Threat Actors Using Legitimate PayPal Accounts To Distribute Chthonic Banking Trojan

proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan

July 26, 2016

July 26, 2016

Updated August 2, 2016, to reflect new information a bout the malware referenced in this post; additional details added at the bottom.

While many email providers, clients, and anti-spam engines have become adept at detecting spam, malicious messages sent via high-profile, legitimate providers are much harder to catch. Threat actors continue to look for new ways to bypass these engines and, in the latest example of innovative approaches to malware distribution, have managed to co-opt PayPal services in a small campaign.

Proofpoint analysts recently noticed an interesting abuse of legitimate service in order to deliver malicious content. Specifically, we observed emails with the subject “You’ve got a money request” that came from PayPal. The sender does not appear to be faked: instead, the spam is generated by registering with PayPal (or using stolen accounts) and then

using the portal to “request money.” We are not sure how much of this process was automated and how much manual, but the email volume was low.

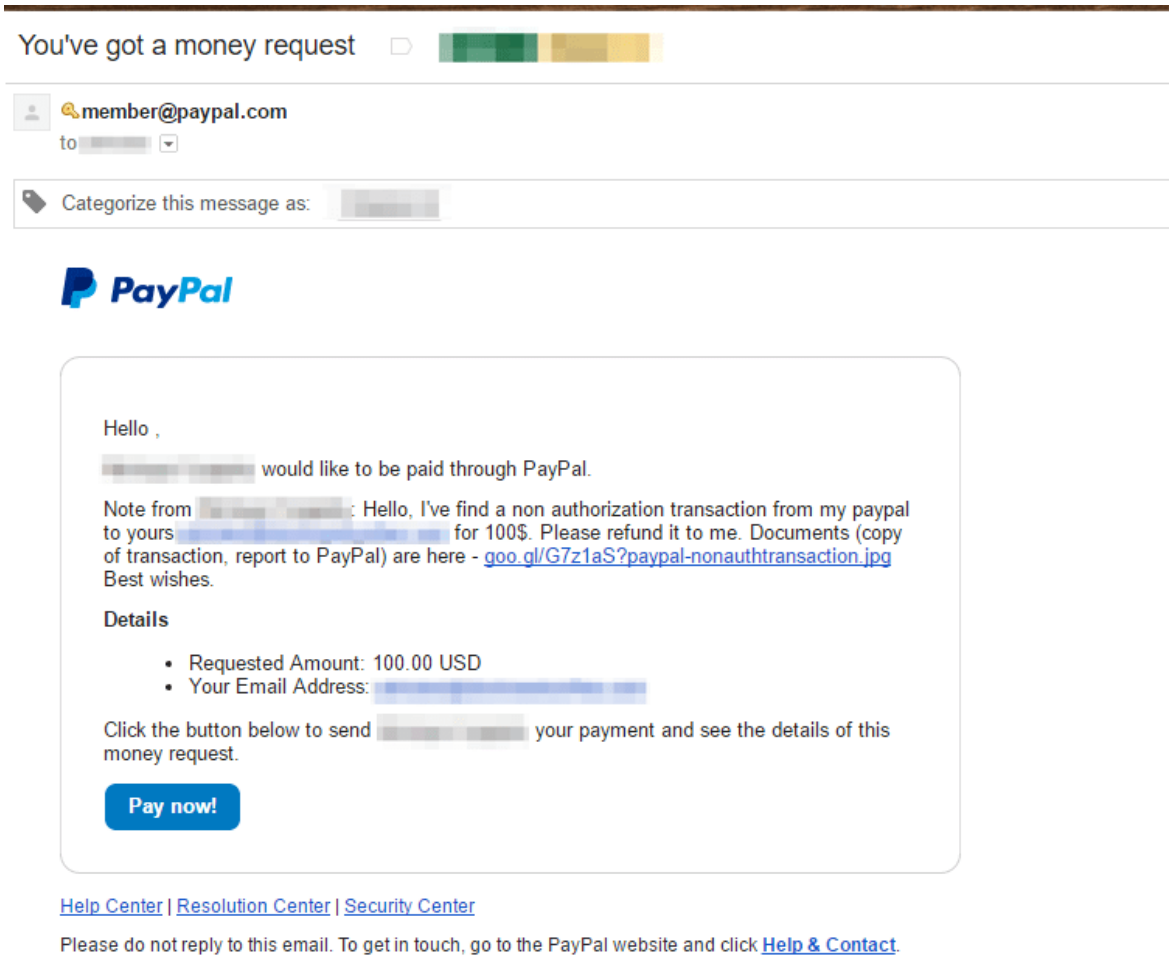


Figure 1: Email delivering malicious content

Although the actual email address is obscured in Figure 1, this message was sent to a Gmail inbox. Gmail failed to block the email since it appears legitimate. PayPal’s money request feature allows adding a note along with the request, where the attacker crafted a personalized message and included a malicious URL. In a double whammy, the recipient here can fall for the social engineering and lose $100, click on the link and be infected with malware, or both.

If the user does click on the Goo.gl link, they are redirected to katyaflash[.]com/pp.php, which downloads an obfuscated JavaScript file named paypalTransactionDetails.jpeg.js to the user’s system. If the user then opens the JavaScript file, it downloads an executable from wasingo[.]info/2/flash.exe. This executable is Chthonic, a variant of the Zeus banking Trojan. The command and control (C&C) for this instance is kingstonevikte[.]com. The following screenshot more clearly illustrates the sequence of events:

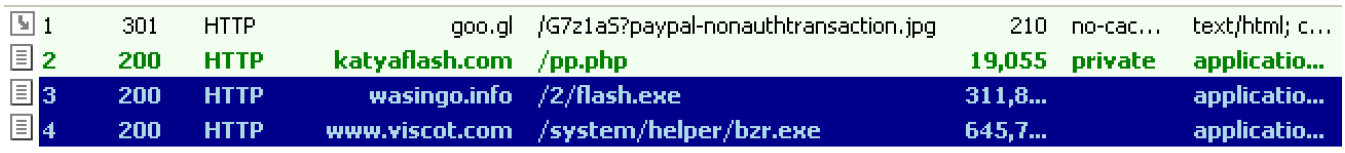


Figure 2: Network traffic generated starting with user clicking on the malicious URL and opening the downloaded JavaScript

It is also interesting that Chthonic downloads a second-stage payload, a previously undocumented malware “AZORult” which we are currently investigating:

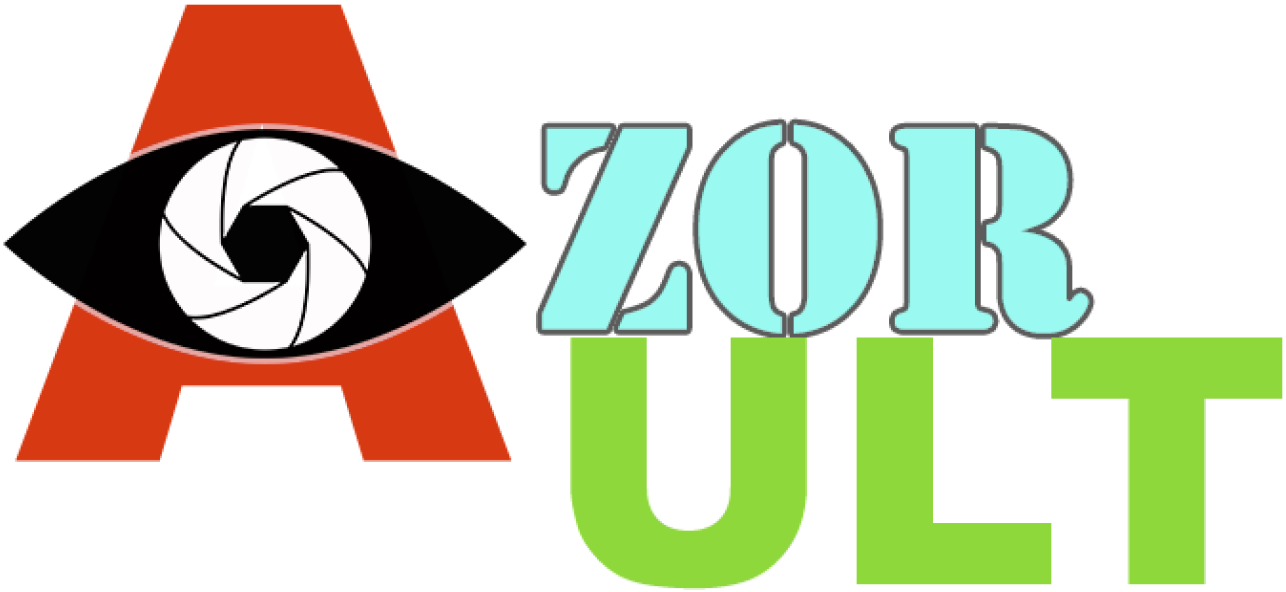


Figure 3: Logo used internally by the AZORult module

Conclusion

Although the scale of this campaign appeared to be relatively small (this particular example was only detected through one of our spamtraps; as of the writing of this blog, the malicious link has only been clicked 27 times according to Google Analytics for the URL shortener), the technique is both interesting and troubling. For users without anti-malware services that can detect compromised links in emails and/or phone homes to a C&C, the potential impact is high. At the same time, the combined social engineering approach of requesting money via PayPal from what appears to be a legitimate source creates additional risk for untrained or inattentive recipients, even if they are not infected with the malicious payload.

PayPal has been notified of this particular abuse of service but this represents yet another technique threat actors can use to bypass traditional defenses, regardless of the specific provider.

Indicators of Compromise (IOC's)

IOC	IOC Type	Description
[hxxp://goo[.]gl/G7z1aS?paypal-nonauthtransaction.jpg]	URL	URL in the email message
[hxxp://katyaflash[.]com/pp.php]	URL	URL after the goo.gl redirect (hosting the js)
865d2e9cbf5d88ae8b483f0f5e2397449298651381f66c55b7afd4b750eb4da4	SHA256	paypalTransactionDetails.jpeg.js
[hxxp://wasingo[.]info/2/flash.exe]	URL	JavaScript payload
0d2def167ecf39a69a7e949c88bb2096cfd76f7d4bf72f1b0fe27a9da686c141	SHA256	flash.exe

kingstonevikte[.]com	Domain	Chthonic C&C
[hxxp://www.viscot[.]com/system/helper/bzr.exe]	URL	Chthonic 2nd Stage hosting
10d159b0ddb92e9f4b395e90f9cfaa554622c4e77f66f7da176783777db5526a	SHA256	Chthonic 2nd Stage (AZORult)
[91.215.154[.]202/AZORult/gate.php]	URL	AZORult C&C

Select ET Signatures that would fire on such traffic:

2810099 || ETPRO TROJAN Chthonic CnC Beacon
2811901 || ETPRO TROJAN Chthonic CnC Beacon
2821358 || ETPRO TROJAN Win32/Zbot Variant Checkin

The information below was added based on additional background research conducted by Proofpoint analysts.

On July 31, Proofpoint researchers discovered an advertisement in an underground forum for the AZORult information stealer. This was the second-stage payload that Chthonic delivered to infected machines. The original ad in mixed Russian and English appears on top with our translation below:

Original Ad

[AZORult - Passwords, cookies, bitcoin, desktop files, etc stealer]
Многофункциональный стиллер.
Функционал:
• Stealer сохраненных паролей из следующих программ(browsers, email, ftp, im):
Спойлер
Google Chrome
Google Chrome x64
YandexBrowser
Opera
Mozilla Firefox
InternetMailRu
ComodoDragon
Amigo
Bromium
Chromium

Outlook
Thunderbird

Filezilla

Pidgin
PSI
PSI Plus

• Stealer cookies(Стиллер куков) из браузеров + данные автозаполнения форм(formhistory, autofill)
Поддерживаемые браузеры:
Спойлер
Google Chrome
Google Chrome x64
YandexBrowser
Opera
Mozilla Firefox

InternetMailRu
ComodoDragon
Amigo
Bromium
Chromium

Куки в следующем формате, для удобного экспорта(Netscape cookie file format):
Спойлер

Instagram[.]com FALSE / FALSE 11129062731157896 csrftoken ebc08a134952abc6a5c36fb54c1aaaa
.microsoft[.]com TRUE / FALSE 13140111158000000 TocPosition 1
www.searchengines[.]ru FALSE / FALSE 11138811175911879 ОАИСАР 640.1
vsokovikov.narod[.]ru FALSE / FALSE 11168272384aaa000 __utma
1.211136481.14511109932.14658111726.1496725111.1
vsokovikov.narod[.]ru FALSE / FALSE 13111168384000111 __utmz 1.1250111526.1.1.utmcsr=
(direct)|utmccn=(direct)|utmcmd=(none)

• Bitcoin clients files
Собирает файлы wallet.dat популярных биткоин клиентов (bitcoin, litecoin, etc)

• Skype message history.
Грабит файл с базой данных переписки. Файл читается специальными утилитами.

• Desktop files grabber.
Собирает файлы указанных расширений с рабочего стола. Фильтр по размеру файла. Также рекурсивно ищет файлы во вложенных папках.

• Список установленных программ.
• Список запущенных процессов.
• Username, compname, OS, RAM

Необходимый функционал можно включать/выключать в админке.

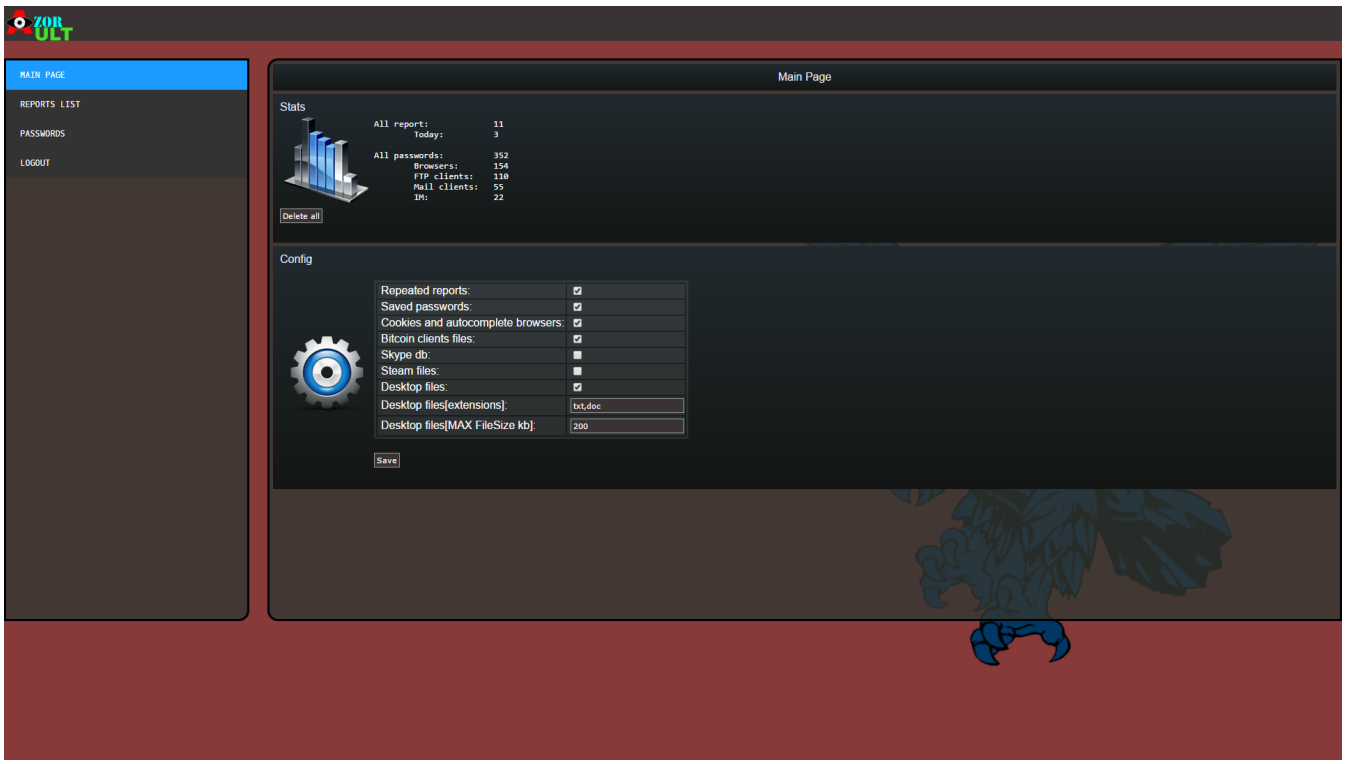
В админке просматривается список поступивших отчетов, список сохраненных паролей из этих отчетов. Фильтры по дате, по типу паролей, поиск по базе.
Остальные данные сохраняются в zip архив(отдельный для каждого отчета). Данные в архиве разложны по папкам. В архиве хранятся все данные, в админке только список отчетов и пароли.

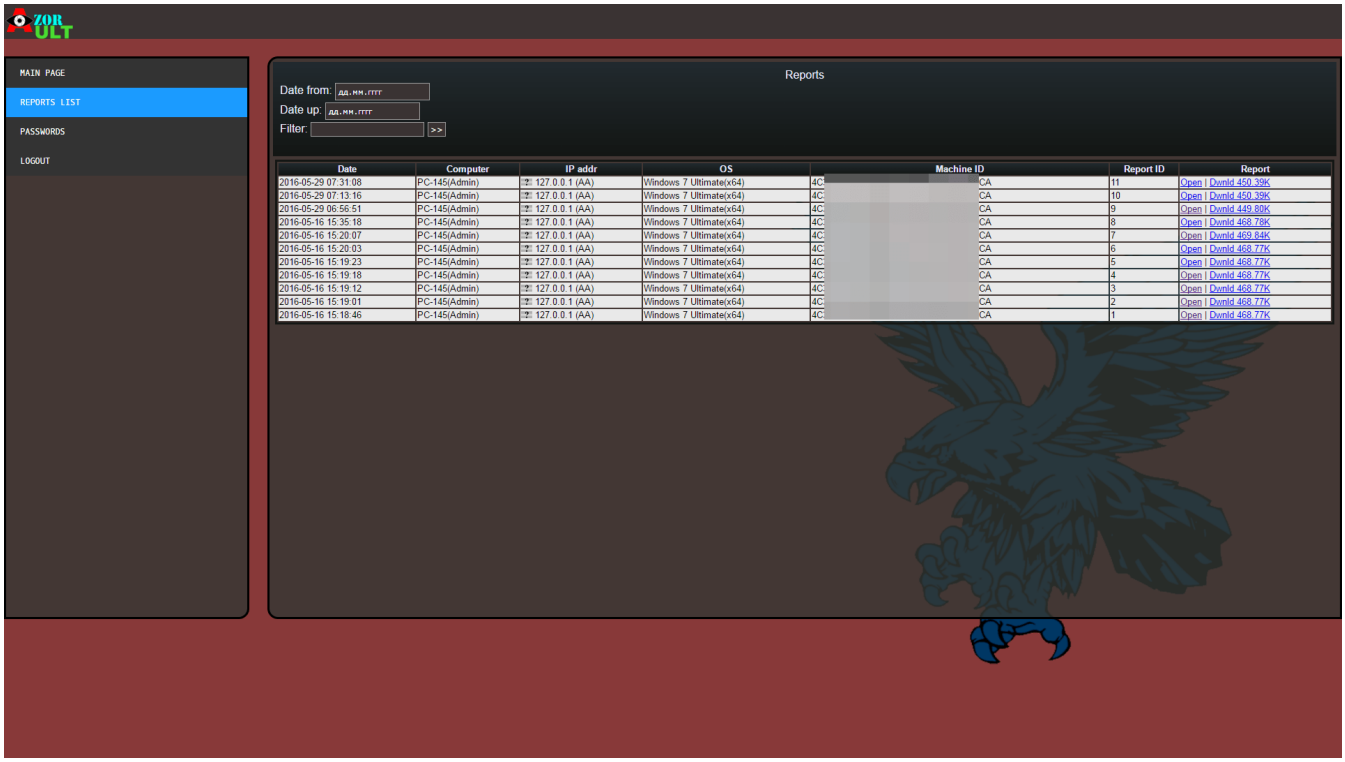
Спойлер
[]Browsers
-[]Autocomplete
--Google_Chrome_Default.txt
-[]Cookies
--Google_Chrome_Default.txt
--MozillaFirefox_tpsasn.default-111340945411.txt
[]Coins
-[]Bitcoin
--wallet.dat
-[]Litecoin
--wallet.dat
...
Info.txt
Passwords.txt
Process.txt
Programms.txt

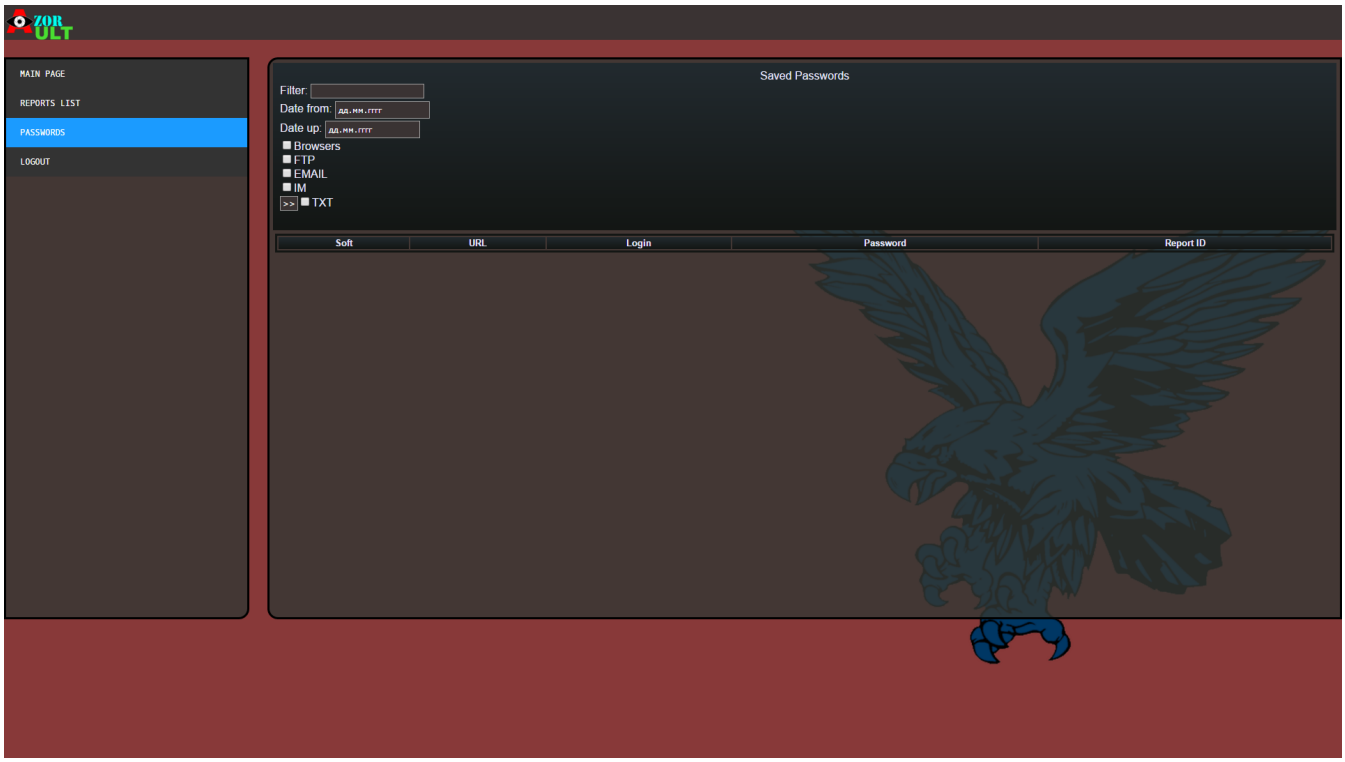
Софт поставляется в виде:
.EXE - при запуске собирается необходимая инфа и отправляется на сервер
.DLL - при подгрузке dll (DLL_PROCESS_ATTACH) собирается необходимая инфа и отправляется на сервер
.DLL(thread) - при подгрузке dll (DLL_PROCESS_ATTACH) создается отдельный поток, в котором производится необходимая работа(собирается необходимая инфа и отправляется на сервер). Например для использования как плагина для популярных лоадеров.

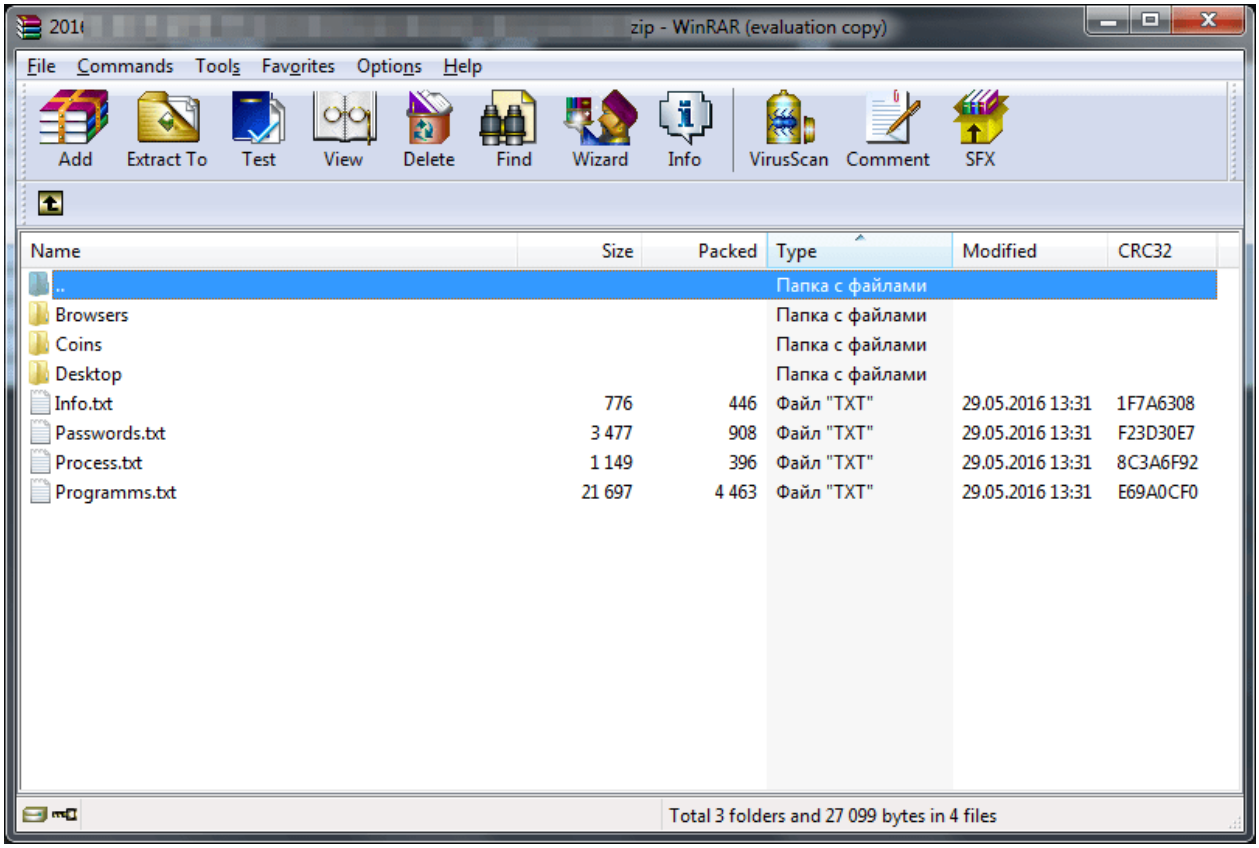
Скриншоты:
Спойлер

[Screenshots linked in the original ad – displayed here]




ZOR ULT
MAIN PAGE
REPORTS LIST
PASSWORDS
LOGOUT
Reports
Date from: дд.мм.гггг
Date up: дд.мм.гггг
Filter: >>
Date | Computer | IP addr | OS | Machine ID | Report ID | Report
2016-05-29 07:31:08 | PC-145(Admin) | 127.0.0.1 (AA) | Windows 7 Ultimate(x64) | 4C CA | 11 | Open | Dwnld 450.39K
2016-05-29 07:13:16 | PC-145(Admin) | 127.0.0.1 (AA) | Windows 7 Ultimate(x64) | 4C CA | 10 | Open | Dwnld 450.39K
2016-05-29 06:56:51 | PC-145(Admin) | 127.0.0.1 (AA) | Windows 7 Ultimate(x64) | 4C CA | 9 | Open | Dwnld 449.80K
2016-05-16 15:35:18 | PC-145(Admin) | 127.0.0.1 (AA) | Windows 7 Ultimate(x64) | 4C CA | 8 | Open | Dwnld 468.78K
2016-05-16 15:20:07 | PC-145(Admin) | 127.0.0.1 (AA) | Windows 7 Ultimate(x64) | 4C CA | 7 | Open | Dwnld 469.84K
2016-05-16 15:20:03 | PC-145(Admin) | 127.0.0.1 (AA) | Windows 7 Ultimate(x64) | 4C CA | 6 | Open | Dwnld 468.77K
2016-05-16 15:19:23 | PC-145(Admin) | 127.0.0.1 (AA) | Windows 7 Ultimate(x64) | 4C CA | 5 | Open | Dwnld 468.77K
2016-05-16 15:19:18 | PC-145(Admin) | 127.0.0.1 (AA) | Windows 7 Ultimate(x64) | 4C CA | 4 | Open | Dwnld 468.77K
2016-05-16 15:19:12 | PC-145(Admin) | 127.0.0.1 (AA) | Windows 7 Ultimate(x64) | 4C CA | 3 | Open | Dwnld 468.77K
2016-05-16 15:19:01 | PC-145(Admin) | 127.0.0.1 (AA) | Windows 7 Ultimate(x64) | 4C CA | 2 | Open | Dwnld 468.77K
2016-05-16 15:18:46 | PC-145(Admin) | 127.0.0.1 (AA) | Windows 7 Ultimate(x64) | 4C CA | 1 | Open | Dwnld 468.77K


ZOR ULT
MAIN PAGE
REPORTS LIST
PASSWORDS
LOGOUT
Saved Passwords
Filter:
Date from: дд.мм.гггг
Date up: дд.мм.гггг
Browsers
FTP
EMAIL
IM
>> TXT
Soft | URL | Login | Password | Report ID



Цена: $100
Ребилд: $30

Связь(jabber): [Redacted]@exploit[.]im

****

Translation:
[AZORult - Passwords, cookies, bitcoin, desktop files, etc stealer]
Multifunctional Stealer.
Functions:
• Stealer of saved passwords from following programs (browsers, email, ftp, im):
Google Chrome
Google Chrome x64
YandexBrowser
Opera
Mozilla Firefox
InternetMailRu
ComodoDragon
Amigo
Bromium
Chromium
Outlook
Thunderbird
Filezilla
Pidgin
PSI
PSI Plus

• Stealer of cookies from browsers and forms (form history, autofill)
Supported Browsers:
Google Chrome
Google Chrome x64
YandexBrowser
Opera
Mozilla Firefox
InternetMailRu
ComodoDragon
Amigo
Bromium
Chromium

Cookies are in following format, for easy export (Netscape cookie file format):
instagram[.]com FALSE /
FALSE 11129062731157111
csrftoken yyyc08a1349526c46a5c36fb54c1ayyy
.microsoft[.]com TRUE /
FALSE 11140260158000111
TocPosition 1
www.searchengines[.]ru FALSE /
FALSE 11138826175965111
ОАИСАР 111.1
vsokovikov.narod[.]ru FALSE /
FALSE 11168272384000111
__utma 1.111136481.1458509111.1465826111.1496725111.1
vsokovikov.narod[.]ru FALSE /
FALSE 13120968384000111
__utmz 1.1110722526.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)

• Bitcoin clients files
Collects wallet.dat files from popular bitcoin clients (bitcoin, litecoin, etc)

• Skype message history.
Grabs files from chat history. Files are read with special utilities.

• Desktop files grabber.
Collects files with specified extensions from Desktop. Filter by file size. Recursively searches files in folders.

• List of installed programs
• List of running processes
• Username, compname, OS, RAM

Necessary functions that can be turned on and of in admin panel

The admin panel has a list of received reports, list of saved passwords from those reports. Has filters by date, type of password, search in the base.
The rest of data from reports is save as a zip aarchive, different one for each report. The data is sorted into folders. The archive contains all data, while the admin panel only list of reports and passwords.

[]Browsers
-[]Autocomplete
--Google_Chrome_Default.txt
-[]Cookies
--Google_Chrome_Default.txt
--MozillaFirefox_tpasdn.default-111140945111.txt
[]Coins

-[]Bitcoin
--wallet.dat
-[]Litecoin
--wallet.dat
...
Info.txt
Passwords.txt
Process.txt
Programms.txt

Software is delivered as:
.EXE - when started, collects necessary info and sends to server
.DLL - when started the dll (DLL_PROCESS_ATTACH) collects necessary info and sends to server
.DLL(thread) - when started dll (DLL_PROCESS_ATTACH) creates a new thread which does the work (collects necessary info and sends to server)

Price: $100
Rebuild: $30

Contact(jabber): [Redacted]@exploit[.]im

Subscribe to the Proofpoint Blog