A deep dive into Eternity Group: A new emerging Cyber Threat

yoroi.company/research/a-deep-dive-into-eternity-group-a-new-emerging-cyber-threat/

May 18, 2022

For months, we at Yoroi Malware ZLab have studied and tracked the evolution of a new emerging cyber-criminal group which has attracted the attention of everyone inside the cyber security threat landscape. This threat actor calls itself “Eternity Group”, previously “Jester Group”, which we internally tracked it as “TH-320”.

This threat has also recently been involved in a cyber-attack against Ukraine, this attack proves that any threat should not be underestimated and could be used and evolve to sabotage critical infrastructures benefiting state-sponsored groups. In the following flashcard we classified the TTPs to summarize the capabilities of this threat:

Jester Group (A.K.A Eternity Group) (TH-320)

Targets	WorldWide	Privates
Objectives	Developing new threats for profit-making	
Payload Delivery	Executables concealed as crack or legit programs to entice the execution	
TTPs	T1059 Command-Line Interface	T1054 Scripting
	T1090 Internal Proxy	T1036 Masquerading
	T1547 Boot or Logon Autostart Execution	T1083 File and Directory Discovery
	T1555 Credentials from Password Stores	T1022 Data Encrypted
	T1027 Obfuscated Files or Information	T1055 Process Injection
	T1036:002 Right-to-Left Ovveride	T1546:001 Event Triggered Execution

While we were monitoring the threat actor, we found the following malicious projects:

- Jester Stealer, later rebranded as Eternity Stealer, it is the first malicious product developed by the threat actor
- Merlynn Clipper, a constantly updated clipper
- Trinity Miner, a stealth miner
- Lilith Botnet, the “all in one” solution provided by the Eternity Group
- Eternity Worm, capable to propagate in different ways
- Eternity Ransomware, a simple but efficient ransomware

To see our deep investigation inside this group and its evolution, you can read our whitepaper:

Download Eternity Group Report