New Shameless Commodity Cryptocurrency Stealer (WeSteal) and Commodity RAT (WeControl)

unit42.paloaltonetworks.com/westeal/

Robert Falcone, Simon Conant

April 29, 2021

By Robert Falcone and Simon Conant

April 29, 2021 at 12:01 AM

Category: Unit 42

Tags: Cryptocurrency, Cybercrime, EMEA, RAT, Remote Access Trojan, WeControl, WeSteal

This post is also available in: 日本語 (Japanese)

Executive Summary

It seems that for every commodity malware takedown and prosecution, another replaces it to take a turn empowering cybercriminals. Often, commodity malware authors will disingenuously attempt to profess a guise of legitimacy for their malware – a strategy that often doesn't stand up in court.

The author of WeSteal, a new commodity cryptocurrency stealer, makes no attempt to disguise the intent for his malware. The seller promises "*the leading way to make money in 2021*" (Figure 1).

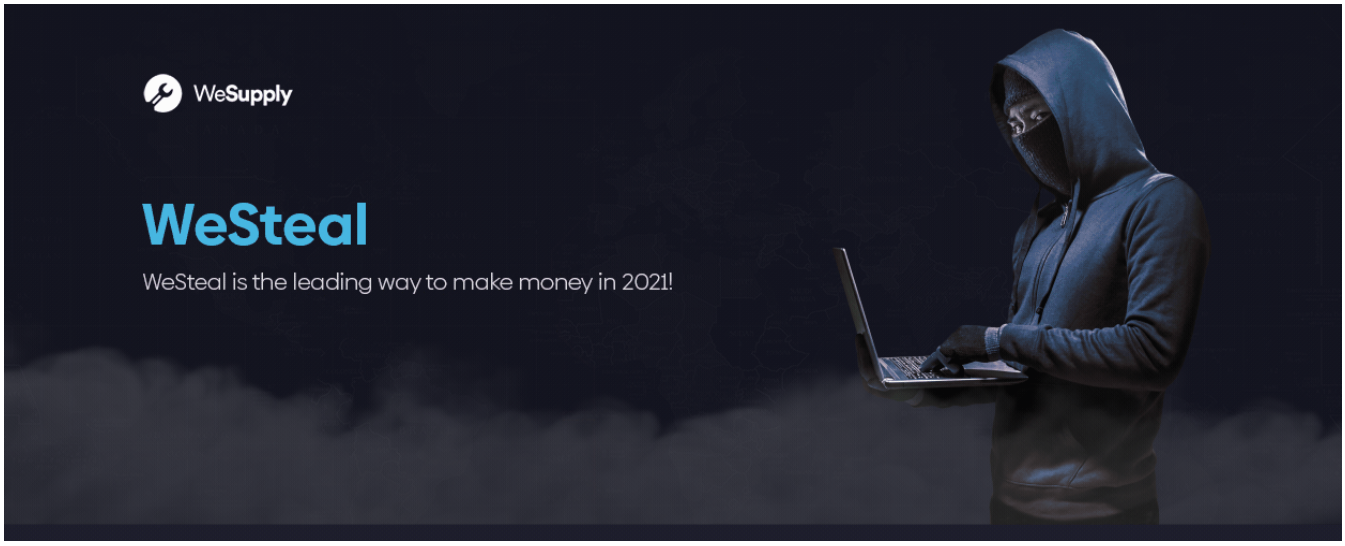

Figure 1. WeSteal advertisement.

In this blog, we analyze WeSteal, detail the obfuscation and techniques it uses for persistence and operation, and examine the customers of this malware. We take a look at the actor WeSupply, with an operation and website by the same name, and at the Italian malware coder ComplexCodes, a co-conspirator and actual author of this malware.

Immediately before the publication of this report, we discovered that the actors had both added some new features to WeSteal, and had also complemented it with a new commodity remote access tool (RAT) called “WeControl”. We document these new revelations at the end of our report.

Palo Alto Networks customers are protected from WeSteal and WeControl with Cortex XDR, the Next-Generation Firewall with WildFire and Threat Prevention security subscriptions, and AutoFocus.

Origin of WeSteal

Actor “ComplexCodes” started advertising WeSteal on underground forums in mid-February 2021. However, ComplexCodes had been selling a “WeSupply Crypto Stealer” since May 2020. A comparison of samples of the earlier WeSupply Crypto Stealer with WeSteal suggests that WeSteal is likely simply an evolution of the same project.

This Italian malware coder previously authored a “Zodiac Crypto Stealer” and “Spartan Crypter” for obfuscating malware to avoid antivirus detection.

The actor’s forum signature indicates an affiliation with a site that sells accounts for services such as Netflix and Disney+ (Figure 2).

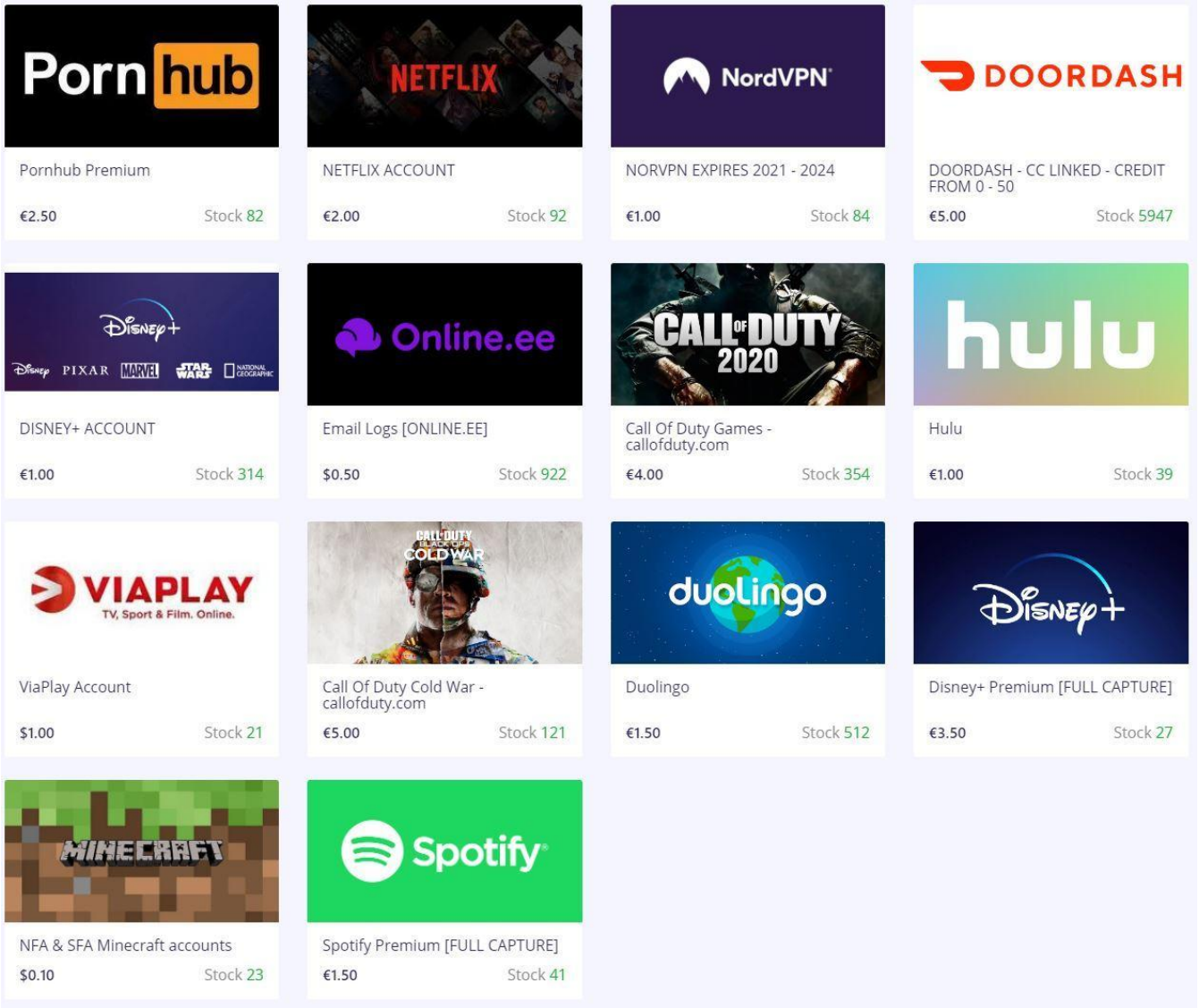

Figure 2. Underground site that sells accounts.

The intent is once again on display with ComplexCode's Discord-based commodity distributed denial-of-service (DDoS) offering, "Site Killah" (Figure 3).

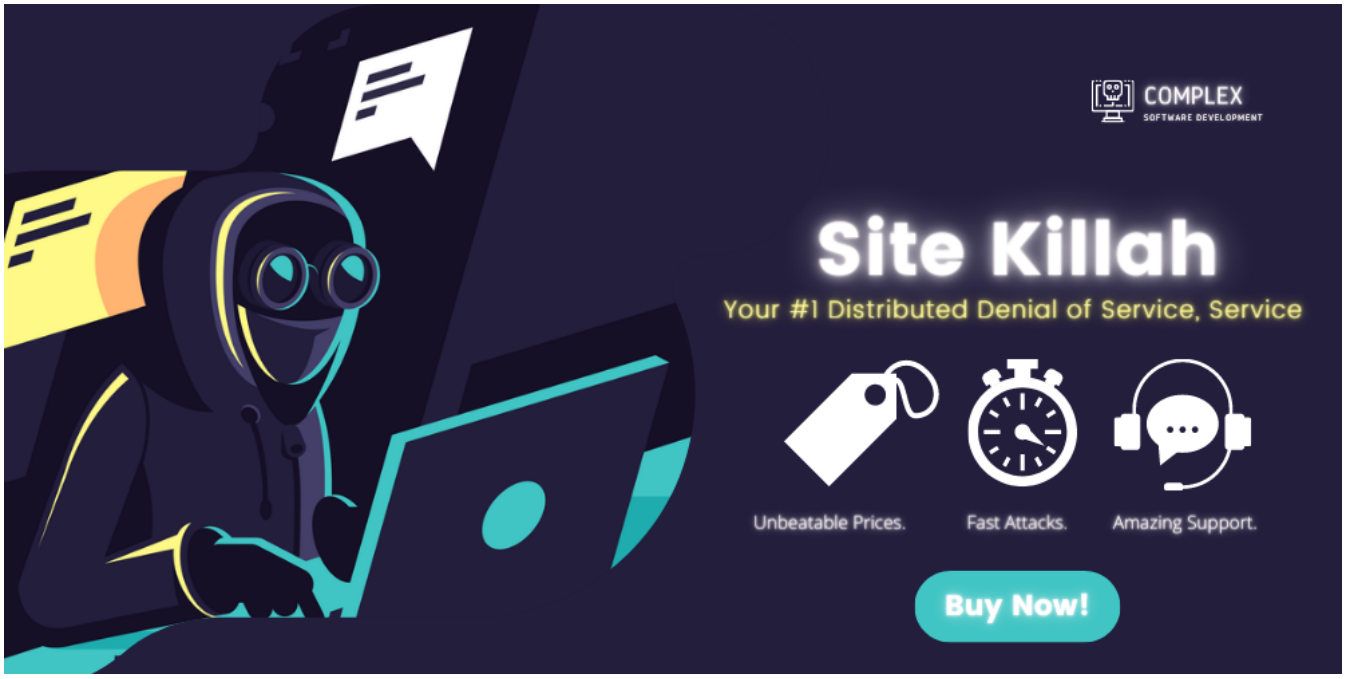

Figure 3. DDoS service advertisement.

Intent of WeSteal

When pursuing cases against malware authors, prosecutors typically need to demonstrate the author's intent for the malware. Many authors will hide behind meaningless Terms of Service statements that end users must not use the malware for illegitimate purposes. They will often describe potential "legitimate" uses for their malware – only to further describe anti-malware evasion properties, silent installation and operation or features such as cryptocurrency mining, password theft or disabling webcam lights.

There is no such pretense by ComplexCodes with WeSteal. There is the name of the malware itself. Then there is the website, "WeSupply," owned by a co-conspirator, proudly stating "WeSupply – You profit" (Figure 4).

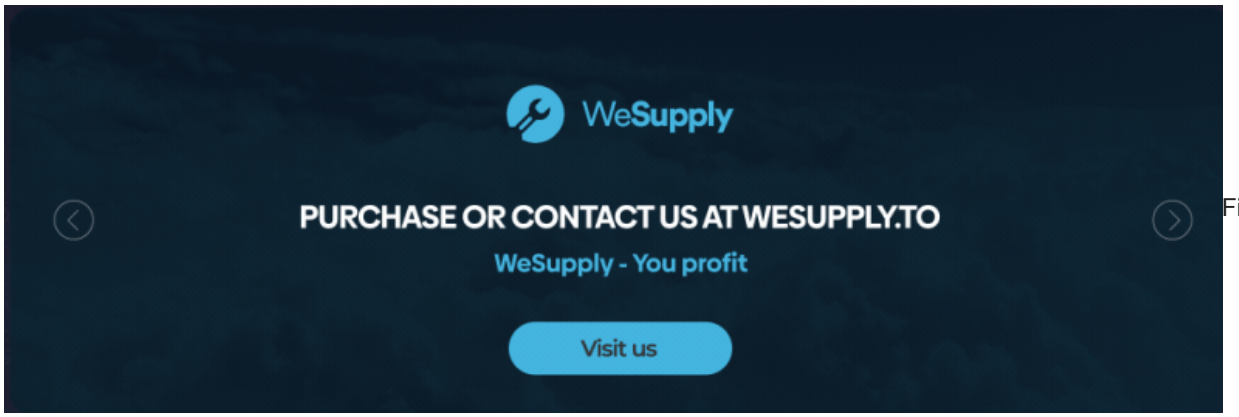

Figure 4. WeSupply advertisement.

As well as calling the malware WeSteal and advertising the "Crypto Stealer" feature, WeSupply's posts on forums also describe support for zero-day exploits and "Antivirus Bypassing" (Figure 5).

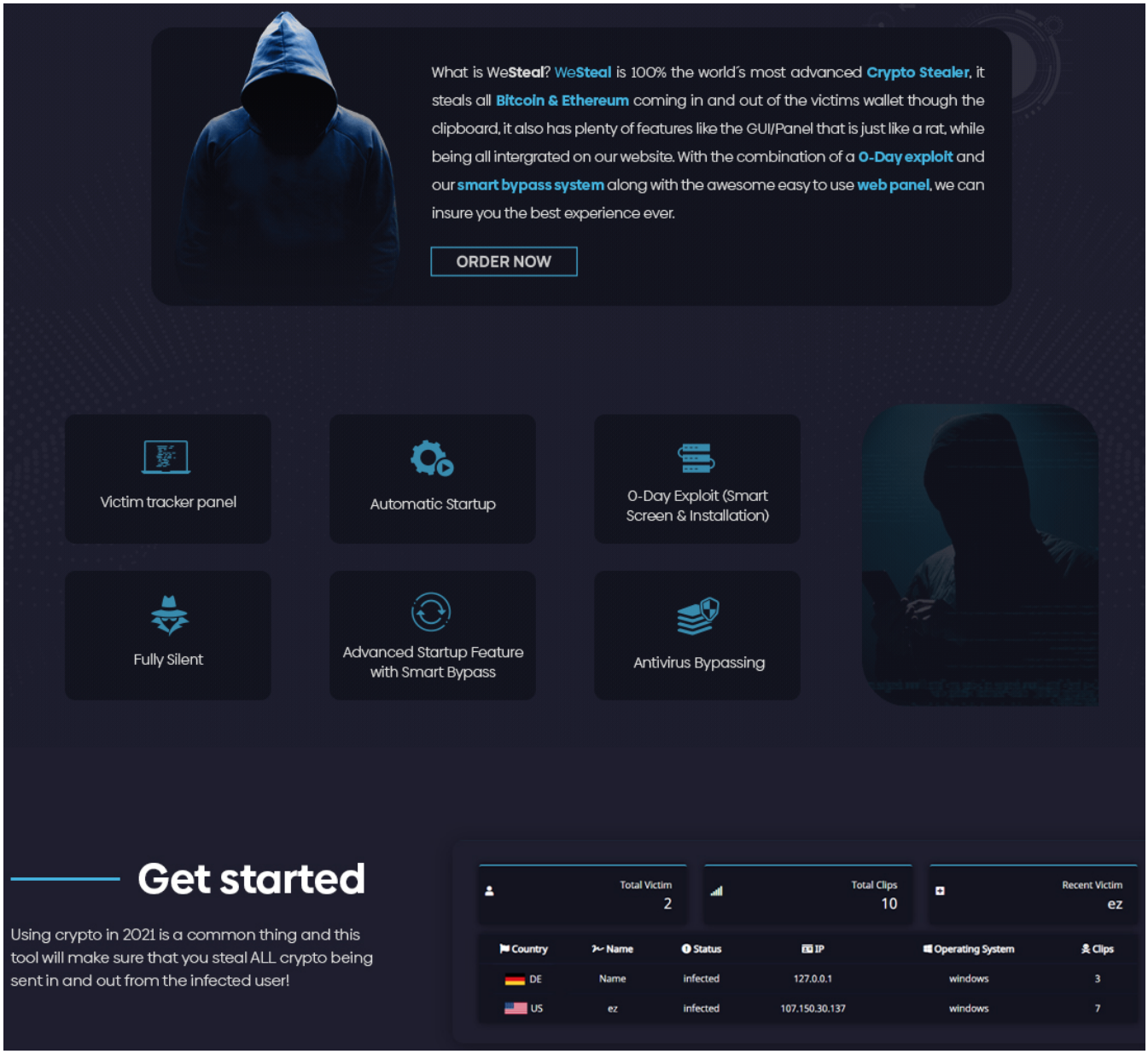

Figure 5. WeSteal features.

This is demonstrated with a screenshot claiming no antivirus detection for a sample (Figure 6). WeSteal includes a "Victim tracker panel" that tracks "Infections" – leaving no doubt about the context.

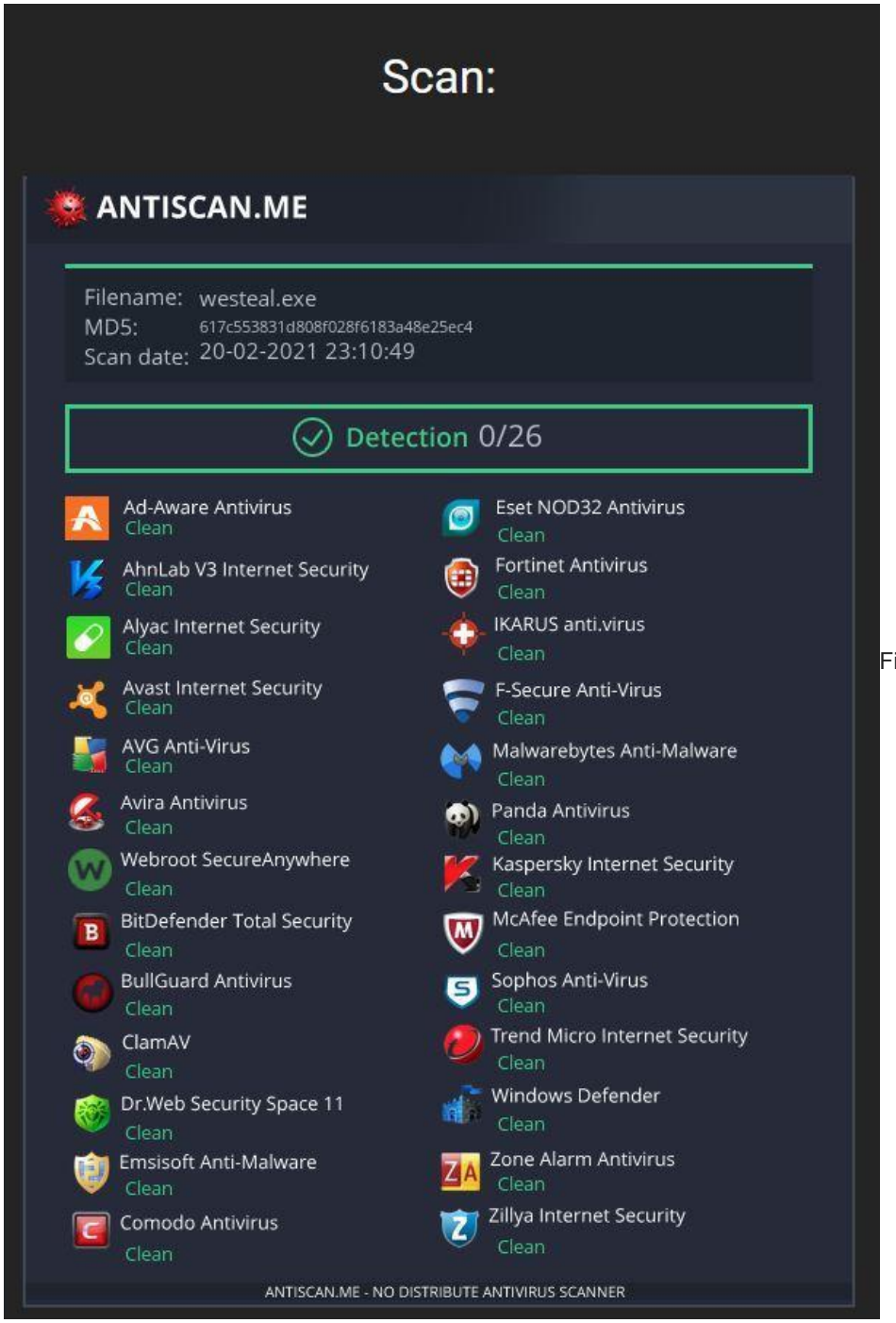

Figure 6. WeSteal antivirus scanning results.

Of course, ComplexCodes profits from the sale of WeSteal by charging €20 for a month, €50 for three months and €125 for one year (Figure 7).

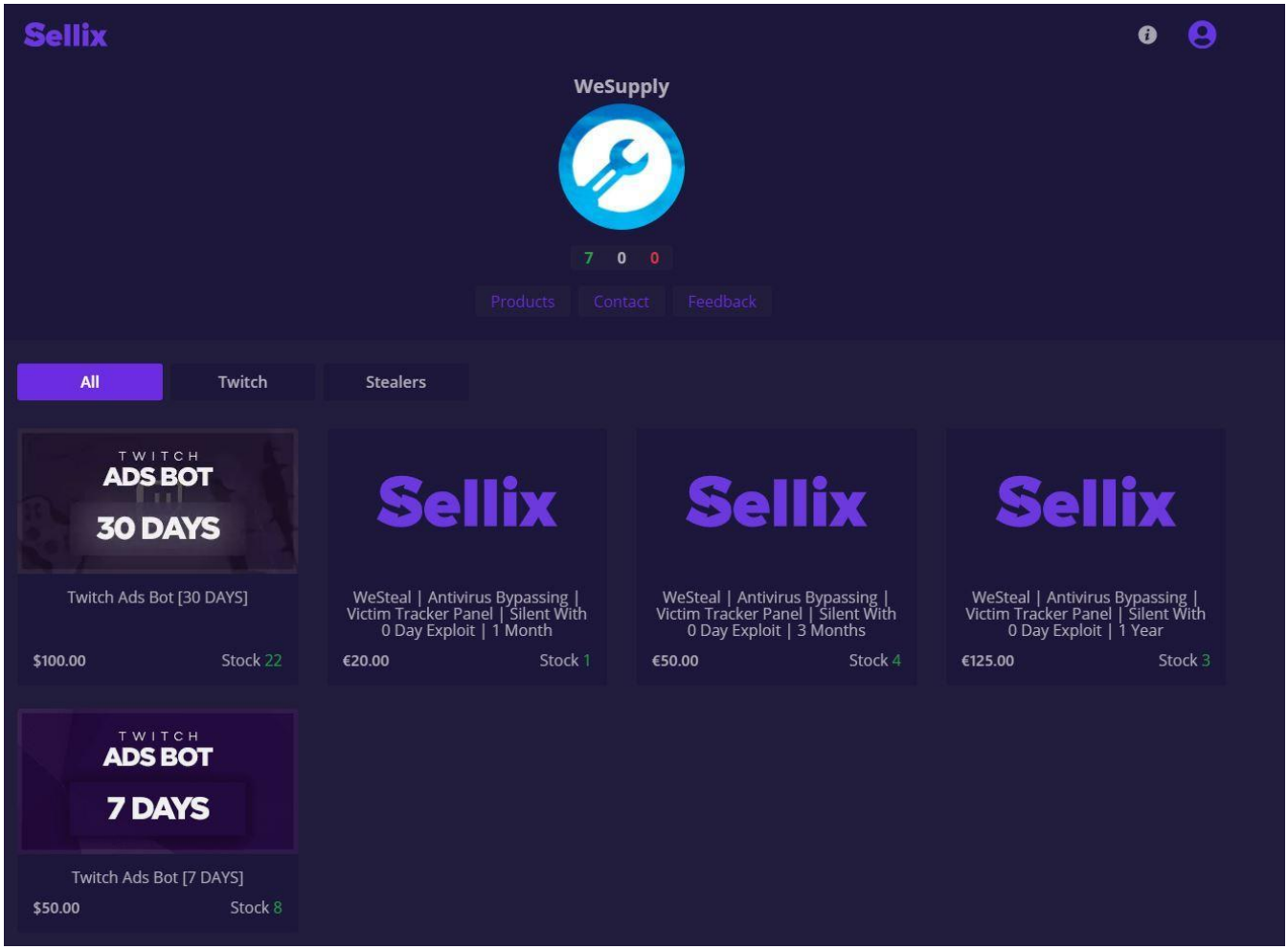

Figure 7. WeSteal advertisement on Sellix, an ecommerce store.

There isn't any possible angle from which to claim legitimacy for a piece of software designed to steal cryptocurrency transactions.

Capabilities of WeSteal

In order to "steal" cryptocurrency from a victim, WeSteal uses regular expressions to look for strings matching the patterns of Bitcoin and Ethereum wallet identifiers being copied to the clipboard. When it matches these, it replaces the copied wallet ID in the clipboard with one supplied by the malware. The victim then pastes the substituted wallet ID for a transaction, and the funds are sent instead to the substitute wallet.

RAT?

WeSteal is advertised as featuring a "RAT Panel." Not a single RAT feature is advertised nor observed in our analysis. It seems that ComplexCodes is rather ambitiously describing their simple hosted command-and-control (C2) service, elsewhere described as a "victim tracker," as a "RAT Panel."

C2 as a Service

As we have observed in some other commodity malware, rather than leaving customers to run their own C2, WeSteal operates with a hosted C2 as a service (C2aaS).

WeSteal is configured to use the following URLs for its C2 communications. We have observed two different C2 domains, one of which is also the sales site for the malware.

hxxps://wesupply[.]to/t_api.php
hxxps://wesupply[.]io/t_api.php

Speaking of "Service"

The WeSupply crew seems very invested in the “success” of their customers. In one forum sales thread, a would-be but apparently inexperienced potential criminal asks:

“*how do you use the tool and how does it target someone?*”

To which the helpful malware peddlers respond:

“*Open a ticket, will help you with all your questions.*”

Obfuscation

WeSteal is distributed as a Python-based Trojan in a script named "westeal.py". ComplexCodes converted it into an executable form using PyInstaller. The Trojan was specifically written for Python 3.9, as the PyInstaller package included python39.dll as the Python interpreter. The developer also used the open source PyArmor source code obfuscator, which encrypts the contents of the Python script and decrypts the contents before sending to the Python interpreter for execution, as seen here:

```
from pytransform import pyarmor_runtime

pyarmor_runtime()

_pyarmor(name, __file_, b'PYARMOR\x00\x00\x03\t\x00a\r\r\n\x06[snip]
```

PyArmor relies on the "_pytransform.dll" library to decrypt the contents of the Python script and sends them to the "python39.dll" interpreter. The WeSteal samples we analyzed were obfuscated using PyArmor's "obf_mode" setting configured to 2. This "obf_mode" setting includes the WeSteal Python bytecode as ciphertext that PyArmor decrypts using AES GCM at runtime.

An Interesting Persistence Technique

The “add_startup” function establishes persistent access to the system, by which WeSteal copies itself to the following location:

```
C:\Users\<username>\AppData\Local.exe
```

WeSteal then creates the following batch script in the startup folder that will run each time the user logs in:

```
c:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\appdata.bat
```

The batch script contains the following command:

```
start %localappdata%
```

The command above uses a novel technique to obfuscate the batch file starting the WeSteal executable. The start command attempts to run the environment variable %localappdata%, which on a default Windows system is a path to the folder C:\Users\<username>\AppData\Local. However, in this context, the Local in that environment variable is interpreted as a file rather than a subfolder. The start command will run the WeSteal executable Local.exe (the start command does not require the .exe file extension) in the path C:\Users\<username>\AppData\.

The “heist” (or “cuckoo’s egg”?)

The get_clipboard and copy_to_clip functions carry out WeSteal’s cryptojacking functionality. These functions check for Bitcoin (BTC) and Etherium (ETH) wallets copied to the clipboard and replace them with an actor's wallet, hoping that the user will then paste the actor’s wallet instead of the intended one, redirecting a cryptocurrency transaction in the actor’s favor. The actor is counting on the victim not noticing the substitution until it is too late and the irrevocable cryptocurrency transaction has been completed.

WeSteal uses regular expressions to identify wallets copied by the user to the clipboard. The regular expressions specifically describing the formats of Bitcoin and Ethereum wallets are seen in the constants identified in the decrypted WeSteal sample (Figure 8).

```
'wi7l0j9a52hx9dd4wrpmbv480v62ehg0tsf8hi8egvi122xrpq'
'X0NR8'
'bc1qkmg9c0p52xgzqjqswdz6k9gxddwvchr8rt3pm8'
'0x86C19f41004d451dc6dcb4f0AC086EDdA1383b70'
'APPDATA'
'\\desktopini.txt'
'C:\\Users\\'
'\\AppData\\Local.exe'
'\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\'
'appdata.bat'
13
'user32'
'kernel32'
66
'https://wesupply .to/t_api.php?login='
'&api='
'&newrecord=no&status=Infected&windowsusername='
'&ip='
'&country='
'&os='
'&newclip=no'
'w+'
'&newrecord=yes&status=Infected&windowsusername='
0.7
'^([13][a-km-zA-HJ-NP-Z1-9]{25,34}|bc1[ac-hj-np-zAC-HJ-NP-Z02-9]{11,71})$'
'&newclip=yes'
'^0x[a-fA-F0-9]{40}$'
```

Figure 8. Constants from a decoded WeSteal sample.

WeSteal's Customers, Wallets and Their "Hauls"

Also encoded in the samples were the hardcoded customer "handle," and their BTC and ETH wallets. From this, we have some idea of the current customer base and possibly an idea of their success.

We collated a small list of customers. In general, the wallets identified had only a small number of transactions since WeSteal was released, and those were of low value. However, at least one wallet (actor "pepsi") received approximately $800 in a single Ethereum transaction. It is, of course, possible that any of these transactions may be unrelated to the malware.

Handle	Etherium Wallet	Bitcoin Wallet
Heroin	0xb5F7Bf1B46854f3EDA1201294941Edb13f9661EA	1AB3XSnioEFKKZcDadmSDX8YRcQzgRnG3c
pepsi	0x5f9C7078dFF737BbF872b438151Cd38ECfe0ebee	1NbyaaQTGPAhj8CuqRSRrXbWCCtyhdyv7T

touourien	0x419f92Af57Eeb3f50fbE10298cC4a684aB452011	bc1qg0gr8286k6kemtd3cwch6guzfp6yn9n3smlqt8
Adribusted	0x49c8d0359cAf80FfebD8424128A951264f4f6506	bc1q8pufxrmm8k5n9v4w2auvlaedx9lm23c7sg6mye
King	0x1FdD9e44048F88B04C6DBba897E05ecCA55A61f9	1KVsfk5jT5fUGbUxomxAsKYxVvSZC9joXs
belzedar	0xc7D4E35C3ea831c3Bbf53550621315C79423E95F	bc1q30el678lr9dwcydtm8gjztf389zrj6gfs6ezj5
xjoking	0xa4FC40168EF940eD013E1dB6986C5746AAC3b2c3	1APLhq2yC421C3G6X5uhLhTmtZMjSUZ38G
Shakho	0x356d6162ADa9db9bd31b95Eec92Cd3B1D3273623	1CUYk9xCDU9WfTbLZj561M32Q55EZtcyEo
WeZesk	0x269eCD3E97A37C27347E4E87D6f3f1B59A0BE2AB	1BcD15EEpeA1Mfz49oAMfdikeXjhCfiUU6
X0NR8	0x86C19f41004d451dc6dcb4f0AC086EDdA1383b70	bc1qkmg9c0p52xgzqjqswdz6k9gxddwvchr8rt3pm8
wizzz	0xAaD7685A29bE275E9404Ba88260E19dB52644DE3	bc1qx7ha77kanm3nn8fe2ap4ts2uyxjxgmc35llud7
Pepe	0xB97749901245b417060bbdFf3D7d1eC90b584a7c	17SjdBcboW2EPFMyoPwzp64eyjMwTLoBSG

The actor WeSupply is unsurprisingly observed using their own tool (using a second forum handle, “Shakho”). Also unsurprising is that many of these handles are also noted in the same forums where WeSteal is promoted.

Recent Observed Updates, Including WeControl RAT

Immediately before the publication of this report, we noticed some new samples that bore a striking similarity to WeSteal (also Pyarmor-obfuscated compiled Python), but were also different from other WeSteal samples.

This caused us to refresh our research of forums and the actors’ website. We note them advertising improvements to WeSteal, as well as selling a new piece of malware called “WeControl” RAT.

WeSteal Improvements

When we first analyzed WeSteal, we wondered why the actors included only the ability to monitor for and steal just two cryptocurrencies, Bitcoin and Ethereum. Although those are the most popular cryptocurrencies, it would surely be simple enough to code for the wallet patterns of other cryptocurrencies as well.

Figure 9. Updated WeSteal marketing.

Unsurprisingly, we now note that the authors have added three cryptocurrencies to the list of those that can be stolen:

- Bitcoin: BTC
- Ethereum: ETH
- Litecoin: LTC
- Bitcoin Cash: BCH
- Monero: XMR

WeControl RAT

Unfortunately, the timing of the discovery of a new commodity RAT at the actors' site precluded us including a full analysis in this report.

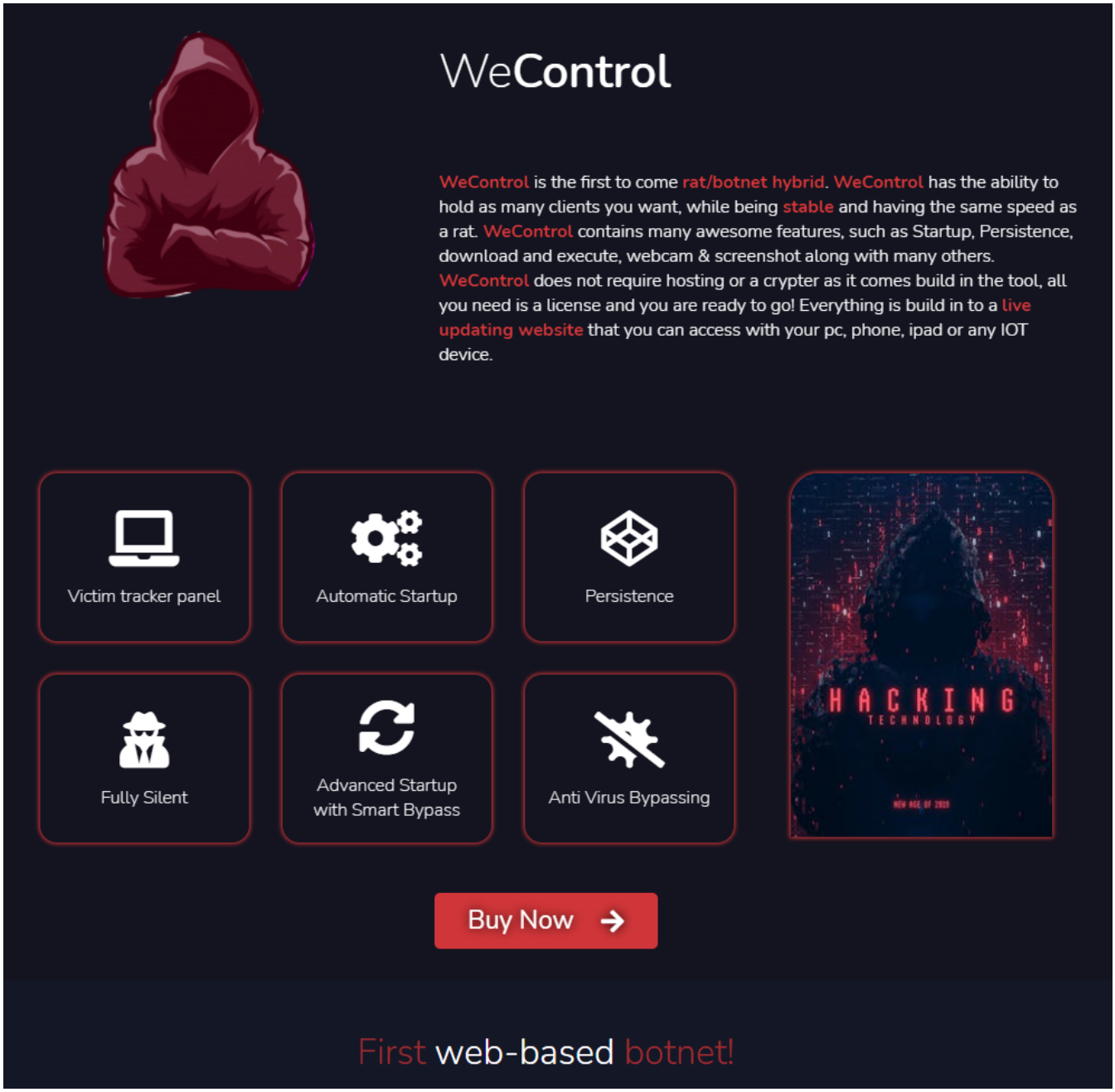

Figure 10. WeControl advertised at the actors' website

WeControl is marketed as a "rat/botnet hybrid." The description seems to indicate that the actors have incorporated the C2-as-a-service model of WeSteal into this RAT as well. This is not "the first" web-based C2aaS as they claim – WebMonitor RAT has been offering C2aaS for over two years.

Using a familiar technique from WeSteal, WeControl is again compiled Python obfuscated with PyArmor.

We first observed a sample of WeControl mid-April 2021. At the time of publication, we have collected just seven samples of WeControl. The hashes for these can be found at the end of this report.

Conclusion

WeSteal is a shameless piece of commodity malware with a single, illicit function. Its simplicity is matched by a likely simple effectiveness in the theft of cryptocurrency. The low-sophistication actors who purchase and deploy this malware are thieves, no less so than street pickpockets. Their crimes are as real as their victims.

The fast and simple monetization chain and anonymity of cryptocurrency theft, together with the low cost and simplicity of operation, will undoubtedly make this type of crimeware attractive and popular to less-skilled thieves.

WeControl is similarly both designed and marketed as a tool for illicit activity, lacking in propriety no less than the earlier WeSteal.

The ease of detection and blocking of the C2 as a service works against the Italian malware author ComplexCodes. It's surprising that customers trust their "victims" to the potential control of the malware author, who no doubt could in turn usurp them, stealing the victim "bots" or replacing customers' wallets with one of ComplexCodes' own at any time. It's also surprising that the malware author would risk criminal prosecution for what must surely be a small amount of profit, given the apparently small customer base.

Organizations with effective spam filtering, proper system administration and up-to-date Windows hosts have a much lower risk of infection.

Palo Alto Networks customers are further protected from WeSteal and WeControl with Cortex XDR or the Next-Generation Firewall with WildFire and Threat Prevention security subscriptions. AutoFocus users can track WeSteal and WeControl activity using the WeSteal and WeControl tags.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to deploy protections to their customers rapidly and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit https://www.cyberthreatalliance.org/.

Indicators of Compromise

WeSteal Samples

A SHA256 hash list of the 157 identified WeSteal samples, as of the time of publishing this report, is available at our GitHub repository.

WeControl Samples

59ffba39fc87eacd7c19498b5bb495d9c86c8bec40f3282e996aa80d77c45fa7
ed6875d60a67149c6cee4798a305810c6bcaa9b0b9349ec397ed331d96707e37
2bdc916680402a973afca8407d83c299092515cf5cc78ad0a92a8ce2d72b6f7c
8d37eef0308d5bd03d6c93ab247ca82d2157053822428ad1c787771de8e4332f
e2b11c10832991577184abd4f57af7383f30142a52fc8e2b41145f416860acf1
0920763b06f0a90f57910aaeff361d978bf37b025cbb9bc206d290eeb81e6217
eac7d579002f5e7f2cbff86b8e233c433f14ae25faf112eabaa1e2dd4f2a9a3d

C2 / sales domains

wesupply[.]to
wesupply[.]io