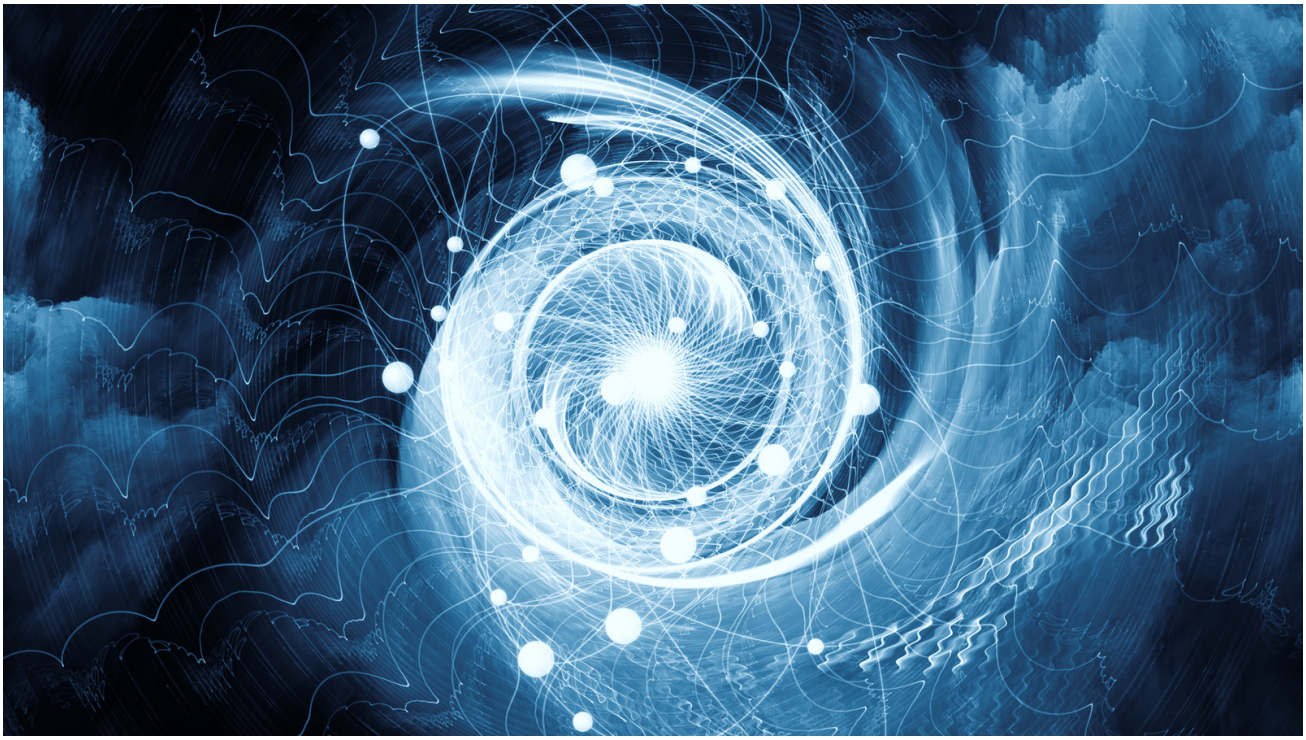
Eternity malware kit offers stealer, miner, worm, ransomware tools

bleepingcomputer.com/news/security/eternity-malware-kit-offers-stealer-miner-worm-ransomware-tools/

Bill Toulas

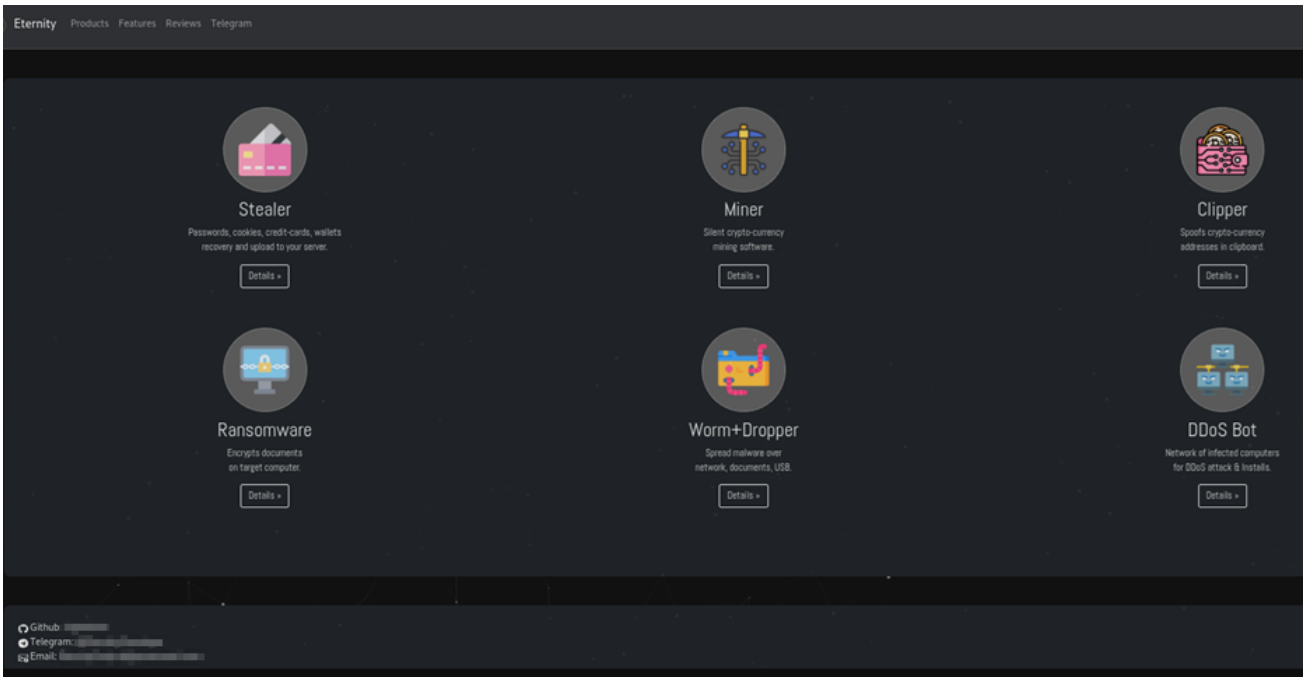
By
Bill Toulas

- May 12, 2022
- 03:18 PM
- 0



Threat actors have launched the 'Eternity Project,' a new malware-as-a-service where threat actors can purchase a malware toolkit that can be customized with different modules depending on the attack being conducted.

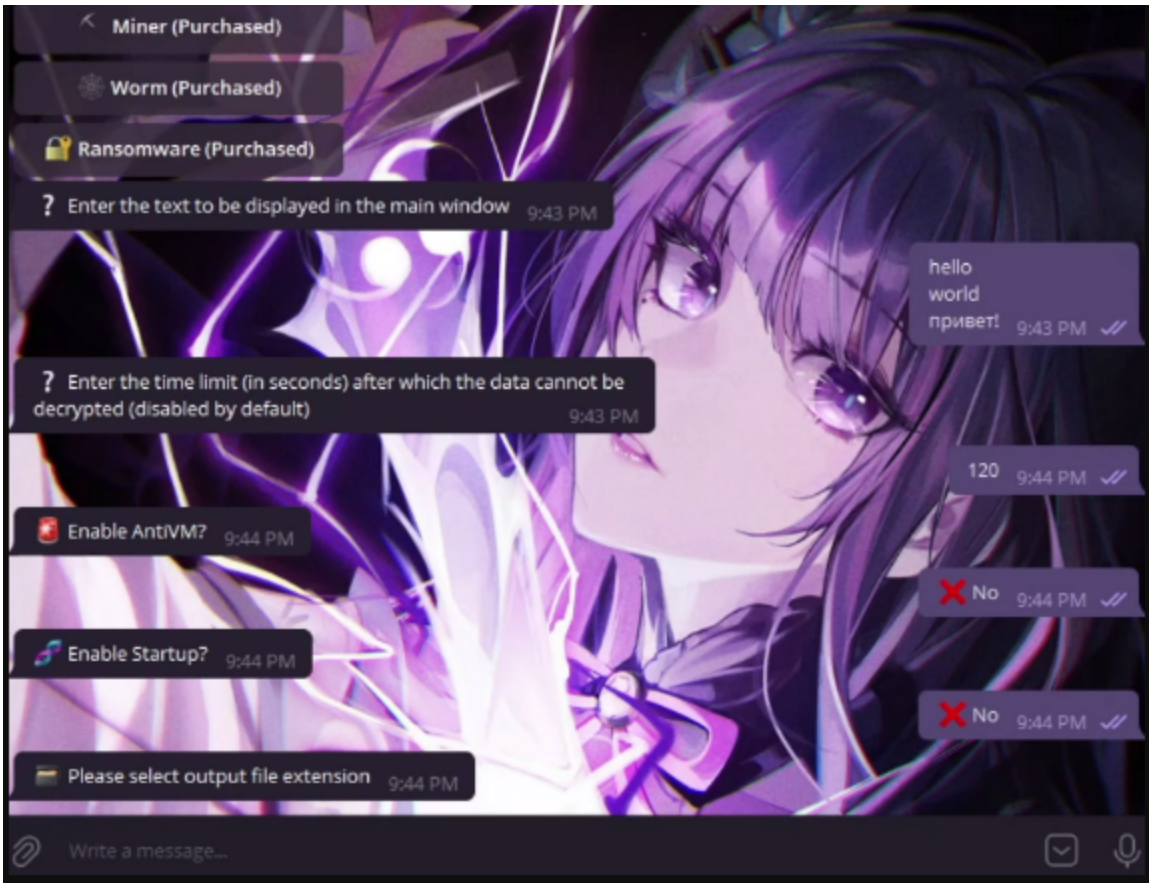
The malware toolkit is modular and can include an info-stealer, a coin miner, a clipper, a ransomware program, a worm spreader, and soon, also a DDoS (distributed denial of service) bot, each being purchase seperately.



The Eternity Project site *(Cyble)*

All of the above are promoted on a dedicated Telegram channel that counts over 500 members, where the authors post release notes for updates, usage instructions, and discuss feature suggestions.

Those who have bought the malware kit can utilize the Telegram Bot to build the binary automatically after selecting which features they want to activate and paying for them with crypto.



Purchasing malware modules for auto-build *(Cyble)*

Tools in detail

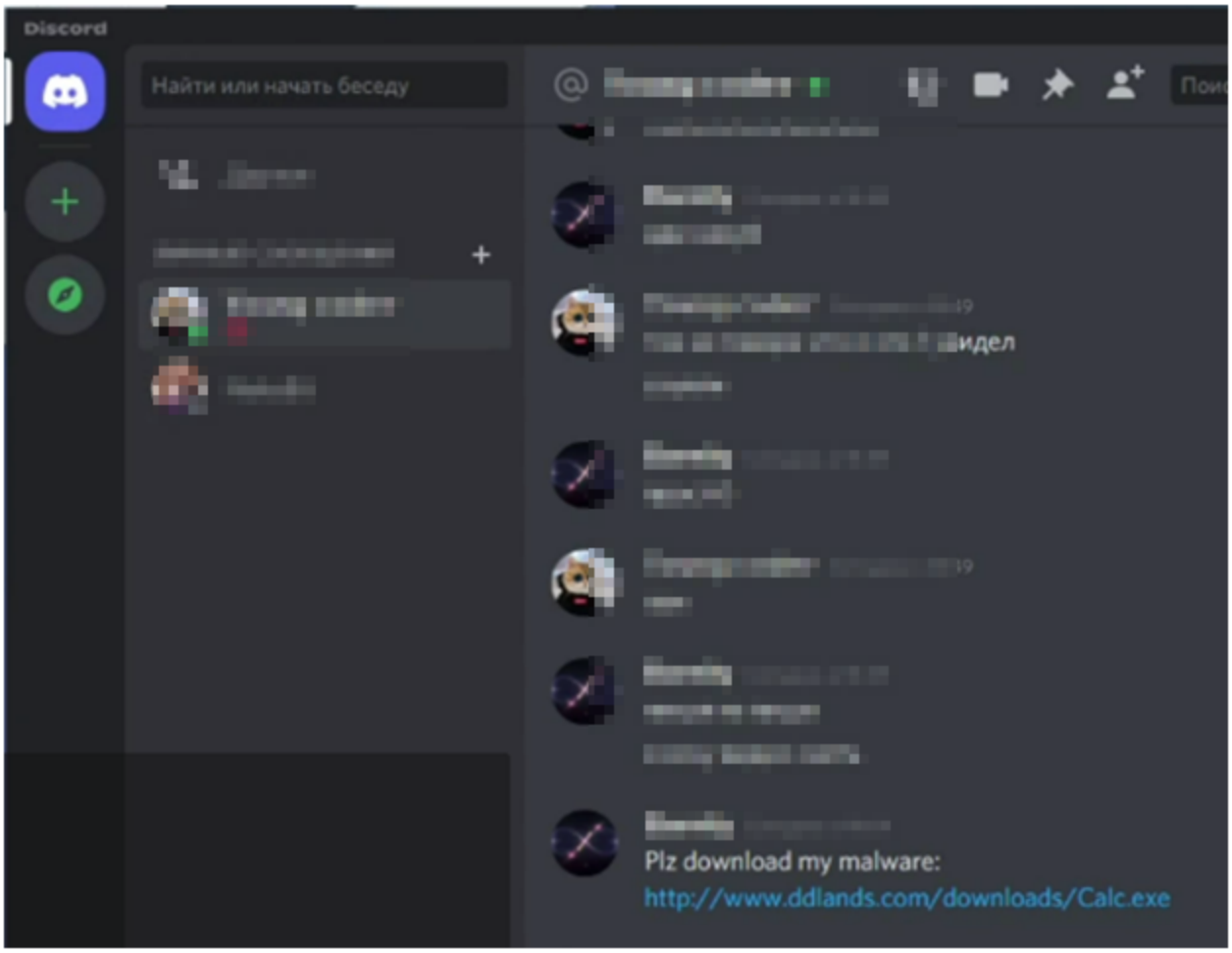
Starting with the info-stealer, which is sold for $260/year, this tool snatches passwords, credit cards, bookmarks, tokens, cookies, and autofill data stored in over twenty web browsers.

Additionally, it can steal information from cryptocurrency extensions or even cold wallets, and it also targets ten password managers, VPN clients, messengers, and gaming clients.

The miner module costs $90/year and features task manager hiding, auto-restart when killed, and startup launch persistence.

The clipper is sold for $110 and is a utility that monitors the clipboard for cryptocurrency wallet addresses to replace them with wallets under the operator's control.

The developer sells the Eternity Worm for a whopping $390, giving the malware the capability to spread on its own via USB drivers, local network shares, local files, cloud drives, Python projects (through the interpreter), Discord accounts, and Telegram accounts.

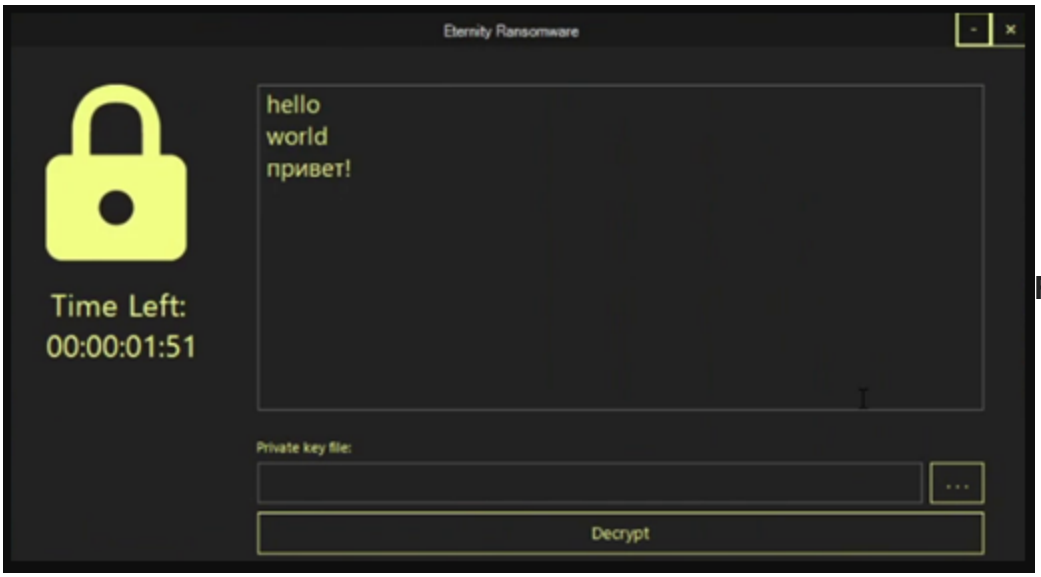


Example of the malware spreading via a Discord account *(Cyble)*

Finally, Eternity ransomware, the most expensive module, is $490. It supports offline encryption using a combination of AES and RSA and targets documents, photos, and databases.

The authors claim it's FUD (fully undetectable), a claim that is supposedly backed by Virus Total results where the strain returns zero detections.

Interestingly, the ransomware module offers an option to set a timer that renders the files completely unrecoverable when it expires. This puts additional pressure on the victim to pay the ransom quickly.



Ransomware timer threatening to corrupt files *(Cyble)*

Real or scam?

Analysts at Cyble who discovered the Eternity Project told Bleeping Computer that while they didn't have the chance to examine all of the modules yet, they have seen samples of the malware circulating and used in the wild, and all user comments on Telegram point to this being a real threat.

By looking into the stealer module, Cyble analysts found several similarities to the Jester Stealer, both probably derived from a GitHub project named DynamicStealer.

As such, the "Eternity Stealer" is most likely a copy of that code, followed by modifications and rebranding to sell it on Telegram for profit.

Even if this is "skidware", the additional modules, customer support, automated building, and detailed instructions on how to use the malware, make it a potent weapon in the hands of unskilled hackers and a severe threat to internet users.

Related Articles:

German automakers targeted in year-long malware campaign

New powerful Prynt Stealer malware sells for just $100 per month

Ukraine warns of “chemical attack” phishing pushing stealer malware

Pixiv, DeviantArt artists hit by NFT job offers pushing malware

Beware: Onyx ransomware destroys files instead of encrypting them

- Clipper

- Info Stealer
- Information Stealer
- Malware
- Ransomware

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: