The Underground Ransomware Group (AKA Underground Team)

Date: 06th May 2024 | Severity: High

Summary

The ransomware group targets organizations with high revenue within several countries. Underground Team created a ransom-demanding message titled “!!readme!!!.txt”. Underground distributes its ransomware using phishing attacks.

Attack Vectors

- Underground distributes its ransomware using phishing attacks. The ransomware does not change the file names or extensions of the encrypted data, and thus, the victim is only aware of the infection once the data is inaccessible. To prevent easy system recovery, the ransomware deletes volume shadow copies.
- Underground always presents its victims with a ransom note (!!readme!!!.txt) containing the type of compromised data and where it was exfiltrated. The note also contains a high ransom demand that fluctuates depending on the revenue of the victim organization and a three-day deadline to pay before the stolen data is uploaded to Underground’s ransomware blog.
- The Underground operators are unique due to their claimed cybersecurity expertise and ability to detect and solve system vulnerabilities where they request payment for their services.
- Ransomware and other malware are mainly spread using phishing and social engineering techniques. The most widely used distribution methods include: drive-by (stealthy/deceptive) downloads, malicious attachments and links in spam mail (e.g., emails, DMs/PMs, SMSes, etc.), online scams, untrustworthy download sources (e.g., freeware and third-party sites, P2P sharing networks, etc.), illegal software activation tools (“cracks”), fake updates, and malvertising.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Hashes	• d4a847fa9c4c7130a852a2e197b205493170a8b44426d9ec481fc4b285a92666
URL	• http://47glxkuxyayqrvugfumgsblrdagvrah7gttfscgzn56eyss5wg3uvmqd.onion/

Recommendation

- In the event of a ransomware attack, users must disconnect infected devices from the network, detach external storage devices if connected, and inspect system logs for any suspicious events, advised CRIL researchers.
- Software must be activated and updated using legitimate functions/tools, as those obtained from third-parties can contain malware.
- We advise being careful while browsing since fake and dangerous online content usually appears ordinary and harmless. Another recommendation is to approach incoming emails and other messages with caution. Attachments or links present in suspicious mail must not be opened, as they can be malicious and cause infections.
- Update and run antivirus software.
- Cyber security awareness training.
- Furthermore, organizations should consider implementing security products that can detect and block phishing attempts, as well as regularly update their security protocols to stay ahead of evolving threats.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.pcrisk.com/removal-guides/27197-underground-team-ransomware
- https://thecyberexpress.com/newbie-group-underground-team-ransomware-group/#google_vignette