DarkGate Malware

Date: 9th June 2024 | Severity: Medium

Summary

- DarkGate loader malware has been around since 2018, typically spreading through phishing emails with malicious attachments or links. The malware itself is quite versatile, capable of stealing credentials, granting remote access to attackers, and even mining cryptocurrency on infected machines.
- DarkGate malware is malicious software designed to infiltrate computer systems and compromise security.
- This strain of malware is potent and adaptable, capable of infiltrating IT systems, evading detection, and executing various cyberattacks. This malware’s name combines “Dark” and “Gate,” representing its secretive nature and the gateway it provides for cybercriminals to exploit.
- It is a Remote Access Trojan (RAT) with infostealer functionality that can give attackers control over compromised systems and extract valuable information.

Attack Vectors

- DarkGate often spreads through phishing emails or malicious attachments, tricking users into downloading and executing the malware.
- DarkGate can exploit unpatched software vulnerabilities to infiltrate systems.
- Once installed on a victim’s system, DarkGate establishes a connection with a C&C server. This connection enables cybercriminals to control and manage the infected devices remotely.
- DarkGate can lead to the theft of valuable information, including personal data, financial records, and intellectual property. This information can be exploited for financial benefit or traded on the dark web.
- DarkGate allows cybercriminals to engage in various illegal activities, such as financial fraud, ransomware attacks, and theft of banking and payment information. These actions can result in substantial financial losses for both individuals and organizations.
- DarkGate attacks can lead to legal repercussions, such as criminal charges and fines, as they violate laws related to cybercrimes and data breaches.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 27502d6406f4c1a723c7f428c48aa35dc5db6bd5edd764e0ba4ae14974ee46fc • b3e2c0afbcfb5c7f74ff16a31a8a11a7243c006a3992d3b5cc55ad385f48ab7c • 46fcdbd2e2e09755d860dd1475713cb608f2345d666e56b69ad6df1f8beaa44a • 651bff979d68c0aa9513c2255aa822016ff1b61b • 752270a00b24ab06d91d07c0979e3d2f28c52d66 • 514fbef6e9d1cbd83bcb5c65f24b4527eaf5fa08 • 9f79d2bd5f0425f658a7ec5a3dd07fe4 • c3813a1159ca69225917ecfba2076084 • 68aab1e12df1249f6c38f02ea9529cfbw
URLS	• http://www[.]rockcreekdds[.]com/1[.]txt

Recommendation

- Block all threat indicators at your respective controls.
- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Never trust or open links and attachments received from unknown sources/senders.
- Implement multi-factor authentication to add an extra layer of security to login processes.
- Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway.

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[.]rewterz[.]com/threat-advisory/darkgate-malware-active-iocs-5
- https://www[.]infosectrain[.]com/blog/what-is-darkgate-malware-and-its-impact/