WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Eternity's LilithBot, Soon Available to Regular Internet Users?

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts and IoCs

Executive Report

Eternity, also known as the "EternityTeam" or "Eternity Project," has been active since January 2022 and tied to the Jester Group. It gained infamy for using the as-a-service subscription model to distribute its own brand of malware modules via underground forums. These modules typically include a stealer, a miner, a botnet, a ransomware, a worm-and-dropper combination, and a distributed denial-of-service (DDoS) bot.

ThreatLabz recently disclosed indicators of compromise (IoCs) for one of Eternity's offerings, LilithBot, comprising four IP addresses corresponding to the group's command-and-control (C&C) servers—77[.]73[.]133[.]12, 45[.]9[.]148[.]203, 91[.]243[.]59[.]210, and 195[.]2[.]71[.]214.

Eternity typically keeps its activities on the down low—in the Dark Web. Still, we sought to determine if LilithBot and Eternity also engaged in dealings on the Surface Web. We did that by looking for potential signs of their presence in the DNS and found:

- 127 domains that shared the IoCs' IP hosts, 13% of which are dubbed "malicious" by various malware engines
- 40 additional domains containing the strings "eternity + malware," "eternity + channel," "eternity + team," "eternity + project," and "lilithbot"

Eternity Facts

Throughout Eternity's operation, it has become a well-known malware-as-a-service (MaaS) provider communicating with buyers notably via Telegram. Its offerings range between US$70–90 that customers need to pay for via a cryptocurrency of their choice—Bitcoin, Ethereum, Monero, or Dash.

Are Eternity's Dealings Limited to the Dark Web?

In an effort to determine if the threat that Eternity and LilithBot pose is limited to the Dark Web, we conducted an IoC expansion investigation using various WHOIS, IP, DNS, and OSINT sources.

Using the IP addresses identified as IoCs as reverse IP lookup search terms allowed us to uncover 127 domains that shared them as hosts. A bulk malware lookup for these showed that 17 have been dubbed "malware hosts" by various malware engines. These malicious domains include:

- coregonid[.]xyz
- decostate[.]xyz
- epicenism[.]xyz
- perilless[.]xyz
- reconceal[.]xyz
- spadebone[.]xyz

Apart from using the same top-level domain (TLD) extension—.xyz, a bulk WHOIS lookup for the malicious domains showed similarities in current registrar (i.e., NameSilo, LLC). Their historical WHOIS records, meanwhile, also yielded interesting breadcrumbs as 15 of them were around the same age (i.e., 412–416 days old). Only two were several years old—epicenism[.]xyz (i.e., 2,316 days old) and theftbote[.]xyz (i.e., 1,170 days old).

In an effort to find other possibly connected artifacts, we used the strings "eternity + malware," "eternity + channel," "eternity + team," "eternity + project," and "lilithbot" as Domains & Subdomains Discovery search terms. That led to the discovery of 40 domains. None of them are currently classified as malicious, but could arguably be of interest to the threat actor or copycats as they feature the publicly known strings the threat actor group uses. Some were also live, and one—eternityprojectblog[.]com—is currently undergoing development. We didn't see definitive signs of its connection to the threat.

Screenshot of eternityprojectblog[.]com

—

Our IoC expansion of LilithBot using WHOIS, IP, and DNS investigation techniques helped identify malicious cyber resources that we wouldn't have found otherwise. In LilithBot's case, the security community may wish to keep a closer watch on .xyz domains, particularly those that share other similarities with the IoCs, and pages sporting known strings associated with the threat actors.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to [contact us](#).

Appendix: Sample Artifacts and IoCs

Sample Domains That Shared the IoCs' IP Hosts

- ablactate[.]xyz
- aisleless[.]xyz
- amendable[.]xyz
- amynodont[.]xyz
- angleworm[.]xyz
- arachnism[.]xyz
- arrowless[.]xyz
- ascaridia[.]xyz

- atikokania[.]xyz
- attestable[.]xyz
- autoheader[.]xyz
- baccaceous[.]xyz
- balsamize[.]xyz
- bicrenate[.]xyz
- bleachyard[.]xyz
- bluethroat[.]xyz
- blunthead[.]xyz
- capitoline[.]xyz
- ceramidium[.]xyz
- chirurgery[.]xyz
- collophore[.]xyz
- collotype[.]xyz
- confrontal[.]xyz
- coregonid[.]xyz
- coseismic[.]xyz
- crambinae[.]xyz
- crenothrix[.]xyz
- cryostase[.]xyz
- cynomorium[.]xyz
- cypripedia[.]xyz
- daphnaceae[.]xyz
- decostate[.]xyz
- dentelated[.]xyz
- depigment[.]xyz
- diachronic[.]xyz
- dihalogen[.]xyz
- dithalous[.]xyz
- epicenism[.]xyz
- epidendron[.]xyz
- externate[.]xyz
- farrantly[.]xyz
- firespout[.]xyz
- forbidding[.]xyz
- gardenize[.]xyz
- halogenous[.]xyz
- hippodamia[.]xyz
- holohedric[.]xyz
- homiletics[.]xyz
- immunogen[.]xyz
- inculture[.]xyz

Sample Domains That Contained “eternity + malware,” “eternity + channel,” “eternity + team,” “eternity + project,” and “lilithbot”

- eternitychannel[.]tk
- eternitychannel[.]com
- eternityproject[.]pl
- eternityproject[.]eu
- eternityproject[.]ru
- eternityproject[.]fi
- eternityproject[.]cf
- eternityproject[.]org
- eternityproject[.]com
- eternityproject[.]net
- eternityprojects[.]com
- eternityproject[.]shop
- eternityprojector[.]com
- theternityproject[.]com
- eternityprojectuk[.]org
- eternityproject[.]co[.]id
- theeternityproject[.]com
- theeternityproject[.]org
- eternityproject[.]org[.]uk
- eternityprojects[.]com[.]au