Ransomware-as-a-Service Transforms Gangs Into Businesses

securityintelligence.com/news/eternity-gang-ransomware-as-a-service-telegram/

News November 9, 2022

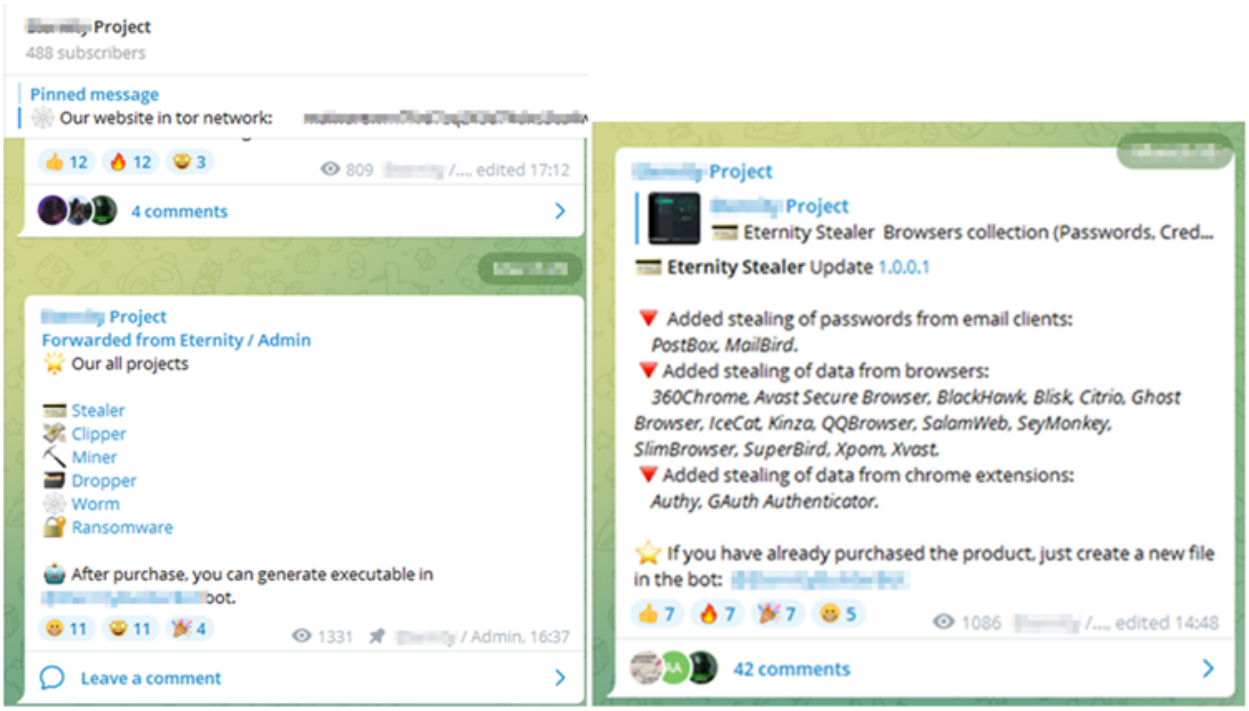
By Jonathan Reed 3 min read

Malware-as-a-Service is getting easier and easier to access, according to a recent threat report. Self-named the ‘Eternity Project’, this cyber threat group offers services from a Tor website and on their Telegram channel. They sell a wide variety of malware in an organized fashion, including stealer, clipper, worm, miner, ransomware and distributed-denial-of-service bot services.

This alarms many security professionals. With Eternity, even inexperienced cyber criminals can target victims with a customized threat offering. Eternity sells malware for $90 to $490. As Malware-as-a-Service grows in sophistication, it’s easier than ever to access attack tools at low prices.

Malware for Sale on Telegram

According to Cyble, Eternity Project offers a wide variety of malware services on its Telegram channel, which has around 500 subscribers. The channel provides detailed information about the service’s features and even uses explainer videos. Eternity Project’s Telegram channel also shares news about their malware’s updates, just like any brand showcasing new features.



Source: Cyble

Eternity Project Stealer

What kind of damage can Eternity Project’s malware do? One example is Eternity Stealer. This malware lets users steal passwords, cookies, credit cards and crypto wallets from targets to later receive the stolen data directly on the Telegram bot.

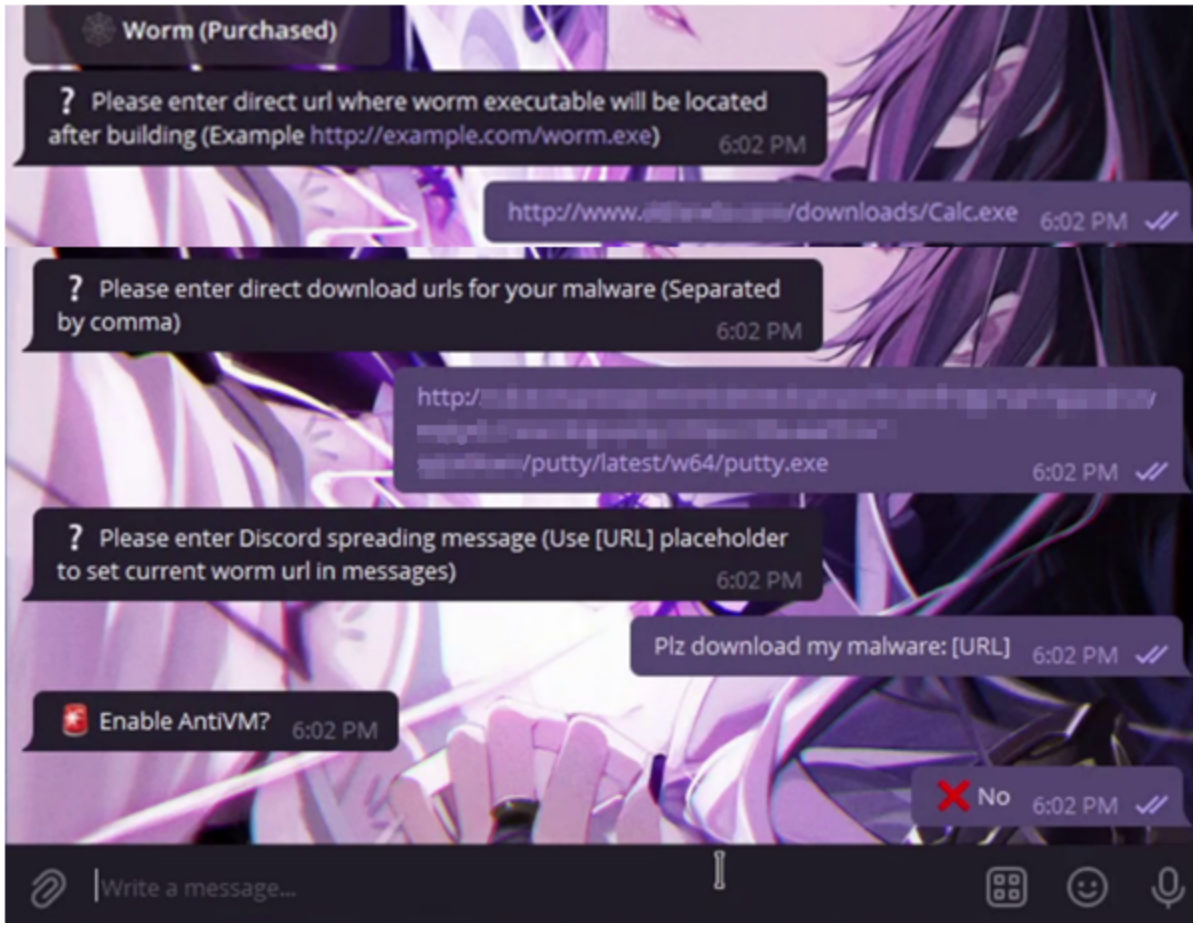
The features of the stealer malware mentioned on the group's Telegram channel include:

- Browsers collection (passwords, credit cards, cookies, autofill, tokens, history, bookmarks)
- Chrome, Firefox, Edge, Opera, Chromium, Vivaldi, IE and other browsers
- Email clients: Thunderbird, Outlook, FoxMail, PostBox and MailBird.

It also offers ways to break into messenger apps, password managers and more.

According to the report, customers can build Eternity Stealer malware directly on the Telegram bot. Once the user selects a stealer product, options appear to add features such as AntiVM and AntiRepeat. Next, the user selects the available payload file extension such as .exe, .scr, .com or pif. Finally, users can download the exfiltrated payload directly from the Telegram channel.

Other services such as miner, clipper, ransomware and worm offer the same kind of convenience and customization. And it all occurs through an easy-to-use Telegram Q&A bot:



Source: Cyble

Malware-as-a-Service Growth

The researchers state that they have seen a major increase in cyber crime through Telegram channels and forums. Threat groups are selling their products in the open without any type of sanction.

A large part of the success of these groups is their businesslike approach. They employ an agile development framework to develop malware. Later they go online to test their products on a victim, then they return to the lab to work out the bugs. They also implement advanced marketing techniques and place an emphasis on user experience and user interface.

Thwarting Malware Attacks

The authors of the threat report suggest some ways to mitigate malware. For example, it's important to keep backups of all critical files. These backups should be kept offline or on completely separate networks. Turn on automatic software updates, and have security teams scan often for warnings and updates about mission-critical software.

The official CISA Stop Ransomware site also provides in-depth guidance against malware.

Jonathan Reed
Freelance Technology Writer

Jonathan Reed is a freelance technology writer. For the last decade, he has written about a wide range of topics including cybersecurity, Industry 4.0, AI/ML...