A closer look at Eternity Malware

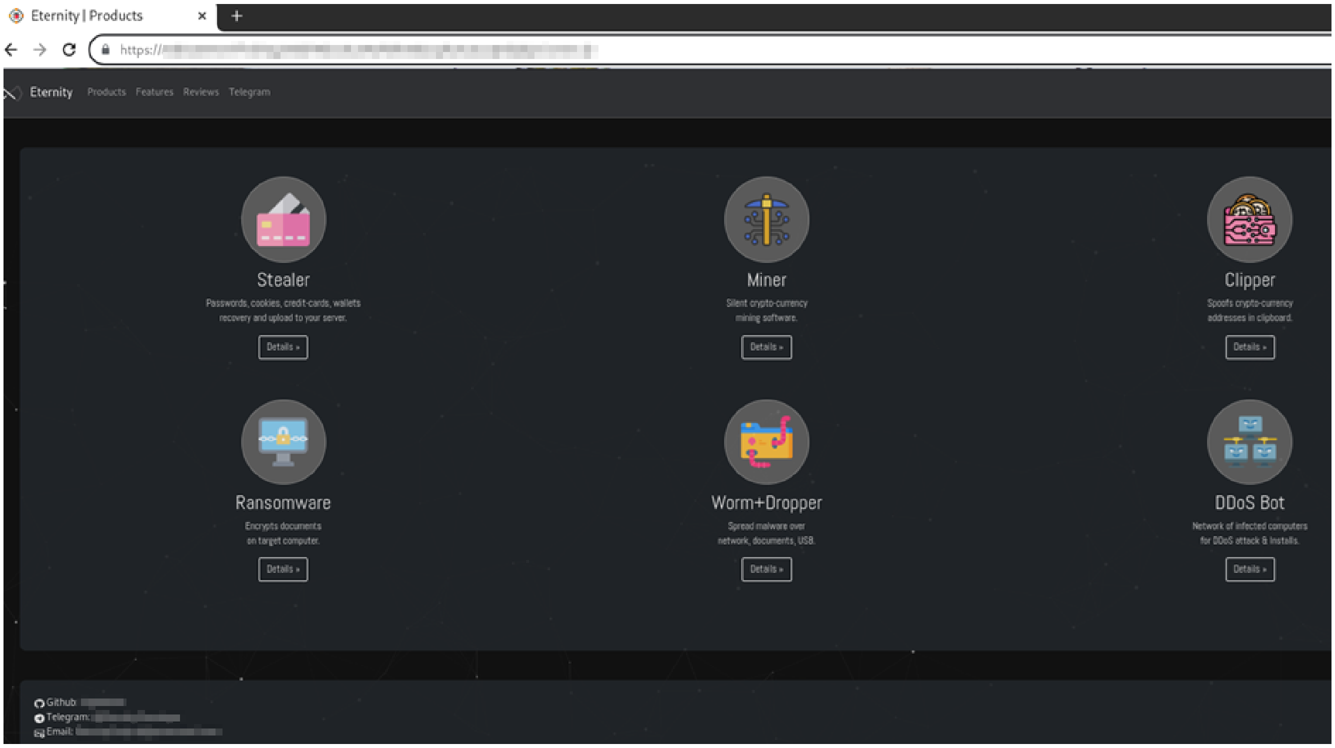
blog.cyble.com/2022/05/12/a-closer-look-at-eternity-malware/

May 12, 2022

CYBLE
A CLOSER LOOK AT ETERNITY MALWARE
THREAT ACTORS LEVERAGING TELEGRAM TO BUILD MALWARE

Threat Actors leveraging Telegram to build malware

During our routine threat hunting exercise, Cyble Research Labs came across a TOR website listing a variety of malware for sale. This includes stealers, clippers, worms, miners, ransomware, and DDoS Bots which the Threat Actors (TAs) have named ‘Eternity Project.’



Eternity | Products

https://[redacted]

Eternity Products Features Reviews Telegram

Stealer
Passwords, cookies, credit-cards, wallets recovery and upload to your server.
Details »

Miner
Silent crypto-currency mining software.
Details »

Clipper
Spoofs crypto-currency addresses in clipboard.
Details »

Ransomware
Encrypts documents on target computer.
Details »

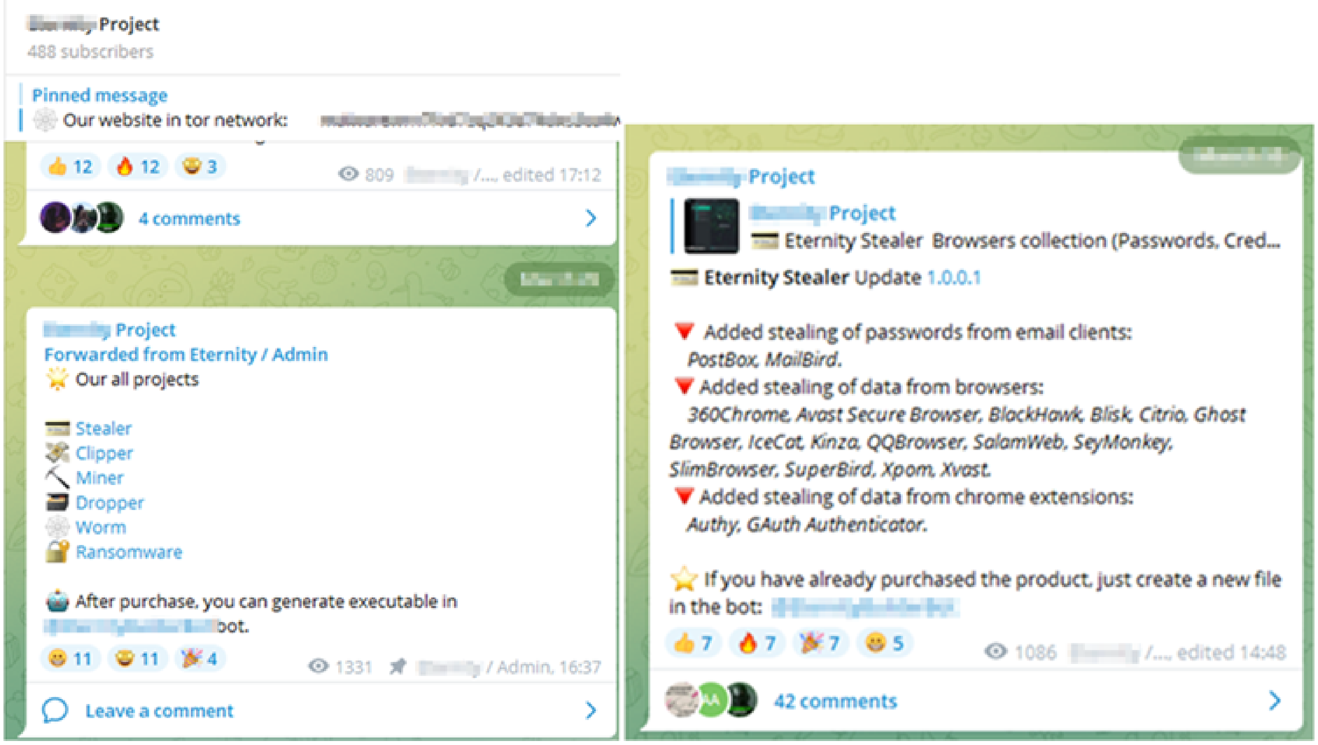
Worm+Dropper
Spread malware over network, documents, USB.
Details »

DDoS Bot
Network of infected computers for DDoS attack & Installs.
Details »

Github: [redacted]
Telegram: [redacted]
Email: [redacted]

Figure 1 – Product Information

Upon further investigation, the TAs also have a Telegram channel with around 500 subscribers, where they have provided information about the malware's operation and features through detailed videos. The Telegram channel also shares information about the malware's updates, which shows that the TAs are actively working to enhance the features of the malware.



[redacted] Project
488 subscribers

Pinned message
Our website in tor network: [redacted]

👍 12 🔥 12 😁 3 👁 809 [redacted] /..., edited 17:12

4 comments ›

[redacted]

[redacted] Project
Forwarded from Eternity / Admin
Our all projects

Stealer
Clipper
Miner
Dropper
Worm
Ransomware

After purchase, you can generate executable in [redacted] bot.

😁 11 😁 11 🎉 4 👁 1331 [redacted] / Admin, 16:37

Leave a comment ›

[redacted]

[redacted] Project

[redacted] Project
Eternity Stealer Browsers collection (Passwords, Cred...

Eternity Stealer Update 1.0.0.1

🔻 Added stealing of passwords from email clients:
PostBox, MailBird.
🔻 Added stealing of data from browsers:
360Chrome, Avast Secure Browser, BlackHawk, Blisk, Citrio, Ghost Browser, IceCat, Kinza, QQBrowser, SalamWeb, SeyMonkey, SlimBrowser, SuperBird, Xpom, Xvast.
🔻 Added stealing of data from chrome extensions:
Authy, GAuth Authenticator.

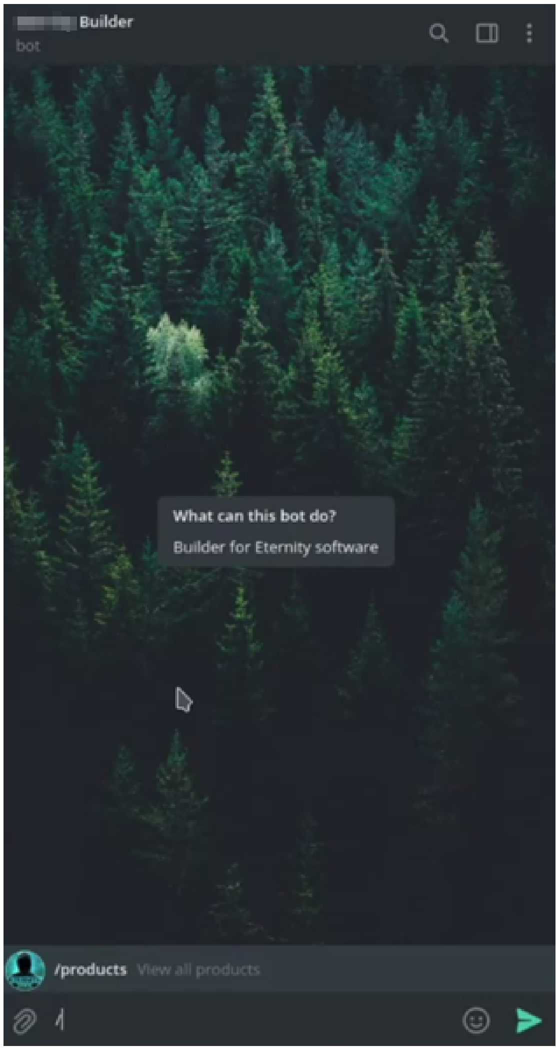
⭐ If you have already purchased the product, just create a new file in the bot: [redacted]

👍 7 🔥 7 🎉 7 😁 5 👁 1086 [redacted] /..., edited 14:48

42 comments ›

Figure 2 – Telegram Channel

Interestingly, individuals who purchase the malware can utilize the Telegram Bot to build the binary. The TAs provide an option in the Telegram channel to customize the binary features, which provides an effective way to build binaries without any dependencies.


[redacted] Builder
bot

What can this bot do?
Builder for Eternity software

/products View all products

Figure 3 – Telegram Builder

This blog showcases our research on Eternity Project’s malware capabilities and steps to secure yourself and your organization accordingly.

Eternity Stealer

The developer sells the Stealer module for $260 as an annual subscription. The Eternity Stealer steals passwords, cookies, credit cards, and crypto-wallets from the victim’s machine and sends them to the TA’s Telegram Bot.

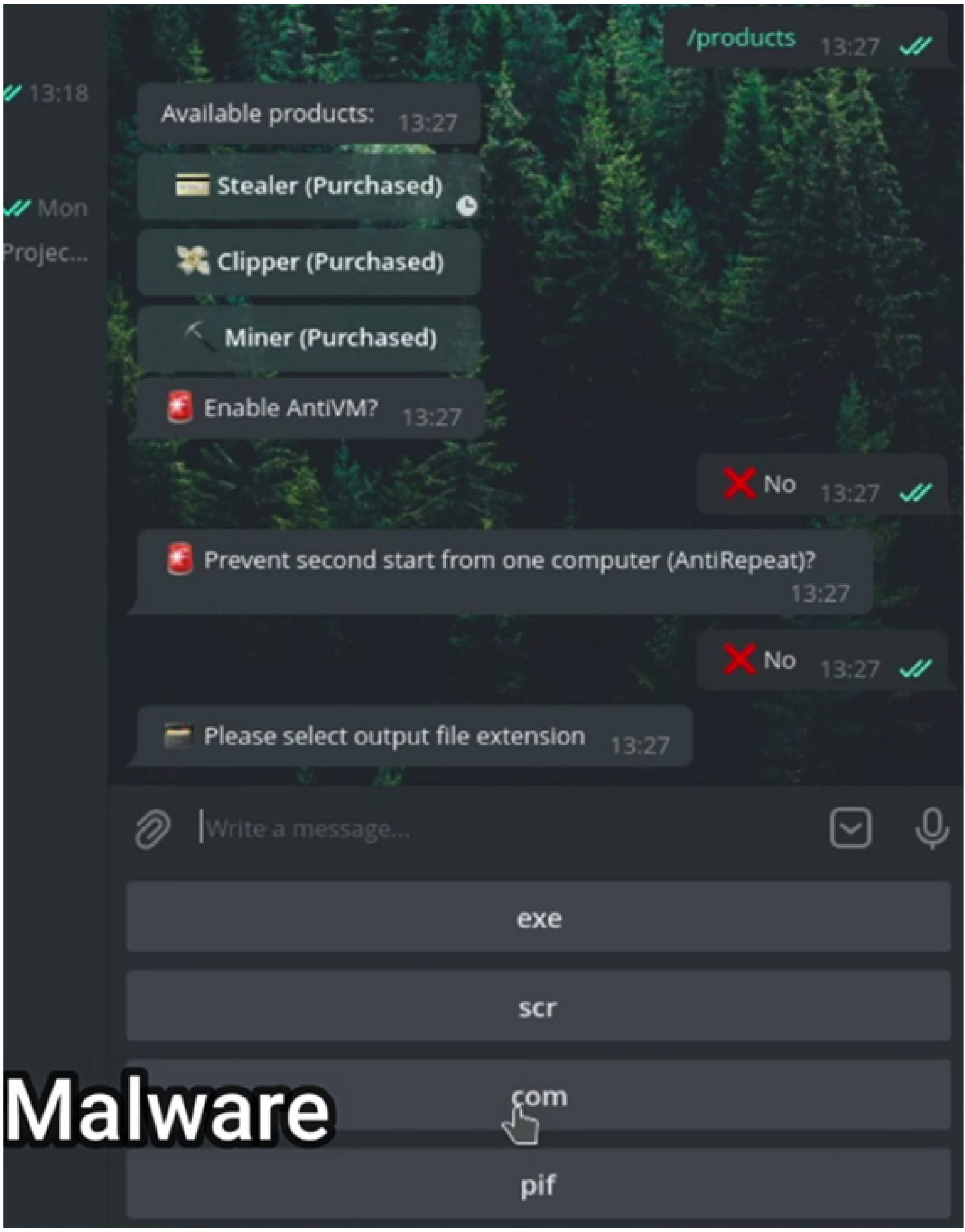
The features of the stealer malware mentioned on the TAs website and Telegram channel are:

- Browsers collection (Passwords, CreditCards, Cookies, AutoFill, Tokens, History, Bookmarks):
- Chrome, Firefox, Edge, Opera, Chromium, Vivaldi, IE, and +20 more.
- Email clients: Thunderbird, Outlook, FoxMail, PostBox, MailBird.
- Messengers: Telegram, Discord, WhatsApp, Signal, Pidgin, RamBox.
- Cold cryptocurrency wallets: Atomic, Binance, Coinomi, Electrum, Exodus, Guarda, Jaxx, Wasabi, Zcash, BitcoinCore, DashCore, DogeCore, LiteCore, MoneroCore.
- Browser cryptocurrency extensions: MetaMask, BinanceChain, Coinbase Wallet, and 30+ more.
- Password managers: KeePass, NordPass, LastPass, BitWarden, 1Password, RoboForm and 10+ more.
- VPN clients: WindscribeVPN, NordVPN, EarthVPN, ProtonVPN, OpenVPN, AzireVPN.
- FTP clients: FileZilla, CoreFTP, WinSCP, Snowflake, CyberDuck.

- Gaming software: Steam session, Twitch, OBS broadcasting keys.
- System credentials: Credman passwords, Vault passwords, Networks passwords).

Figure 4 demonstrates the steps to build Eternity Stealer malware through the Telegram Bot. Initially, the Telegram channel shows available products to users who purchased the malware when they enter a command **/Product**.

Once the users select the stealer product, they are presented with further options for features such as AntiVM and AntiRepeat. Finally, the user has the option to select the available payload file extension such as .exe, .scr, .com, and pif. After selecting the file extension, the user can download the stealer payload from the Telegram channel.



/products 13:27

Available products: 13:27

Enable AntiVM? 13:27

No 13:27

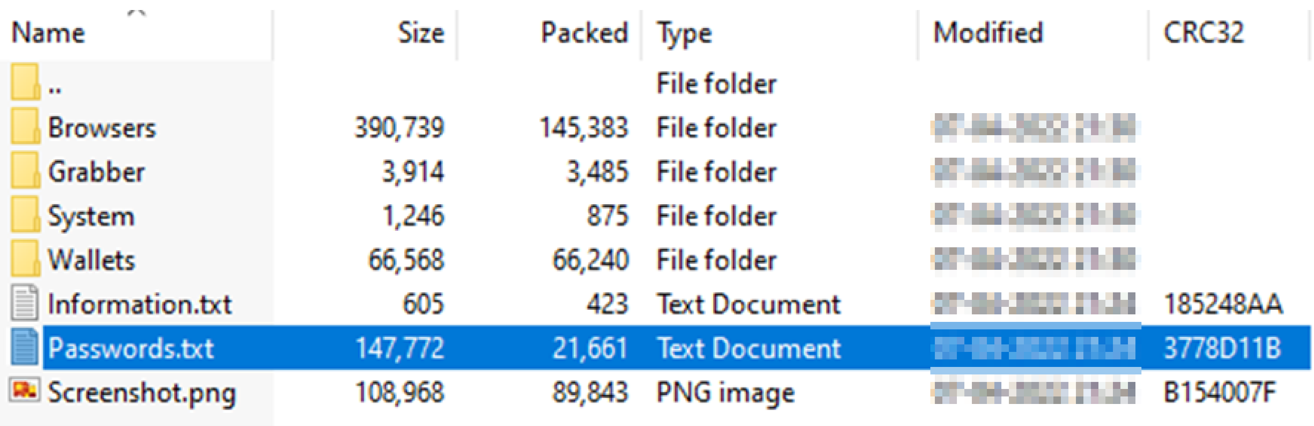
Prevent second start from one computer (AntiRepeat)? 13:27

No 13:27

Please select output file extension 13:27

Figure 4 – Purchasing and Building Eternity Stealer Payload

The stolen information is saved in *.txt* files, as shown below.



Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Browsers	390,739	145,383	File folder	[redacted]	
Grabber	3,914	3,485	File folder	[redacted]	
System	1,246	875	File folder	[redacted]	
Wallets	66,568	66,240	File folder	[redacted]	
Information.txt	605	423	Text Document	[redacted]	185248AA
Passwords.txt	147,772	21,661	Text Document	[redacted]	3778D11B
Screenshot.png	108,968	89,843	PNG image	[redacted]	B154007F

Figure 5 – Stolen Information Saved in .txt files

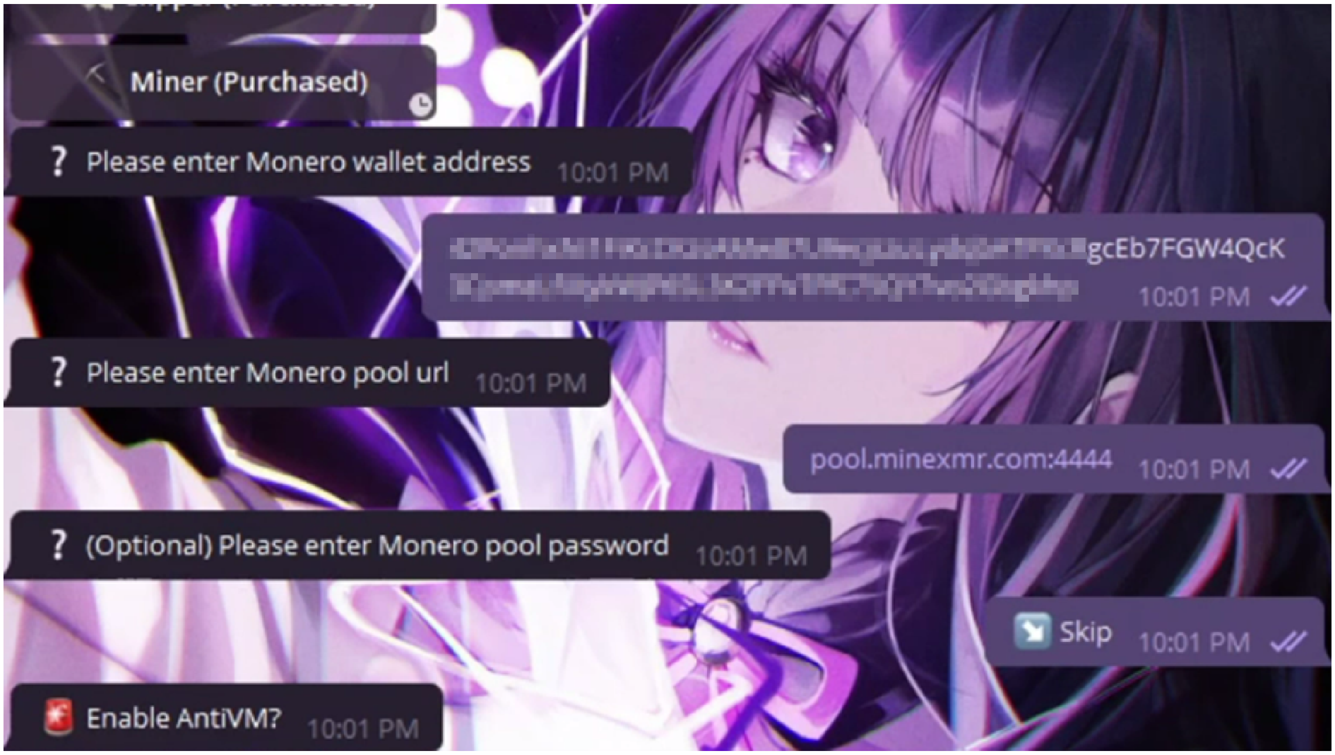
Eternity Miner

The developer sells the Miner module for **$90** as an annual subscription. The Eternity Miner is a malicious program that uses the resources of an infected computer to mine cryptocurrency.

The features of the miner malware mentioned on the TA's website and Telegram channel are:

- Startup
- Small size
- Silent Monero mining
- Restart when killed
- Hidden from the task manager

Figure 6 demonstrates the steps to build Eternity Miner malware through the Telegram Bot. Here, the users can enter their Monero wallet address and Monero pool URLs while building the binary.



Miner (Purchased)

? Please enter Monero wallet address 10:01 PM

[redacted]gcEb7FGW4QcK 10:01 PM

? Please enter Monero pool url 10:01 PM

pool.minexmr.com:4444 10:01 PM

? (Optional) Please enter Monero pool password 10:01 PM

Skip 10:01 PM

Enable AntiVM? 10:01 PM

Figure 6 – Building Miner Payload

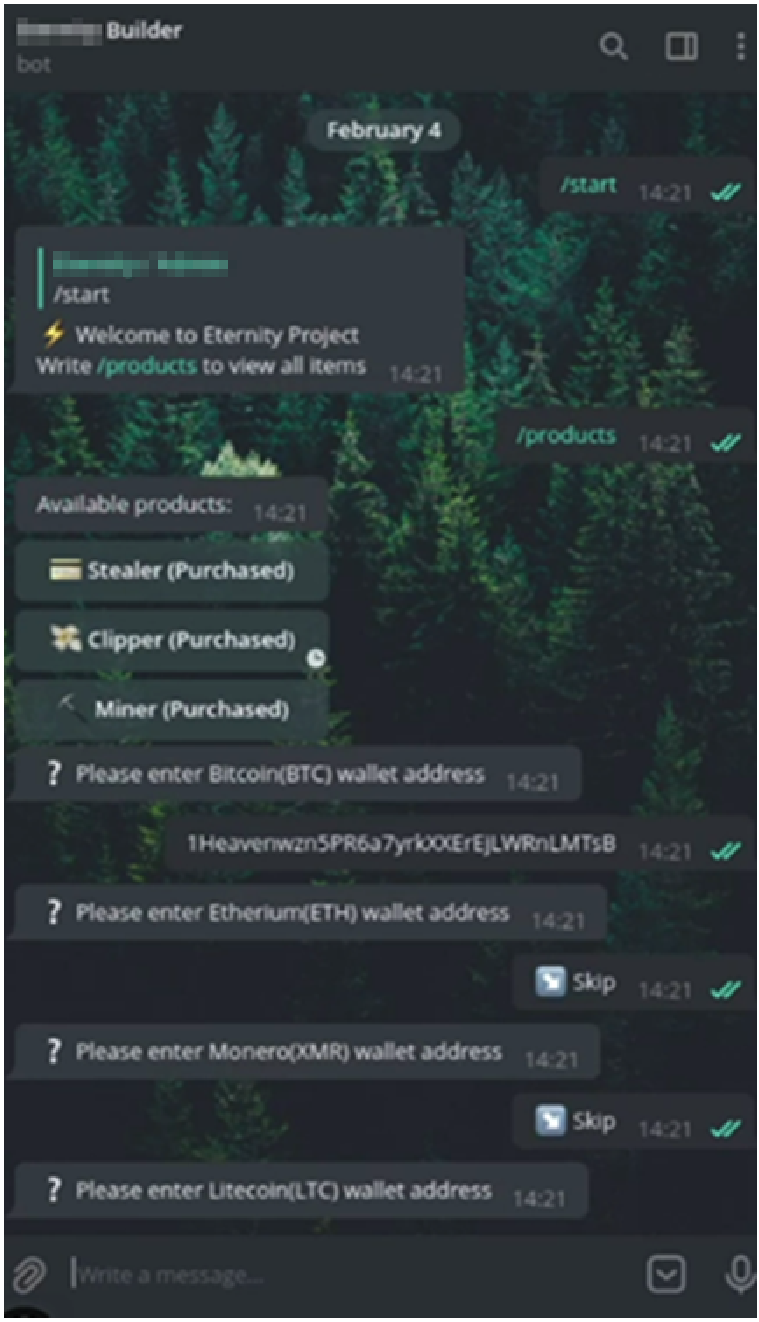
Eternity Clipper

The developer sells the clipper malware for $110. The Eternity Clipper is a malicious program that monitors the clipboard of an infected machine for cryptocurrency wallets and replaces them with the TA's crypto-wallet addresses.

The features of the Clipper malware mentioned on the TA's website and Telegram channel are:

- Startup
- Small size
- Hidden from the task manager
- Reporting to Telegram Bot
- Prevents second reporting of replacement to prevent spam
- Support of multiple address formats for BTC, LTC, ZEC, and BCH

Figure 7 demonstrates the steps to build the Eternity Clipper malware through a Telegram Bot. Here, users can enter their crypto wallet addresses while building the binary.



[redacted] Builder

bot

February 4

/start 14:21

[redacted]

/start

⚡ Welcome to Eternity Project

Write /products to view all items 14:21

/products 14:21

Available products: 14:21

Stealer (Purchased)

Clipper (Purchased)

Miner (Purchased)

? Please enter Bitcoin(BTC) wallet address 14:21

1HeavenwznSPR6a7yrkXXErEjLWRnLMTsB 14:21

? Please enter Etherium(ETH) wallet address 14:21

Skip 14:21

? Please enter Monero(XMR) wallet address 14:21

Skip 14:21

? Please enter Litecoin(LTC) wallet address 14:21

Figure 7 – Eternity Clipper Payload Building

Eternity Ransomware

The developer sells the Eternity Ransomware for $490. Eternity Ransomware is a malicious program that prevents users from accessing their machine, either by locking the system’s screen or encrypting the users’ files until a ransom is paid.

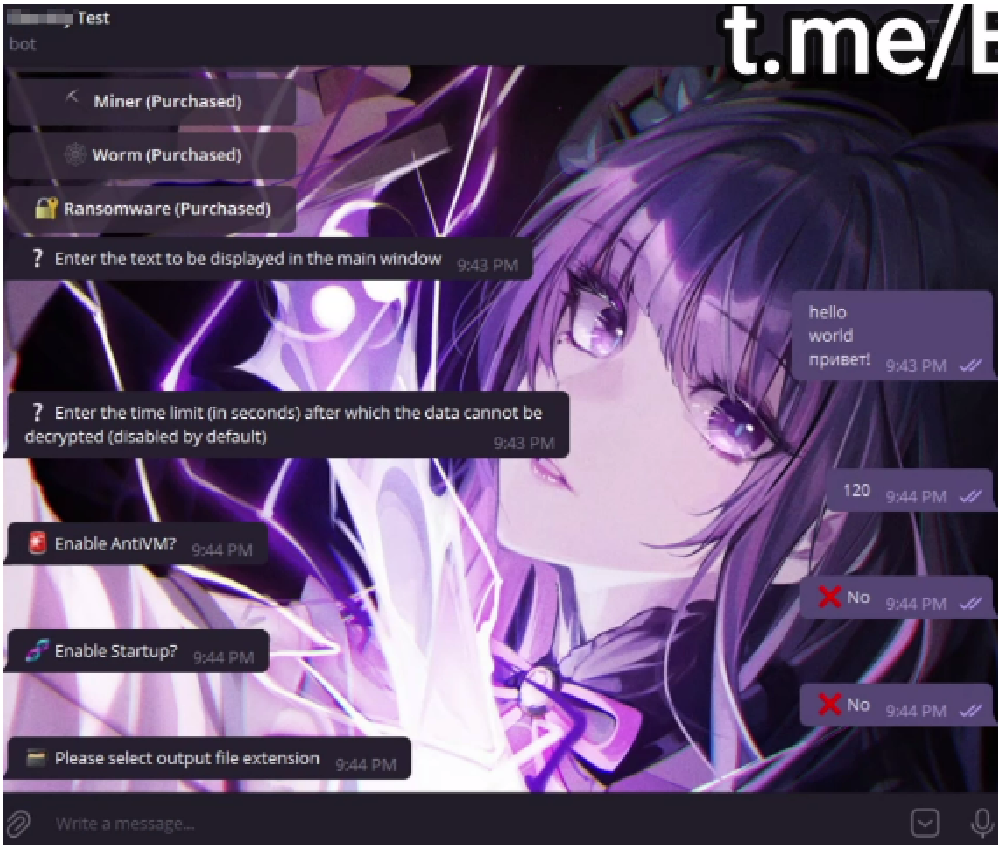
The features of the ransomware mentioned on the TA’s website and Telegram channel are:

- Encrypts all documents, photos, and databases on disks, local shares, and USB drives.
- Offline encryption (Doesn’t requires network connection)
- Uses a very strong algorithm of encryption utilizing both AES and RSA.
- The ability to set a time limit after which the files cannot be decrypted.
- Execution on a specific date
- Currently, FUD (0/26)

- Small size ~130kb

Figure 8 depicts the steps to build Eternity Ransomware through the TA’s Telegram channel. Here, users can enter text to be shown once the victims open an encrypted file. The TAs can mention the ransom notes and payment details etc., for further communication with victims.

Additionally, users have the option to enter the time limit for the ransom payment. If victims fail to pay the ransom within the time limit, the encrypted files can’t be decrypted. This is set as a default feature while compiling ransomware binary.



[redacted] Test
bot

t.me/E

? Enter the text to be displayed in the main window 9:43 PM

hello
world
привет! 9:43 PM

? Enter the time limit (in seconds) after which the data cannot be decrypted (disabled by default) 9:43 PM

120 9:44 PM

Enable AntiVM? 9:44 PM

❌ No 9:44 PM

Enable Startup? 9:44 PM

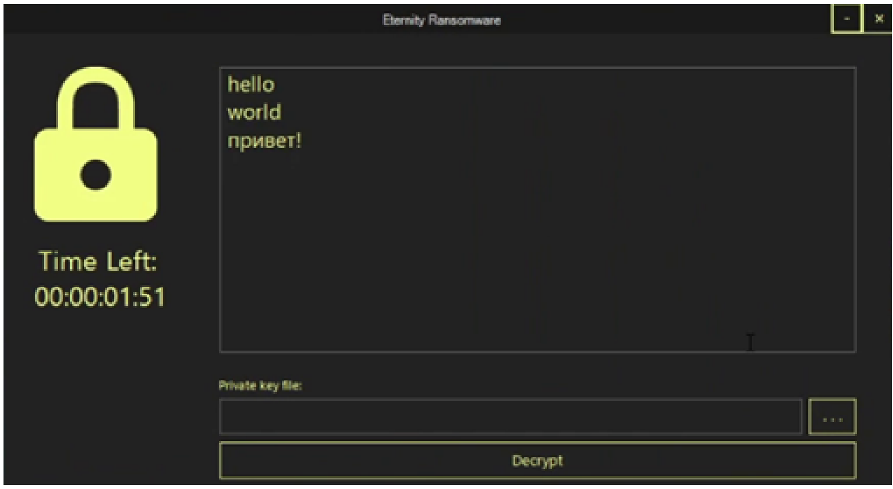
❌ No 9:44 PM

Please select output file extension 9:44 PM

Write a message...

Figure 8 – Ransomware Payload Building

Figure 9 shows the Eternity Ransomware Decryption window when users open an encrypted file.



Eternity Ransomware

hello
world
привет!

Time Left:
00:00:01:51

Private key file:

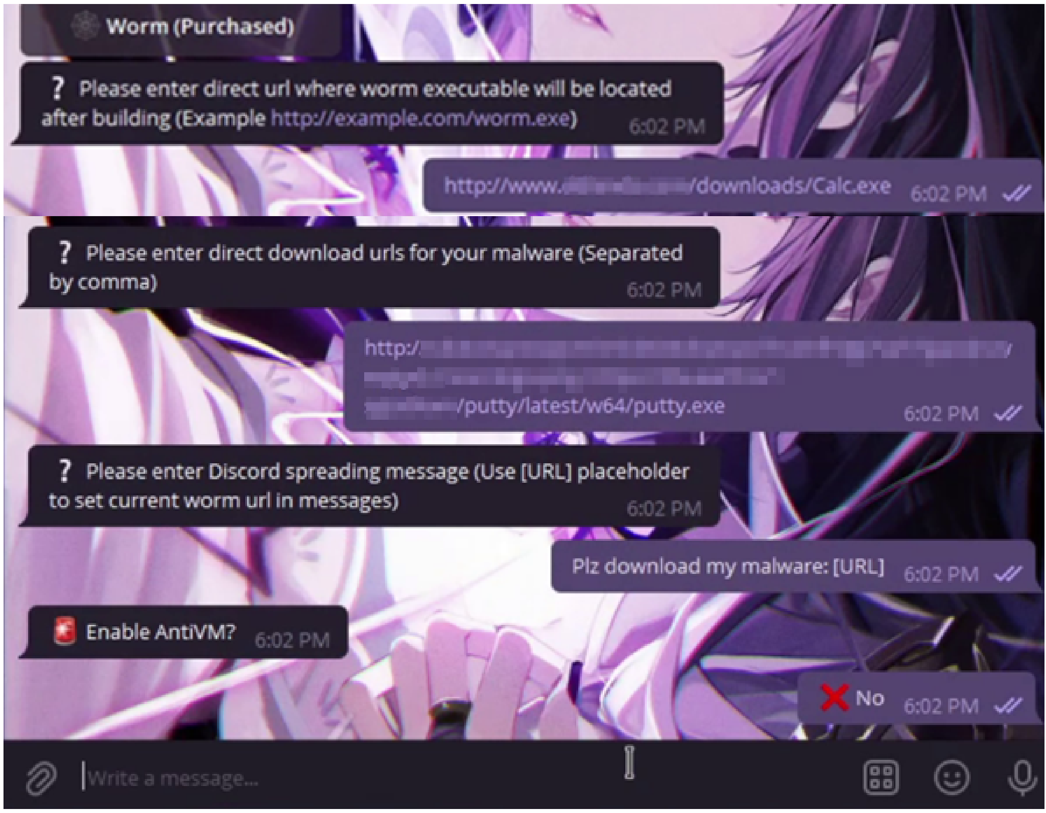
Figure 9 – Eternity Ransomware Decryption Window

Eternity Worm

The developer sells the Eternity Worm for $390. It is a virus that spreads through infected machines via files and networks. The features of the worm dropper malware mentioned on the TA’s website and Telegram channel are:

- USB Drives
- Local network shares
- 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)
- Telegram Spam (Sends your messages to all channels and contacts)

Figure 10 depicts the steps to build Eternity worm malware through the TAs Telegram channel. Here, users can provide the URL where the worm payload will be located and also provide direct download URLs to download the worm payload. Eternity Worm can infect local files and spread through Discord and Telegram channels.



Worm (Purchased)

? Please enter direct url where worm executable will be located after building (Example http://example.com/worm.exe) 6:02 PM

http://www.[redacted]/downloads/Calc.exe 6:02 PM

? Please enter direct download urls for your malware (Separated by comma) 6:02 PM

http:/[redacted]/putty/latest/w64/putty.exe 6:02 PM

? Please enter Discord spreading message (Use [URL] placeholder to set current worm url in messages) 6:02 PM

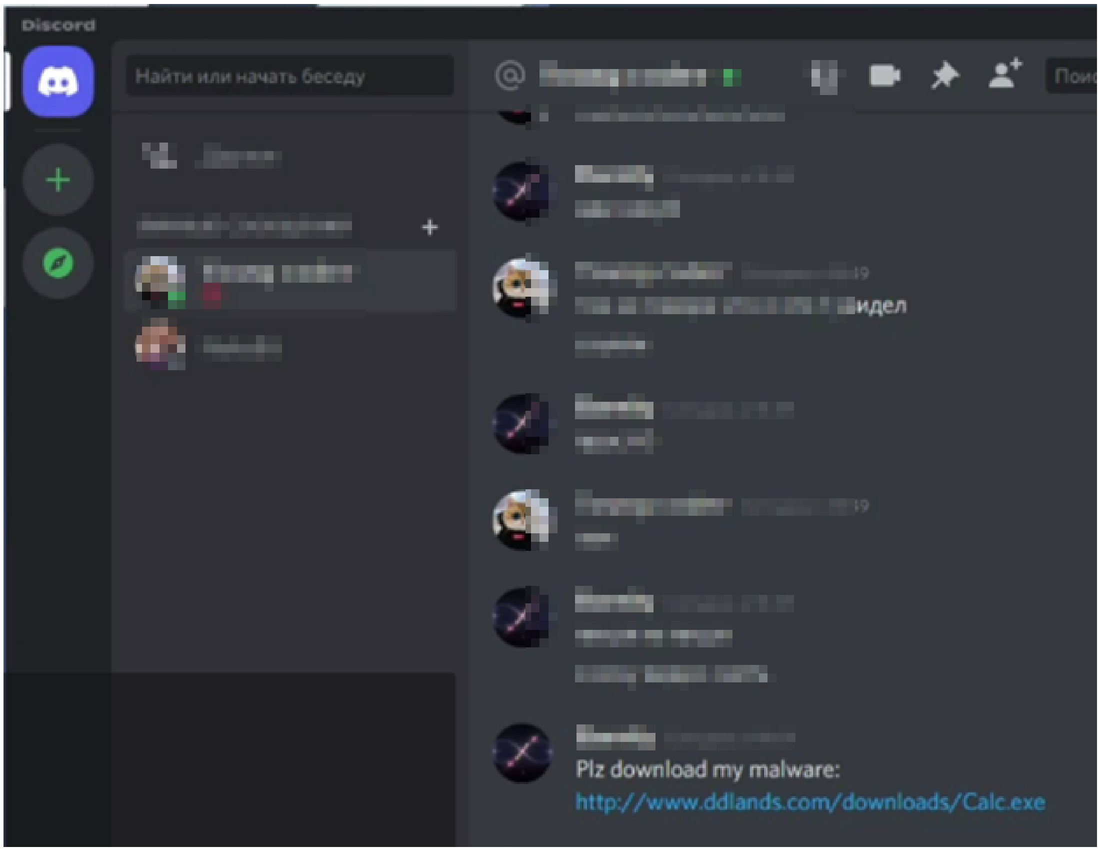
Plz download my malware: [URL] 6:02 PM

Enable AntiVM? 6:02 PM

❌ No 6:02 PM

Figure 10 – Worm Malware Building

The below image shows the malware spreading via Discord.



видел

Plz download my malware:
http://www.ddlands.com/downloads/Calc.exe

Figure 11 – Discord Account

Eternity DDoS Bot

According to the TA's website, the DDoS Bot malware is currently under development.

We suspect the developer behind the Eternity project is leveraging code from the existing Github repository and then modifying and selling it under a new name.

Our analysis also indicated that the Jester Stealer could also be rebranded from this particular Github project which indicates some links between the two Threat Actors.

Conclusion

Cyble Research Labs has observed a significant increase in cybercrime through Telegram channels and cybercrime forums where TAs sell their products without any regulation. We have encountered the Eternity products being sold on one such Telegram channel and TOR website.

Cyble will continue to monitor Eternity Project's products and update our readers with the latest information.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

Safety measures needed to prevent malware attacks

- Conduct regular backup practices and keep those backups offline or in a separate network.

- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.

Indicators Of Compromise (IOCs)

Indicators	Indicator type	Description
8d52a66459df0ea387d5aab3fc7a2bc9	MD5	Eternity Stealer Payload
1707b034483eb9f279dfaa3a8862592bddb2ac4e	SHA1	Eternity Stealer Payload
eb812b35acaeb8abcb1f895c24ddba8bb32f175308541d8db856f95d02ddcfe2	SHA256	Eternity Stealer Payload
c4b46a2d0898e9ba438366f878cd74bd	MD5	Eternity Clipper Payload
f95a0529fbb8aa61cd3dee602fa6555b2c86dd62	SHA1	Eternity Clipper Payload
025e74a98cb22aab0eb2dbff69cb5abd4f1d529925d9e456f92f5fd6ff1e11c3	SHA256	Eternity Clipper Payload
76c5b877fb931ed728df30c002bf8823	MD5	Eternity Ransomware Payload
16a8a21ef1a30849bedc514e42286de7676db5af	SHA1	Eternity Ransomware Payload
55bf0aa9c3d746b8e47635c2eae2acaf77b4e65f3e6cbd8c51f6b657cdca4c91	SHA256	Eternity Ransomware Payload
b35aa57c5c963bde7abee2a4e459b146	MD5	Eternity Worm Payload
e0817176fa7e1875a5d301b47d9a9a6977c39da5	SHA1	Eternity Worm Payload

656990efd54d237e25fdb07921db3958c520b0a4af05c9109fe9fe685b9290f7	SHA256	Eternity Worm Payload