New KPOT v2.0 stealer brings zero persistence and in-memory features to silently steal credentials

MAY 09, 2019 | DENNIS SCHWARZ AND THE PROOFPOINT THREAT INSIGHT TEAM

Overview

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.

Proofpoint researchers started seeing KPOT Stealer distributed via email campaigns and exploit kits in August 2018 (Figure 1). In addition, colleagues at Flashpoint Intel observed the malware targeting users of the Jaxx cryptocurrency wallet in September 2018 [8].

Clusters	Tags	Date
Fallout	exploit-kit Fallout TheGreenCoffee Keitaro Malvertising zeropark CAN USA Smokebot KPOT ServHelper UndefinedDrop	2019-05-02
RIG	exploit-kit RIG-v Bikarys Malvertising POL Smokebot AZORult KPOT Brazzzers Amadey AlphaIRCBot	2019-04-04
RIG	exploit-kit RIG-v Bikarys Malvertising USA KPOT	2019-04-05
RIG	exploit-kit RIG-v Ebates Bikarys Keitaro Malvertising USA KPOT	2019-03-25
RIG	exploit-kit RIG-v Ebates Bikarys Keitaro Malvertising adcash FRA GBR KPOT Brazzzers	2019-03-24
Fallout	exploit-kit Fallout Ebates Bikarys Keitaro Malvertising GBR KPOT Brazzzers	2019-03-12
Fallout	exploit-kit Fallout Ebates Bikarys Keitaro Malvertising USA KPOT Brazzzers	2019-03-11
RIG	exploit-kit RIG-v Bikarys Ebates Malvertising USA KPOT Brazzzers	2019-03-03
Fallout	exploit-kit Fallout Ebates Malvertising POL FRA CAN Gozi v2 RM3 10291029JSJUYNHG KPOT	2018-11-22

Figure 1: Exploit kit campaigns distributing KPOT Stealer, November 2018 to May 2019

Recently, actors began delivering a newer version of the malware; this post analyzes one of those campaigns along with the malware itself. This newer version is commercially available as "KPOT v2.0" on various underground hacking forums for around $100 USD (Figure 2).

```
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 2: Portion of a Russian forum advertisement describing changes in KPOT v2.0 and its price (Google translation)

Campaign Analysis

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.

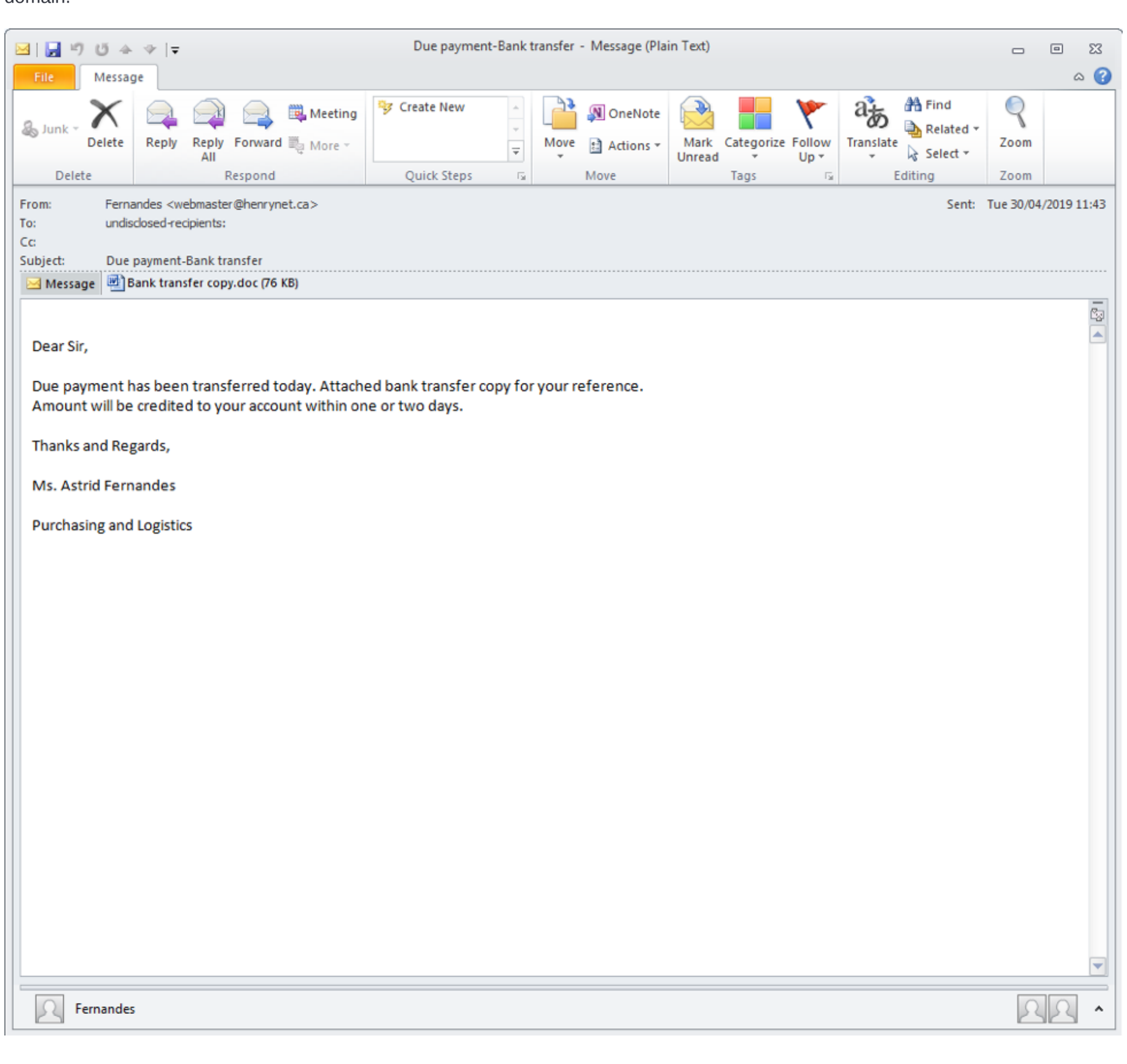

Figure 3: Email message for the KPOT campaign

From: Fernandes <webmaster@henrynet.ca>

Subject: Due payment-Bank transfer

Date: Tue, 30 Apr 2019

Attachment: "Bank transfer copy.doc"

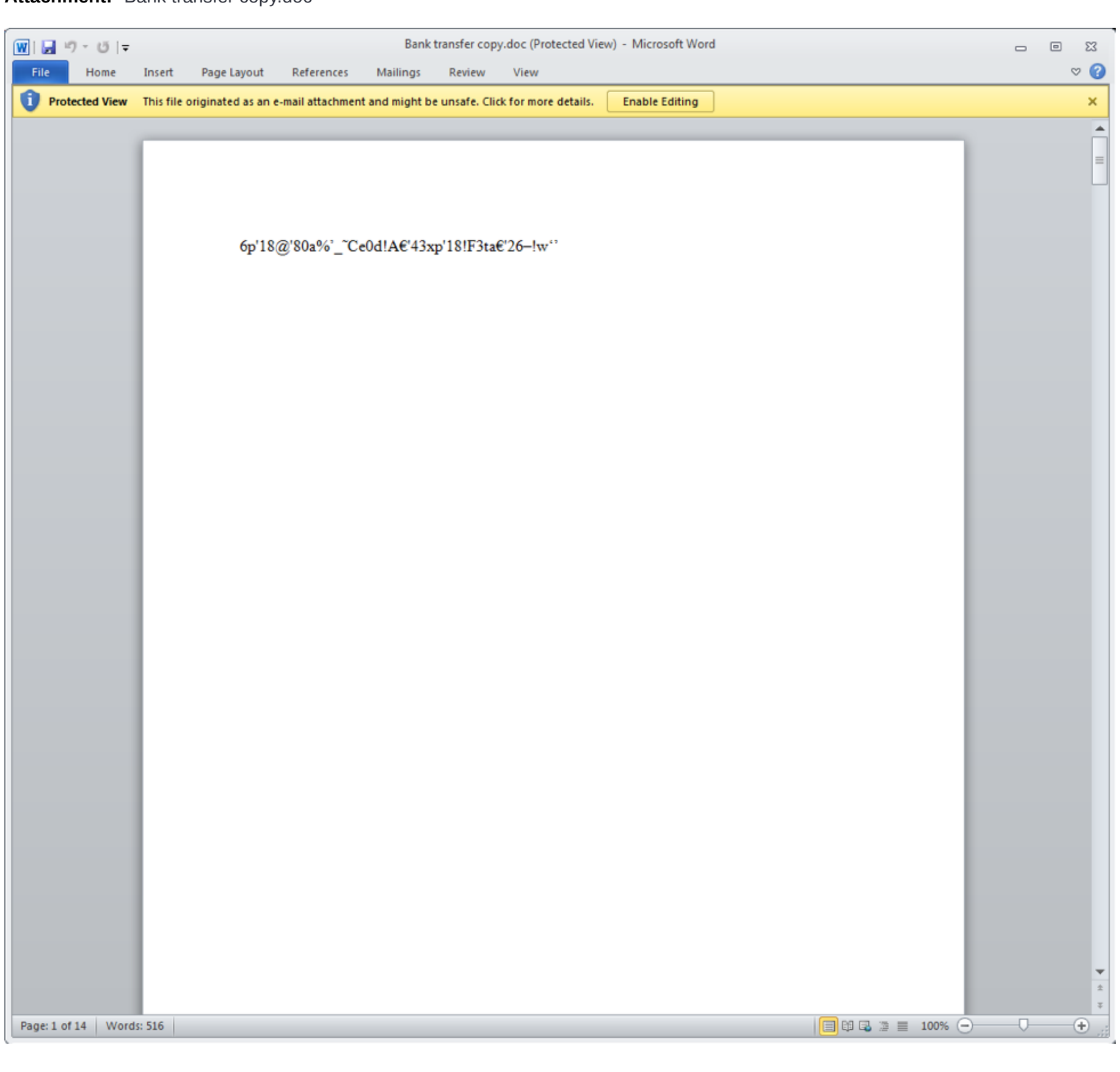

Figure 4: RTF document attachment containing the CVE-2017-11882 exploit (aka Equation Editor)

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
```

Malware Analysis

KPOT Stealer is a "stealer" malware written in C/C++ that focuses on stealing account information and other data from various software applications and services. Its name is based on the command and control (C&C) panel used in earlier versions of the malware (Figure 5):

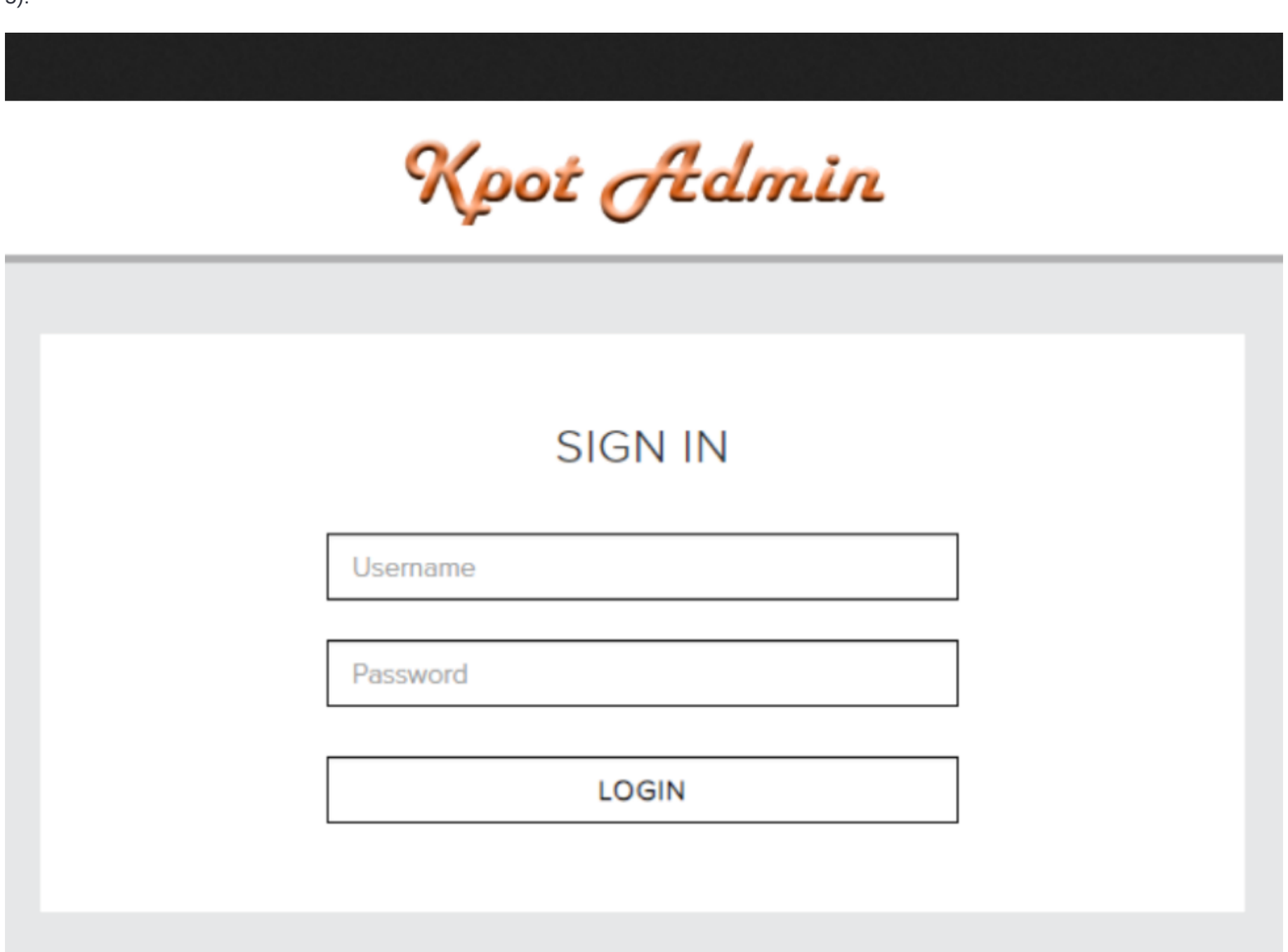

Figure 5: Old KPOT C&C panel login

A screenshot of the C&C panel login for the newer version analyzed in this post is available in Figure 6. As can been seen, the self-identifying mark has been removed.

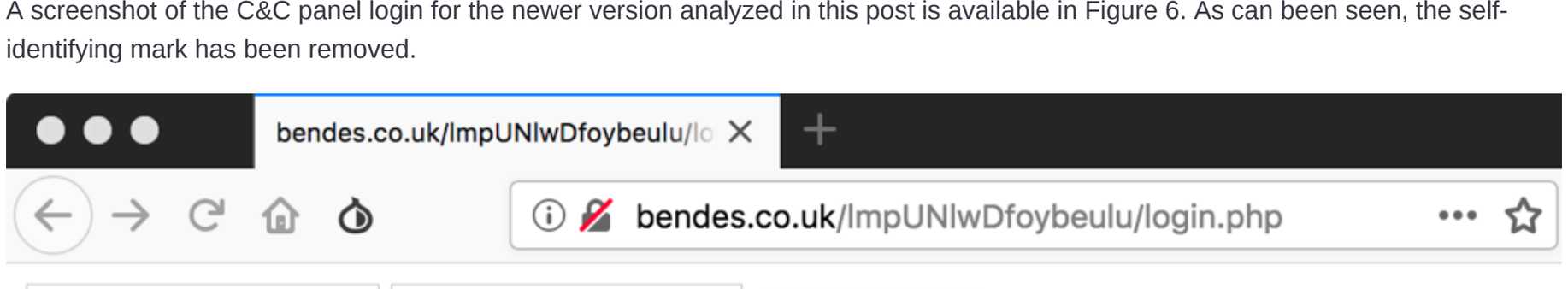

Figure 6: New C&C panel login

Strings

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. [1] is an IDA Python snippet that can be used to decrypt the strings in the analyzed sample and [2] contains a list of the decrypted strings.

Windows API Calls

KPOT Stealer resolves most of the Windows API functions it uses at runtime by hash. The hashing algorithm used is known as MurmurHash [3] and it is seeded with 0x5BCFB733 in the analyzed sample. The following table contains a list of some of the hashes used and their corresponding Windows API name:

0xEC595E53	GetModuleFileNameW
0x68CCF342	CreateStreamOnHGlobal
0xCF724FBB	GetVolumeInformationW
0xB6B1AD4A	InternetOpenW
0x6EAB51D	socket

Command and Control

KPOT uses HTTP for command and control. The URL components are stored as encrypted strings. In the analyzed sample the URL was "hxxp://bendes[.]co[.]uk/lmpUNlwDfoybeulu/gate.php". The malware also has support for .bit C&C domains which are becoming more prevalent.

Two types of requests are sent to the C&C server. The first request is a GET request (Figure 7):

```
GET /lmpUNlwDfoybeulu/gate.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: bendes.co.uk
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 01 May 2019 16:51:37 GMT
Content-Type: text/html
Content-Length: 336
Connection: keep-alive
X-Powered-By: PHP/5.4.16

[redacted]
```

Figure 7: GET request to C&C server

The response from the C&C is base64 encoded and XOR'd with a hardcoded key that is stored as an encrypted string. In the analyzed sample, the key was "4p81GSwBwRrAhCYK". An example of the plaintext response looks like:

1111111111111100__DELIMM__A.B.C.D__DELIMM__appdata__GRABBER__*.log,*.txt,__GRABBER__[appdata][__GRABBER__0__GRABBER__1024__DELIMM__desktop_txt__GRABBER__]*.txt,__GRABBER__[userprofile]%\Desktop__GRABBER__0__GRABBER__150__DELIMM____DELIMM____DELIMM__

The data is delimited by "__DELIMM__" and can be split into the following types of data:

1. A bit string indicating what commands to run
2. The external IP address of the victim
3. "GRABBER rules" specifying what files to search for and exfiltrate

Before any commands are run, the malware checks to see if the victim is located in any of the Commonwealth of Independent States (CIS) [5]. If it is, the malware exits without further action. The specific languages it checks for can be seen in Figure 8:

```
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
}
```

Figure 8: Commonwealth of Independent States (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 [7].

After the commands are run, a POST request is sent to the C&C (Figure 9):

```
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

[redacted]
```

Figure 9: POST request to C&C server

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_". Sections include:

- 62-byte structure containing:
  - Is process token elevated
  - Process integrity level
  - Windows version
  - Locale
  - Bot ID
- Additional system information including:
  - Windows version
  - Machine GUID
  - External IP
  - CPU
  - RAM
  - Screen
  - Computer name
  - User name
  - Local time
  - GPU
  - Keyboard layouts
  - Installed software
- Command outputs
- Exfiltrated files

Commands and Functionality

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 (Figure 10). This feature was also highlighted in an earlier version by a security researcher on Twitter [4].

```
[bot]
chromium = 1
mozilla = 1
wininetCookies = 1
crypto = 1
skype = 1
telegram = 1
discord = 1
battlenet = 1
iexplore = 1
steam = 1
screenshot = 1
ftp = 1
credentials = 1
jabber = 1
exeDelete = 0
dllDelete = 0
```

Figure 10: Command bit string to command name mapping

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

Although there aren't specific command bits controlling the functionality, 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. "Rules" specifying what files to search for can be delivered in the above GET response. Each rule has five components delimited by "__GRABBER__". The components include:

1. Rule name
2. File mask (comma separated)
3. Search path
4. Minimum file size
5. Maximum file size

An example rule split up into its components looks like:

['appdata', '*.log,*.txt,', '[appdata]%', '0', '1024']

This rule is called "appdata" and looks for any ".log" or ".txt" files in "[APPDATA]" that are between 0 and 1024 bytes.

The analyzed sample lacks a persistence mechanism. 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. This has been seen in other stealer malware such as Pony since it lowers their chance of being detected.

Conclusion

Client desktop operating systems running many types of applications, such as web browsers, instant messengers, email, VPN, RDP, FTP, cryptocurrency, and gaming software are increasingly being targeted for credential and other data theft by relatively quiet off-the-shelf malware such as KPOT Stealer through email campaigns (and more infrequently, exploit kits). The commercial nature of these tools means that sophisticated capabilities are accessible to even technically unskilled criminals and highlight the ease with which threat actors can get started and change tools and tactics. We advise our customers to remain vigilant in terms of securing their client systems with the latest vendor patches, platform updates, and improving general awareness of social engineering techniques within their respective user populations.

References

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

[2] https://github.com/EmergingThreats/threatresearch/blob/master/kpot_stealer/plaintext_strings.txt

[3] https://en.wikipedia.org/wiki/MurmurHash

[4] https://twitter.com/sysopfb/status/1035177455667957760

[5] https://en.wikipedia.org/wiki/Commonwealth_of_Independent_States

[6] https://www.proofpoint.com/us/threat-insight/post/lcg-kit-sophisticated-builder-malicious-microsoft-office-documents

[7] https://www.recordedfuture.com/ar3s-prison-release/

[8] https://www.flashpoint-intel.com/blog/malware-campaign-targets-jaxx-cryptocurrency-wallet-users/

Indicators of Compromise

67f8302a2fd28d15f62d6d20d748bfe350334e535 3cbdef112bd1f8231b5599d	SHA256	KPOT Stealer (Malware Analysis)
1f2852eeb1008b60d798f0cbcf09751e26e7980b4 35635bbef568402b3f82504	SHA256	KPOT Stealer (Campaign Analysis)
36dcd40aee6a42b8733ec3390501502824f570a2 3640c2c78a788805164f77ce	SHA256	Intermediate downloader (Campaign Analysis)
hxxp://bendes.co[.]uk/lmpUNlwDfoybeulu/gate.php	URL	KPOT Stealer C&C URL (Malware Analysis)
hxxp://5.188.60[.]131/a6Y5Qy3cF1sOmOKQ/gate .php	URL	KPOT Stealer C&C URL (Campaign Analysis)