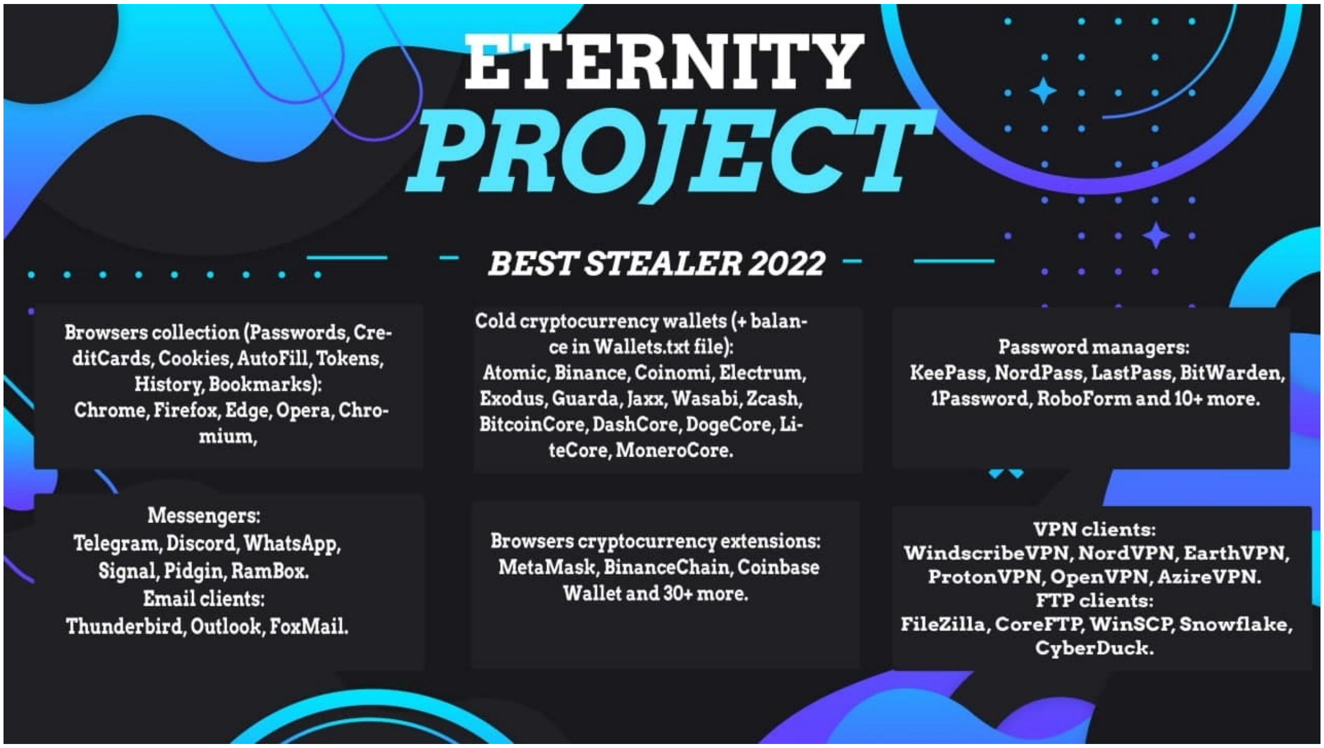
EternityTeam: a new prominent threat group on underground forums

blog.sekoia.io/eternityteam-a-new-prominent-threat-group-on-underground-forums/

May 17, 2022



ETERNITY
PROJECT

BEST STEALER 2022

Browsers collection (Passwords, CreditCards, Cookies, AutoFill, Tokens, History, Bookmarks):
Chrome, Firefox, Edge, Opera, Chromium,

Cold cryptocurrency wallets (+ balance in Wallets.txt file):
Atomic, Binance, Coinomi, Electrum, Exodus, Guarda, Jaxx, Wasabi, Zcash, BitcoinCore, DashCore, DogeCore, LiteCore, MoneroCore.

Password managers:
KeePass, NordPass, LastPass, BitWarden, 1Password, RoboForm and 10+ more.

Messengers:
Telegram, Discord, WhatsApp, Signal, Pidgin, RamBox.
Email clients:
Thunderbird, Outlook, FoxMail.

Browsers cryptocurrency extensions:
MetaMask, BinanceChain, Coinbase Wallet and 30+ more.

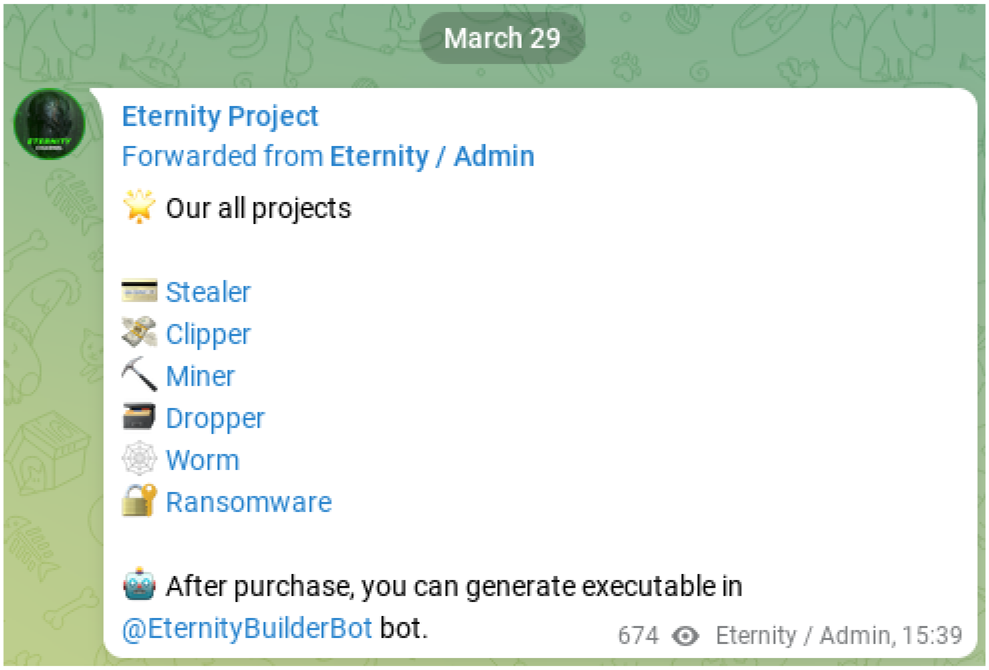
VPN clients:
WindscribeVPN, NordVPN, EarthVPN, ProtonVPN, OpenVPN, AzireVPN.
FTP clients:
FileZilla, CoreFTP, WinSCP, Snowflake, CyberDuck.

This blog post on EternityTeam originally came from a FLINT (SEKOIA.IO Flash Intelligence) report sent to our clients on April 12, 2022.

During our monitoring of Dark Web cybercrime forums, we came across **EternityTeam**: a new active and organized threat group that is developing and advertising several malware. We have identified different pieces of malware related to this group: Eternity Stealer, Eternity Worm, Eternity Miner, Eternity Clipper, Eternity Botnet, and Eternity Ransomware.

There are several reasons to believe that the EternityTeam could become a prominent malware seller and that their malware could spread in the wild:

- their malware software capability;
- their presence on numerous underground forums;
- their effort invested in the marketing;
- the number of Eternity Stealer samples identified by SEKOIA.IO in the wild;
- the “project” of the Eternity threat group has been “verified and approved” by the administrators of several cybercrime forums in early February 2022, as a guarantee of the worthiness of the products they sell.



March 29

Eternity Project

Forwarded from Eternity / Admin

🌟 Our all projects

💳 Stealer
💸 Clipper
⛏ Miner
🗃 Dropper
🕸 Worm
🔐 Ransomware

🤖 After purchase, you can generate executable in @EternityBuilderBot bot.

674 👁 Eternity / Admin, 15:39

Figure 1. Eternity's malware catalog advertised on their Telegram channel

In this blog post, we describe the activities on underground forums of EternityTeam members, share an overview of the different malware and present a quick analysis of the Eternity Stealer that appears to be their best-selling malware.

EternityTeam activity on underground forums

EternityTeam is a group that develops and sells different malware since at least January 2022. The threat group is present on numerous Russian-speaking underground forums, such as *XSS*, *UfoLabs*, *BHF*, *RuTOR*, *SkyNetZone*, *DarkClub*, and others for advertising and selling their malware.

We noticed that several profiles are selling the EternityTeam malware, for example:

- *UnderD0g* advertises all products on the UfoLabs forum with the Telegram channel (*t[.]me/EternityTeam*) of the EternityTeam. It is interesting to note that UnderD0g has a profile on the XSS forum but has not used it to communicate about Eternity activities.
- *Neizvestnost74* advertises, with its own Telegram profile, all the products (except the worm) on XSS, UfoLabs and BHF forums, among many others. The threat actor has entered the hacking forum scene at least since 2019 for selling dedicated servers, malware, or for buying brute force services.
- *EternityTeam* is a recent profile that has only advertised the Eternity Stealer and the Eternity Worm on several forums.
- *CyberSurprice* advertises information stealer on numerous forums. As EternityTeam, this profile seems to have been created for purposes of the Eternity projects.

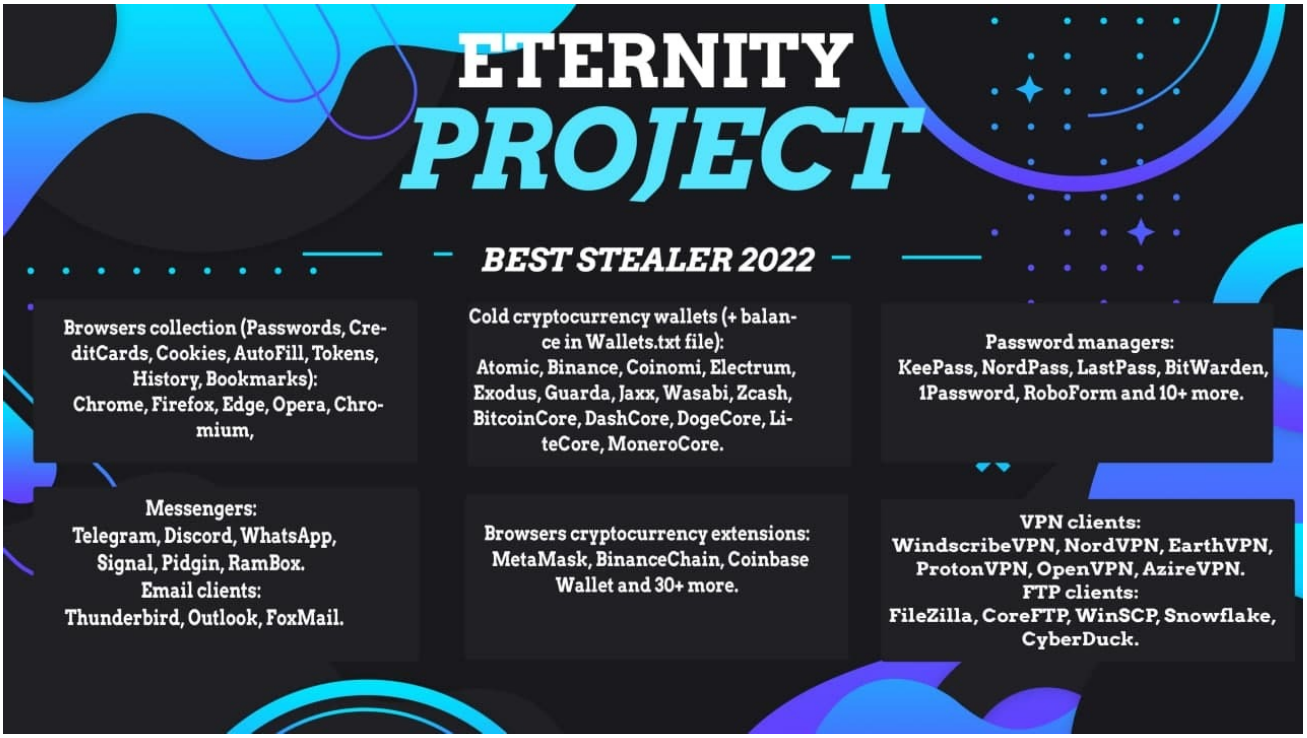
All profiles are responsive to questions from potential or current clients, either on technical (detection) or business issues. The group members communicate in Russian (mainly) and English.

In addition to this, EternityTeam maintains a Telegram channel (*t[.]me/s/EternityMalware*), an .onion website (*malwarewrn7fvd7zq243d74dxs3ca4wh5kw6i2opkzeusuoajtd2j5yd[.]onion*) and a GitHub repository (*github[.]com/L1ghtM4n*) in which they share details, videos, updates about all their malware in their catalog.

In the light of the above, we can assume that **EternityTeam** is a new group of several threat actors familiar with the cybercrime ecosystem. They surely started their business for financial gain.

Eternity's malware catalog

The Eternity information stealer, advertised as the **Eternity Stealer** or **Eternity Project**, is the one that interests the most on forums. More details on this malware are given in the following part.



ETERNITY PROJECT

BEST STEALER 2022

Browsers collection (Passwords, CreditCards, Cookies, AutoFill, Tokens, History, Bookmarks):
Chrome, Firefox, Edge, Opera, Chromium,

Cold cryptocurrency wallets (+ balance in Wallets.txt file):
Atomic, Binance, Coinomi, Electrum, Exodus, Guarda, Jaxx, Wasabi, Zcash, BitcoinCore, DashCore, DogeCore, LiteCore, MoneroCore.

Password managers:
KeePass, NordPass, LastPass, BitWarden, 1Password, RoboForm and 10+ more.

Messengers:
Telegram, Discord, WhatsApp, Signal, Pidgin, RamBox.
Email clients:
Thunderbird, Outlook, FoxMail.

Browsers cryptocurrency extensions:
MetaMask, BinanceChain, Coinbase Wallet and 30+ more.

VPN clients:
WindscribeVPN, NordVPN, EarthVPN, ProtonVPN, OpenVPN, AzireVPN.
FTP clients:
FileZilla, CoreFTP, WinSCP, Snowflake, CyberDuck.

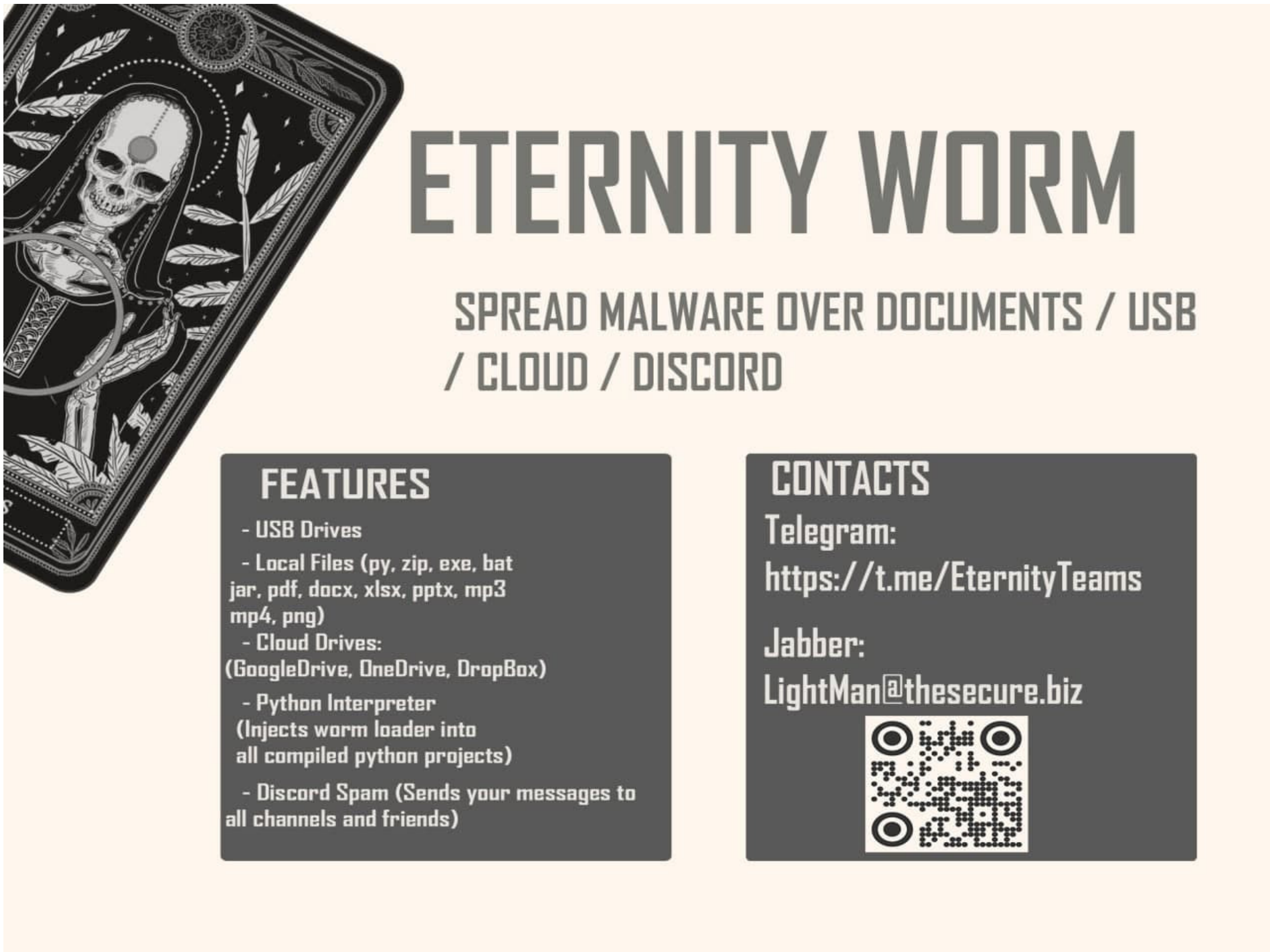
Figure 2. Eternity Stealer advertisement published on several underground forums

The **Eternity Miner** is sold for $110. It aims to mine Monero cryptocurrency on Windows hosts. The malware implements several defense evasion techniques, such as masking as a system process, hiding from the task manager, preventing hibernation, and persistence.

The **Eternity Clipper** substitutes the cryptocurrency wallet address of the intended recipient with that of the attacker. It is sold for $99.

The **Eternity Botnet** (also named **Eternity Dropper**) allows an attacker to perform DDoS attacks using different methods (HTTP, TCP Flood or UDP Flood), and to drop files on the infected host using UAC bypass. The agent builder and the administration panel are sold for $150 a month.

The **Eternity Worm** is able to spread itself over documents, USB, Cloud, and Discord. The price for Eternity Worm is $300 and the source price is $1200.



ETERNITY WORM

SPREAD MALWARE OVER DOCUMENTS / USB / CLOUD / DISCORD

FEATURES

- USB Drives
- Local Files (py, zip, exe, bat jar, pdf, docx, xlsx, pptx, mp3 mp4, png)
- Cloud Drives: (GoogleDrive, OneDrive, DropBox)
- Python Interpreter (Injects worm loader into all compiled python projects)
- Discord Spam (Sends your messages to all channels and friends)

CONTACTS

Telegram:
https://t.me/EternityTeams

Jabber:
LightMan@thesecure.biz

Figure 3. Eternity Worm advertisement published on several underground forums

The **Eternity Ransomware** is only advertised on their Telegram channel. According to EternityTeam’s description, it is a generic ransomware that encrypts all documents, photos, databases on disks, local shares, USB drives, removes system restore points and deletes shadow copies, among other classic features.

Webinar : How to improve the Analyst Experience with Sigma Correlation

Date : May, 31st – 4:00pm

Focus on the Eternity Stealer

As mentioned in the introduction, we discovered the threat group, and its malware catalog, in February 2022, shortly after its emergence, during our Dark Web monitoring. We managed to find a sample of Eternity Stealer on a file-sharing platform, and we quickly analyzed it.

Eternity Stealer is a complete information stealer written in .NET and sold with the malware-as-a-service model for $99 per month. The malware targets personal information from:

- several browsers (passwords, cookies, credit cards, autofill data, history, and bookmarks);
- browser cryptocurrency extensions;
- cryptocurrency wallets;
- numerous applications (password managers, messengers, VPN and FTP clients, and gaming software).

We found that Eternity Stealer is able to steal credentials of Growtopia accounts. Growtopia is a game with almost endless possibilities for world creation, developed by the French video game company Ubisoft. This stealing capability echoes the profitable and illegal business of Roblox (a mega-popular gaming platform) account theft, often targeting young players. As mentioned in the Vice article, attackers stole over ten thousand dollars worth of virtual items in a few minutes. Information stealers targeting video game accounts is not a new trend, but it later appears to be on the rise. This business can be very lucrative as huge virtual markets exist for many video games, and the targeted users are often young and not very careful concerning cyber risks.

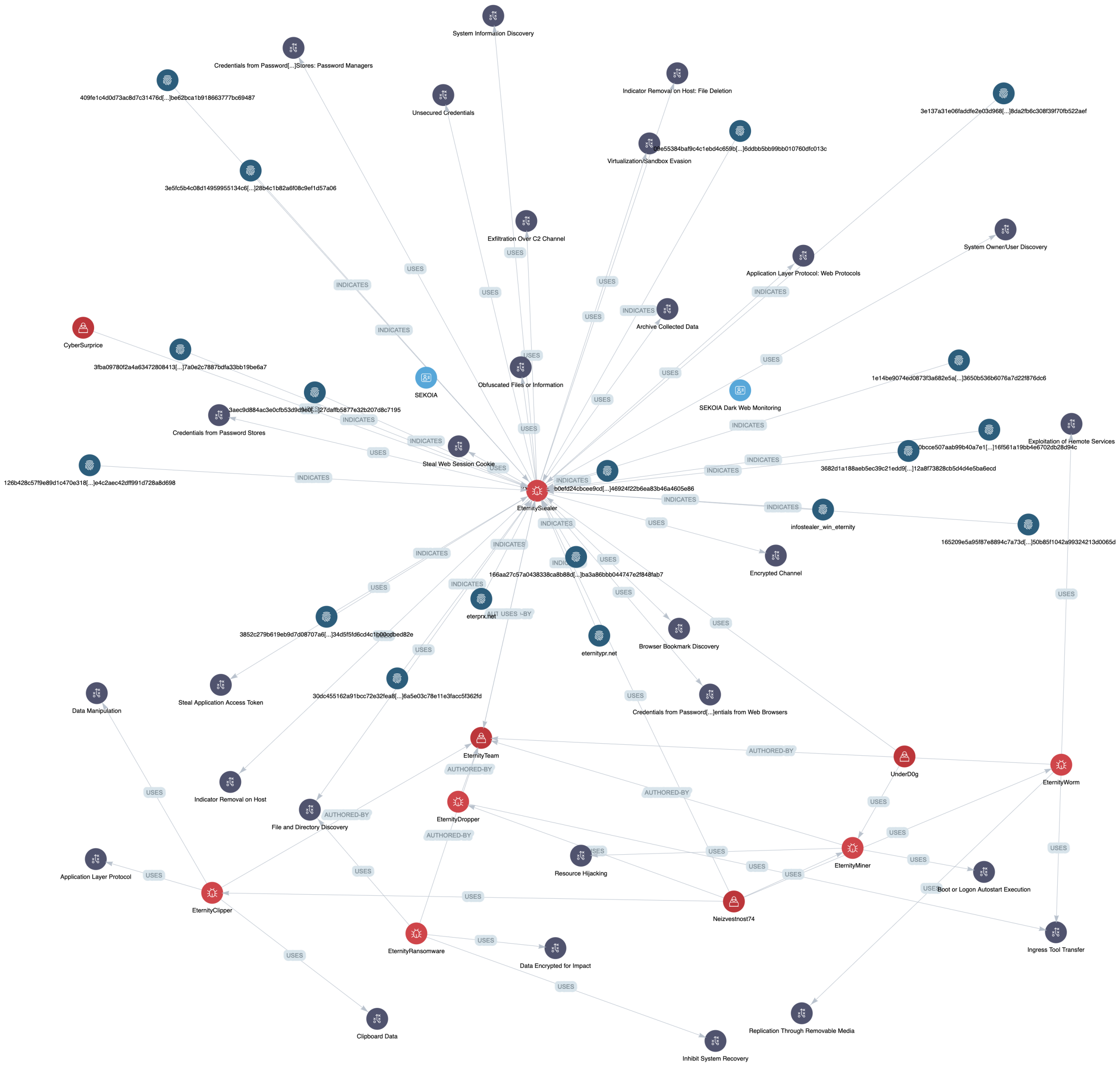
Investigating Eternity Stealer samples confirm this trend. Indeed we found some samples distributed as a glitch program for Growtopia (“*Growtopia Growtoken Glitch 3.82+.exe*“), or a cracked version of Growtopia (“*Growtopia_Hack_3.82.exe*“).

Regarding data exfiltration, Eternity Stealer sends the stolen data to the Eternity Team servers via HTTPS POST requests. Data is then redirected to the attacker on its Telegram bot.

SEKOIA.IO Threat & Detection Research Team will continue to monitor EternityTeam activities, as well as their malware catalog to provide contextualized and actionable intelligence on these threats.

In conclusion, information from our Dark Web monitoring is **a data source in its own right**. The results allow us to **identify trends and emerging threats**. SEKOIA.IO analysts then make this information **actionable** for our clients.

Discover some of our previous investigations about other information stealers such as Mars Stealer or how ransomware groups weaponize such tools, as was the case with Spook leveraging the Thanos builder.


System Information Discovery
Credentials from Password[...]Stores: Password Managers
409fe1c4d0d73ac8d7c31476d[...]be62bca1b918663777bc69487
Unsecured Credentials
Indicator Removal on Host: File Deletion
3e137a31e06faddfe2e03d968[...]8da2fb6c308f39f70fb522aef
09e55384baf9c4c1ebd4c659b[...]6ddbb5bb99bb010760dfc013c
Virtualization/Sandbox Evasion
3e5fc5b4c08d14959955134c6[...]28b4c1b82a6f08c9ef1d57a06
Exfiltration Over C2 Channel
System Owner/User Discovery
Application Layer Protocol: Web Protocols
Archive Collected Data
CyberSurprice
3fba09780f2a4a63472808413[...]7a0e2c7887bdfa33bb19be6a7
SEKOIA
Obfuscated Files or Information
1e14be9074ed0873f3a682e5a[...]3650b536b6076a7d22f876dc6
SEKOIA Dark Web Monitoring
3aec9d884ac3e0cfb53d9d9e0[...]27daffb5877e32b207d8c7195
Credentials from Password Stores
Exploitation of Remote Services
0bcce507aab99b40a7e1[...]16f561a19bb4e6702db28d94c
Steal Web Session Cookie
3682d1a188aeb5ec39c21edd9[...]12a8f73828cb5d4d4e5ba6ecd
126b428c57f9e89d1c470e318[...]e4c2aec42dff991d728a8d698
b0efd24cbcee9cd[...]46924f22b6ea83b46a4605e86
EternityStealer
infostealer_win_eternity
165209e5a95f87e8894c7a73d[...]50b85f1042a99324213d0065d
166aa27c57a0438338ca8b88d[...]ba3a86bbb044747e2f848fab7
Encrypted Channel
eterprx.net
3852c279b619eb9d7d08707a6[...]34d5f5fd6cd4c1b00cdbed82e
eternitypr.net
Browser Bookmark Discovery
30dc455162a91bcc72e32fea8[...]6a5e03c78e11e3facc5f362fd
Data Manipulation
Steal Application Access Token
Credentials from Password[...]entials from Web Browsers
EternityTeam
UnderD0g
EternityWorm
Indicator Removal on Host
EternityDropper
File and Directory Discovery
Resource Hijacking
EternityMiner
Application Layer Protocol
Boot or Logon Autostart Execution
EternityClipper
Neizvestnost74
EternityRansomware
Ingress Tool Transfer
Data Encrypted for Impact
Clipboard Data
Replication Through Removable Media
Inhibit System Recovery
USES
INDICATES
AUTHORED-BY

IOCs & Technical Details

Eternity Stealer C2 servers:

```
eterprx[.]net
eternitypr[.]net
```

Eternity Stealer SHA-256 hashes:

```
09e55384baf9c4c1ebd4c659b86c20f0ef6c7846ddbb5bb99bb010760dfc013c
126b428c57f9e89d1c470e3184147c289e9e11de4c2aec42dff991d728a8d698
165209e5a95f87e8894c7a73d108434f82c0e0f50b85f1042a99324213d0065d
166aa27c57a0438338ca8b88d751d8be91d81a6ba3a86bbb044747e2f848fab7
1e14be9074ed0873f3a682e5af5fe61948475713650b536b6076a7d22f876dc6
245d50bcce507aab99b40a7e187c4a53e435da416f561a19bb4e6702db28d94c
30dc455162a91bcc72e32fea809a9a1480492ff6a5e03c78e11e3facc5f362fd
31a113ebe2b0efd24cbcee9cdfbe4959368419e46924f22b6ea83b46a4605e86
3682d1a188aeb5ec39c21edd915e286f23fc76112a8f73828cb5d4d4e5ba6ecd
3852c279b619eb9d7d08707a66d6bc2a8118d7334d5f5fd6cd4c1b00cdbed82e
3aec9d884ac3e0cfb53d9d9e0ced5d2b173017227daffb5877e32b207d8c7195
3e137a31e06faddfe2e03d96895c748084d47318da2fb6c308f39f70fb522aef
3e5fc5b4c08d14959955134c6f28bb939dbc18528b4c1b82a6f08c9ef1d57a06
3fba09780f2a4a63472808413887dd5201e78707a0e2c7887bdfa33bb19be6a7
409fe1c4d0d73ac8d7c31476d96bed92fb67921be62bca1b918663777bc69487
a428cce6ed823b8d63c251f84cede5b9b127c7c67699aa77da723dd4b79af0aa
c13e2b1821a4221d8b863e726c181131439ba0110999c12f943ed4f309fb035a
05f636dc9dd4e75a187e5c6eed4acaa9c51de1727c9ea744570f19d0091ec007
81f4a6d3b836ca31aa31b2a318b177631c54f1e41f08f6b6a2a7150433729938
826630786821ba231e6843fc949a833ec695511ad96da162fbbf040878002083
f40b21888e97fd44afa76344cf8eae4f48aa24654482042a03ce94472f72f221
e03181411fd119fae6633218dc0c742e15dadbff2d156c821195649b4af02998
0195e11cb02a1f3e050fab8522abf3246f42910d583d7b41f33a49fffe0beb60
b7e5a2b07ef23f3eb2fd199589ecf5ada9ca920f446ef4e48d95c6f371292fa9
aef43ba0cae68b2d69af9ade247c64b6a24dafa1c22b9fda9c087b2d4faf2eeb
519854c9bfbb3d3bd0be42dcb25712d1567b2f35c3ef4fe03b2132fa96057393
859231cd841df8d01279b321b8e89d07d070a7162ee9b768e453caebd1035d18
68aa0a6d2dc873ddd8506fc8d76f2ecb5e16f297d258ed1f3409eac06f89d290
a8ae8b85db65241159faf6df3427858e72377d66c959952133acbf074964a768
c157f0aa2913d15866b4a55489e3e78c27ecc3005036923bf89011f1e6c9ab76
911b668dfe39f12368935c48b062f64153ae4b5d0acae67dd3d67306ff77ed3a
ef36b26d3823f02101a43163dd7868b76e87b845f4231cb606e891b8f684d834
99350c906761346c503b6fb058be626171fbf4865ce9bedc139c67aadb1ea165
600212c819e76234c7d7d81e38a62ef49c2939a7de7223b28d8d2049454ce74a
1a402676a4436aff52d27186edac7cbc02f282d2168d9ff48fc3cd61900ba9ce
5b5908988bfd53e29ada48b33839d6c732f290bacaab537b74b719d54d54325d
10ea4054a6755a5188466e9a34b21cc12b003e2d929a924cbf00d982e2e13d48
9d8efdc07b00d6dcc48c020be21ecdaaf220a2567edb942644a15f1795aa0f12
788ae87ec85623435fa2742bbcccfe9ee2c11bbdefcf0b63ec59e53d94d74e6f
1ff552dcd636c5601b4389566c417daef7fcc3887b29ac35fa71f9e727c2cd72
7b933b60011e9d0bd9412ac7f37491f0ce4b08c2a2b09264269a637d88adc7ec
e39993f219117284db8cc1d47b88c68b7af845bad23bfcdcfd01636f4582a8e6
a1402fd77cce7eb6ab989c0b014d2e0999a89519a3e2cda166bdd11adb86146c
a5c1a01d64ddc8f26f9582911f1e2973843988866afc9501fd7c8d1d1724ebcd
298cd2cc2b9193605e00caaee02e2463c8329f3db70c615afad7f8f6c9f39535
d527570ccfdfde1cf0f4d37bf44563fb8f1c4215cd17464a868ecaa45501d613
a51aa87ae265c34e1a79c8287481b167dad9df926eb14d17e0ae265093808689
46e518dc61b63cc253641e9927383e058b816d7402a3447563ee8770892b59a6
8e5abfcfbd4e09bca6e58c38c201d6bd159c76e137c499d261a0175c10385f84
b899f3da3c71401a7dd9768eb78570bfdf9745cb63823eca378545320e58a4dc
92624a6ffe39c33192aaced2c1d94ebbc18cd6aee530df80ab25e7e8b986197c
7dfd5b26bab1e10bef45782211e12438f426717f1a81e5da709d0c7a4bbb3c2a
6726a7edafc2cebf7876d3ef8ae1fb448ccbfec917e3e7d64c7a334b44eafd2c
5af8eaffc3aab828331b085abfb575c323cfc95fe34078ec6b28dd1ba098dbf0
576d801fcca70ab4b97fe7b1d2ddeec3b1ab2eeb03a2aaecb97dac4f015333a9
```

```
cc61c79640e70080a10ed98a7aea4f73104af59e6f31d42ef76f62400762bb21
1e6d64869761427efbd3b5d4344768776e4e4dacb9900b1aab0d0c17b8574e2f
5033fa9ad2d44b3eac74bee121f4a9cd759202cb49a2e019f08faeedbe4ed5a3
e059fe759120ddc381561b671d84b68babff7a5aa2f8df8a148c40e8ec996f50
0fa0917455a0fdb7f7e1210ccb28c9e35dfc4329776309de8cf67b91f805df79
f28dab909f51c0bdb9b4d59249600e4e92d5e5eef7602041997e1fcf4a771301
0064c22385b6cc7641e3a888062c8d9ad30ced13bbdaf3b976ea7905b1ad4be0
f35155fcf26e6e029ecbb19aadc91935b201f42d8001855bcef73c0b820b22b9
9b272e20c6f1fa2db2b1c8aedd260683c223548f92e52b04d5444a3c3ca2cb7b
93ffcfa46b75b09efde95169523515789602 8b5b78a71e655ad4245f1d0b26cf
38bedad9001a36172551ec25de82d661f595e347df23dcac9531d450ab8305e5
99dacfaffe443309956d4ffa10b58e5c87de6c73339473712d9ade2cda57c923
7f6ab1b61d261bd2875399b4281ed8b87c0cc2cb4bfe0c9a102fb0ff7d291e3f
ec0d6d1f8fb9f376a0f332b17e7316ba06b2049878e91d1631cd3921e63dc0dd
9ffe4402cdb5794143f1caf029154cb0e923f9089e01cfb78f4c4d82f1f548a5
b8575fbb226bbe496ec821ee093bcd2455eb34deb967b41782bf86989c99b673
fc43f7f5af5be42d3a5fda928dda968118fcafcc08f73aa694bd575a3ef117d8
97dc31d88caaa42709550fceeb4901713c4aebbd8efddfdec3ab67eb0baa5683
ea68e9a8ebf94ab76b3546d15a12d1fd0f32ecd3ff42286eda76be084bd0c2a0
4423af11e0271c5eaee4ebf34841f9fa2419069581844533b821aaca5c8cb2f8
d7254d08ccfeef82e11bb670f1dade3e144c139c189f013a8f2598ba5a85827d
166bfdef3d7ff470cc266a011f41abece798f3a18b195fde44b9eb9be625b9df
9634a426c27b291355fad176acd086abbd0535c9260458b47640302c9dcbe7fb
eb812b35acaeb8abcb1f895c24ddba8bb32f175308541d8db856f95d02ddcfe2
d4f4debfe7d20a195dd5d2cf0853f21807fa6ab0152b3f0b3ac02e6a388ebdf8
9a129a6ea7edd1553f948f48a581c4ad6e1ebf5e504dbd9c44e22517e4e86f28
e33528dad511e9c09ec3bc66499fcb4b388cdcf0757a830192ae030f7ce7bd73
8892a97cb26dd49886b9f9e1f11bbdc3abf2f40a5b8a543257461ea0c79a9269
a2986810a3bdeeeab764b0a3ecc4e8befad6ceb9b52dbe51a1698d0579ddd0f0
ff75df6f9819b4522f6319bf7abf05221473066f4c955074187a91b9459cef8a
f98b17f45d29f817e0debcd92756512acea397250fcfdfffdf12d78653f58fa9
be66b87a75d34df9b483a62287295063c9f89c9778d0b459a66e95b88fe5a7f6
e42e75d7f8e2b48cfd005ad30435d521ca05a107adc7944c2467fea7266dbb81
c917c2bd1643d4c9cfc821a084f1d4b93a7787c97ced7de2083adde083dbdd32
ce74ce22527dff2dcdc94c32c8a48ef57bae0a9cfe2bbefada621b747fd6355a
fd4c85e7d9683cf7ea50317260a491a5b1f988c8e2d480afbc9d2b8901d0179b
e618fb92617c97fa5b16420167b982416c21b1788cf51f7bd462af6d1acd341c
0765e1261030d068e6061ec961a959a355ef03b0cf944961ff0404f1f9046d09
19981056b66a1cb7bad210e55bf5028c435f392041ab8e62933caae7e20e4ebc
756969b63bb99406b42e1f0c75008b8d033f4a2531e6af8d009109bb17785745
aaa7b14145369e5756a7d23cdff28b2a9e52a1495d6a01ac9dade3f5afcb7265
52bb26050b07afd109d6a1d8fe7f88d9855cbf097276e46ff25a33ed4cd2eb61
39bf22e3efc458cf4824cffcfb7e8649319fd2bd862ca84b6d87a91e41d0ca05
e1c9ad3550affab7fb40c22b37399fec61fba46632aa65db1aa8b2223b7fca7b
27a4428288cc2835cd3a124b80880e3eb6c8485691616f785767ffbc38b26efd
43590fcdc469dfef103797723d09e9d1e5de6a798d449dfc685c9c17589fadff
27f9c8399b5aa4324759ba1bec08c520fcb9221e97b4b0fd8963c9c0e279bdb4
28d8f09f9e35fa440ec8371cc78365b93aa5526cb38a7eb2ab74cfa3ce9a5196
0dca5ace3971a93ea570fc49003a8d35b69c76449a70664b0cb1ec989b253b9a
bb2d701f2ac6982afe79e5b1f21dae9ed54f5b46f4a75db280c827f68891172f
7777a06da25535658da605d65e49e801dacf6b9d4955016247184 7186ce3c31f
727e642f947dbd42cb59e97ff6b99dd00ed4216308bb71e48fd647b4c8c3d337
93ca0085c47a2246a9bad50dd6aa0a6919f723b530880af8a83db1e3e3067221
e68ebf69f8199a8e867b84a60955c0eaf393e2f8da6ff598de5c77466b9699b2
a3f81a6c2bc1da49e5729d182353ebfe59f6bfe121556bcbe339eb7126da78a2
```

```
82fa086803d681e951436ded0f129592b80567e78d51b03092f75714f7bf6315
dd3c04a44b4353f3eb4386352041bc217a868d00f4728b397758bef3854ed333
6940959af8bcc4efa84801ba9be324f1623049ffc06ee594e89903214f5b9628
16dec1fe2067b0a7de84fbab21b8e766a23d61443a0a3a2a1c5e754e12e71487
cffa6b568bb6b90858311e93d6cd5117a9ec9a2de491b79838c2634f13472796
712d11522b19a1cf1c6e026aa78cdc239aec6ce24d84b6a89b901ce9bb4eb5fe
54a813951d785e6b7946de41a5be03486d6827a32ceed20fd74d4274ff0a900f
aabd09d784d25a2857bef4e433b8acee7151fa125d523025b4f6bc2d875f4d11
c982fa2c8dd19ad9c5f289a031ad71e5116004733e25bdbb58c00786a177a235
5c82185c5701c73d77a1fcb0d4d18dcec679687fe8d014bdf2c95e4114be46a4
930c0a0ff2bfa76fa45d394e09e2e0716eb96e229bb9aaa01dc5bb1650929d70
c6d2b498b4080c788362f51aba32065ea5531bc2a38f8e06c5ed0a104ff9d1f0
fbd896ac261b78ede37290c0f5e6b236dc5aeb9a1de573fa760871ea3f03ea00
0b838ca129f55887d9013748bc114df9530fe53c8392826603baab926c9bce10
ca63473125b8f48f075af1119c7ec080c2ec8f25aee0f9068a3cd0f5873d67aa
01207ce98db20f18da3ed68f933a001152b7d7809b7135e0a6535018cc175c0d
fe3a933806cb53f2b3027e171db2e470972a8791e2a4f3bc3c34b75ae652442f
67ed1389d89673f64c0235bbc767ba9210040c0aa478433288c22397a363a6f0
783502f920356f306c112adc485de195bf7797bad3ff2308f44fd1f1d8f27513
92267ace82e852bf55308f224629217957b7c00c5c6bd1191c605df0a7669189
95d9dd6ee61e580c857552c0a3f0a8c80db1b403704498b2032c72540acc5580
82142a98dcbad144cfdfbc66dec431e68352bd989acb49d977f01209be00ba49
```

YARA rule

```
import "pe"

rule infostealer_win_eternity {
    meta:
        malware = "Eternity Stealer"
        description = "Identify Eternity Stealer samples based on specific strings \\
        or PE section names"
        source = "SEKOIA.IO"
        classification = "TLP:WHITE"

    strings:
        $str0 = "Sending info to Eternity.." wide
        $str1 = "Debug mode, dont share this stealer anywhere." wide
        $str2 = "\\Growtopia.exe" wide
        $str3 = "Software\\Growtopia" wide
        $str4 = "Corrupting Growtopia.." wide
        $str5 = "Disabling Task Manager.." wide
        $str6 = "Deleting previous file from startup and copying new one." wide
        $str7 = "Hiding file in Startup folder.." wide
        $str8 = "Initializing File watcher.." wide
        $str9 = "Decoder: Failed to delete temp login. No problem, continuing.." wide
        $str10 = "dcd.exe" wide

    condition:
        uint16(0)==0x5A4D and
        (for any i in (0..pe.number_of_sections-1): ( pe.sections[i].name == ".eter0"
) and
        for any i in (0..pe.number_of_sections-1): ( pe.sections[i].name == ".eter1"
)) or
        6 of ($str*)
}
```

Chat with our team!

Would you like to know more about our solutions? Do you want to discover our XDR and CTI products? Do you have a cybersecurity project in your organization? Make an appointment and meet us!

Contact us