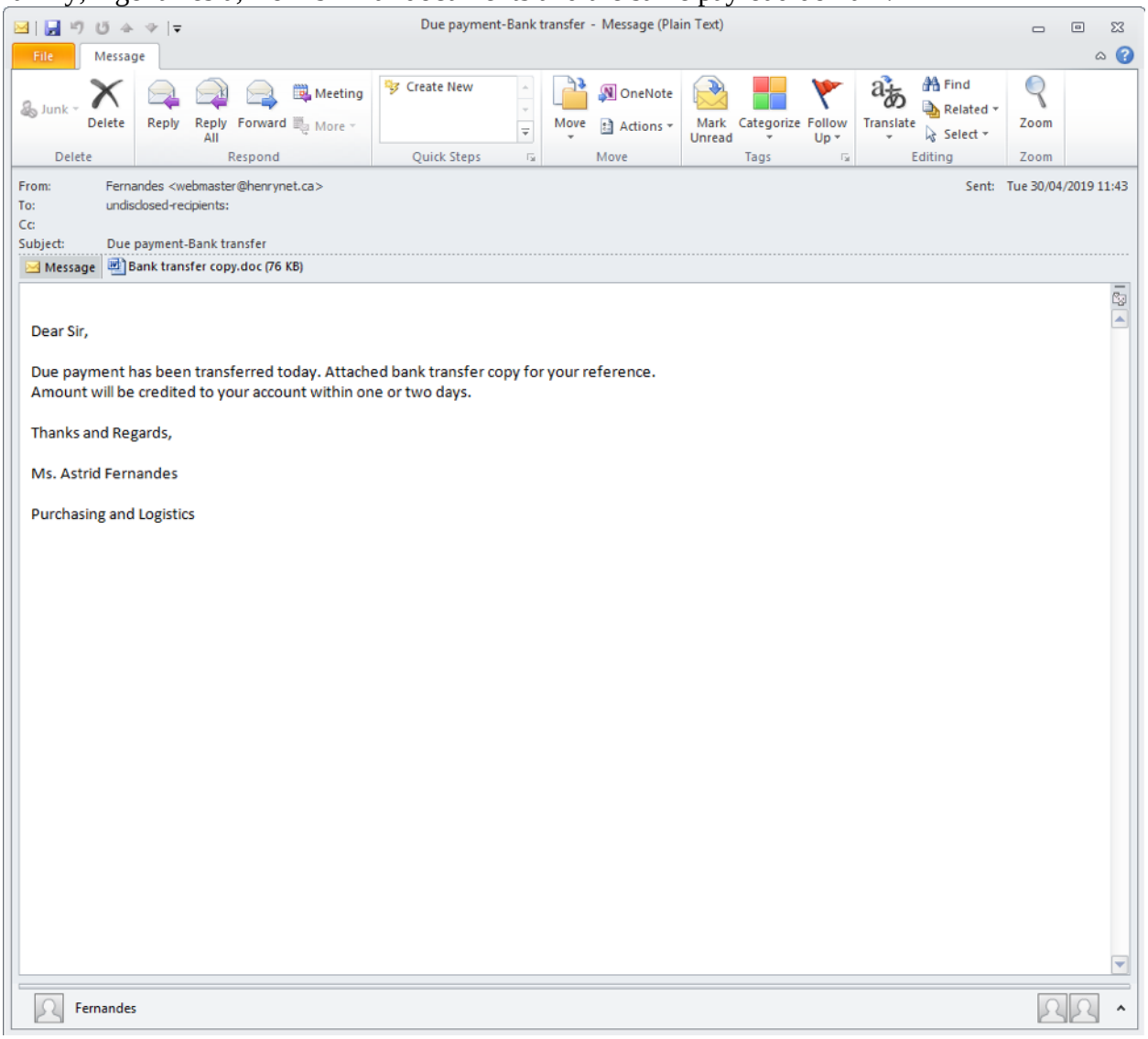

Figure 2: Email message for the KPOT campaign

In this example, the attachment was an LCG Kit [6] variant RTF document which uses Equation Editor exploit CVE-2017-11882 to download an intermediate downloader via a bit.ly link:
hxxps://bit[.]ly/2GK79A4 -> hxxp://internetowe[.]center/get/udeme.png

The downloader, in turn, fetches parts of a PowerShell script that includes the Base64-encoded payload from the various paste.ee links:
hxxps://paste[.]ee/r/BZVbl (PowerShell script segment including an accompanying binary used for reflective DLL injection)
hxxps://paste[.]ee/r/mbQ6R (base64-encoded payload)
hxxps://paste[.]ee/r/OsQra (tail of the PowerShell script)

The payload is KPOT Stealer with configuration:

C2: hxxp://5.188.60[.]131/a6Y5Qy3cF1sOmOKQ/gate.php
XOR key: Adx1zBXByhrzmq1e

Threat Summary

Name	KPOT Trojan
Threat Type	Trojan, Password-stealing virus, Banking malware, Spyware
Symptoms	Trojans are designed to stealthily infiltrate the victim's computer and remain silent, and thus no particular symptoms are clearly visible on an infected machine.
Distribution Methods	Infected email attachments, malicious online advertisements, social engineering, software 'cracks'.
Damage	Stolen banking information, passwords, identity theft, victim's computer added to a botnet.

Malware Selected

Malware Sample Name: 2018-05-KPOT
Sample Location: malware-samples/2018-05-KPOT at master · InQuest/malware-samples · GitHub
Files Present:

- 36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce
- 67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d

Yara Rule

```
rule lab3exe
{
meta:
        Description = "Simple YARA rule to detect 2018-05-KPOT"
        Author = "Pradeesh Kumar.R (MT20ACS523)"
        Date = "2021-08-31"

strings:
        $str01 = "http://%s"
        $str02 = "https://%S/a/%S" wide
        $str03 = "HTTP Server URL" wide
        $str04 = "password-check"
        $str05 = "*.wallet" wide
        $str06 = "*.rdp" wide

        $sr01 = "9087654356.exe" wide
        $sr02 = "PowerShell"

        $reg01 = /(SMTP|POP3|IMAP)\s(User|Password|Port|Server)/ wide
        $reg02 = /(HttpWeb|Web|Get)(Request|Response|Client)/

condition:
```

```
        all of ($str*)
        or all of ($sr*)
        and 1 of ($reg*)
}
```

Description of Yara Patterns

- $str01 and $str02 references a URL pattern in http and https
- $str03 references HTTP Server URL
- $str04 references to checking passwords
- $str05 references to .WALLET file belongs to the category of Data Files used in operating systems such as Windows 11, 10, Windows 7, Windows 8 / 8.1, Windows Vista, Windows XP. A WALLET file is a file encrypted by the CryptoMix, or CrypMix, virus, which is ransomware utilized by cybercriminals. It contains a user's file, such as a . PDF or . DOCX file, encrypted with AES encryption by the virus.
- $str06 references to RDP files mostly belong to Remote Desktop Connection by Microsoft Corporation. An .RDP file contains all of the information for a connection to a terminal server, including the options settings that were configured when the file was saved.
- $sr01 references a malicious exe file present in the sample
- $sr02 references a downloader that fetches parts of a PowerShell script that includes the Base64-encoded payload from the various links
- $reg01 references to username, password, port 587 (SMTP – sending mails), 995 (POP3 – receiving mails) and 143 (IMAP - to retrieve email messages from a mail server) and server
- $reg02 references to request and respond data from a host server

Github Repository Location

CS-5202-Threat-intelligence/Lab3 at main · PradeeshKumar-NIIT/CS-5202-Threat-intelligence (github.com)

Conclusion

The malware is statically analyzed and yara rules has been created for the selected (KPOT V2) malware.

References

[1] Free Automated Malware Analysis Service - powered by Falcon Sandbox - Viewing online file analysis results for '36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce' (hybrid-analysis.com)

[2] Free Automated Malware Analysis Service - powered by Falcon Sandbox - Viewing online file analysis results for '67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d' (hybrid-analysis.com)

[3] https://www.virustotal.com/gui/file/36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce/detection
[4] https://www.virustotal.com/gui/file/67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d/detection
[5] Use Ghidra to decrypt strings of KpotStealer malware – nullteilerfrei
[6] Sha256: 36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce - AlienVault - Open Threat Exchange
[7] Sha256: 67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d - AlienVault - Open Threat Exchange
[8] New KPOT v2.0 stealer brings zero persistence and in-memory features to silently steal credentials | Proofpoint
[9] How to remove KPOT Stealer - virus removal instructions (updated) (pcrisk.com)
[10] yara-rules/KPOT_v2.yara at master · deadbits/yara-rules · GitHub