Malware: Agent Tesla and DarkGate

C-Suite level threat review by applicable business area addressing active threats.

Malware-as-a-service (MaaS), a prevalent part of the threat landscape, is where adversaries provide use of their malware for a fee. This model lowers the barrier of entry for cybercriminals by providing ready-made, easily deployable malware. Since the use of MaaS is widespread among threat actors, understanding the capabilities of key ones like Agent Tesla and DarkGate will help organizations better defend against current cybersecurity threats.

Agent Tesla:

Agent Tesla, created in 2014, is a popular MaaS due to its reliability, routine upkeep and extensive functionality. It enables remote access to its victims' environments and facilitates data exfiltration. This malware has been used in campaigns targeting many different industries over the years including finance, retail, healthcare and travel. Most recently, Agent Tesla malware was used in a campaign targeting private organizations and government agencies in the United States and Australia.

DarkGate:

DarkGate malware, first reported in 2018, is utilized by groups such as Black Basta, RastaFarEye, and TA577. It is capable of malicious activities including keylogging, browser data theft, and crypto mining. The malware's sixth version, released in March 2024, features advanced evasion techniques. DarkGate has been observed targeting various industries such as healthcare, technology, telecommunications, and fintech, across the United States, Europe, and Asia.

Agent Tesla

Threat Level: High

Attack:

Email phishing campaigns are a common method malicious actors use to deploy Agent Tesla malware to its victims' environments (MITRE T1566). Agent Tesla is a remote access trojan (RAT), meaning it is designed to enable remote control over its victims' environments. It is equipped with evasive maneuvers such as the capability to discern if it is running in a debugger environment before execution (MITRE T1622). Once installed, it starts to gather information about its victims' environments such as the computer's hardware and operating system, as well as key strokes and saved credentials (MITRE T1016, T1082, T1087.001, T1555 and T1056.001). All this information can then be utilized by the attacker to advance its attack. Agent Tesla can also be coupled with other types of malwares such as ransomware.

Remediation:

- Conduct periodic phishing simulations to ensure users are trained to identify a malicious phishing email.
- Acquire an anti-phishing tool to identify and block phishing emails.
- Maintain a comprehensive patching program to ensure operating systems and applications are regularly updated.

DarkGate

Threat Level: High

Attack:

DarkGate malware, a remote access trojan, is commonly spread through phishing emails and Microsoft Teams messages (MITRE T1566). It is also circulated via malvertising (i.e., malicious advertising) and Search Engine Optimization Poisoning, which is when attackers manipulate search engine algorithms to promote malicious webpages (MITRE T1583.008 and T1608.006). Once installed, DarkGate can exfiltrate sensitive data, including login information from browsers (MITRE T1555.003). DarkGate malware may also be a prelude to a more elaborate attack as it can download and execute additional malware. DarkGate employs advanced defense evasion techniques, such as process hollowing and the use of the scripting language AutoHotKey (MITRE T1055.012 and T1059.010). Process hollowing is a form of code injection; legitimate code is replaced with malicious code. AutoHotKey can be used to mimic real user activity; it can automate tasks and replicate keystrokes. The architects of DarkGate malware continue to evolve the malware's capabilities, advancing its defense evasion and data exfiltration techniques.

Remediation:

- Implement an Endpoint Detection and Response (EDR) platform to detect and block malware.
- Implement multifactor authentication to mitigate an attacker from accessing an account even after capturing the account credentials.
- All users should be trained to recognize social engineering attacks.

Agent Tesla:

- **Overview of capabilities:** https://cyware.com/resources/research-and-analysis/behind-the-code-deciphering-the-evolution-of-agent-tesla-malware-24d5
- **Recent malicious campaign utilizing Agent Tesla:** https://blog.checkpoint.com/research/agent-tesla-targeting-united-states-australia-revealing-the-attackers-identities/

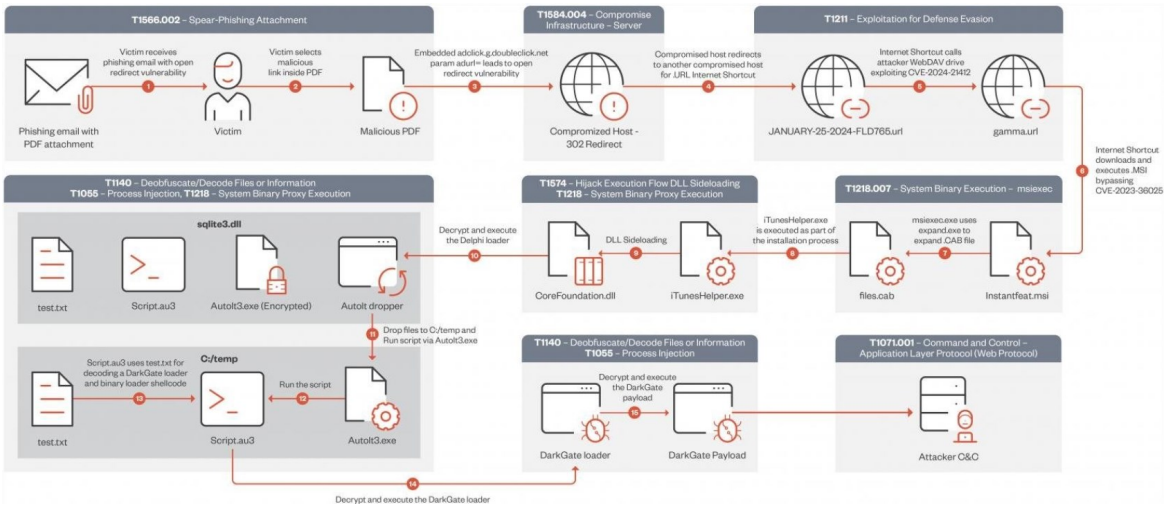
DarkGate

- **DarkGate infection chain:** https://www.logpoint.com/en/blog/inside-darkgate/
- **Overview of DarkGate malware, including its history and current capabilities:** https://socradar.io/darkgate-malware-exploring-threats-and-countermeasures/

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Response (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SaaS)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
- Threat Intelligence
  - Notification to customers of threats
  - On-demand briefings
  - Threat exposure workshops
  - User awareness training seminars
  - Monthly and quarterly threat intelligence reports

Attack Chain Utilizing DarkGate Malware



Source: https://www.bleepingcomputer.com/news/security/hackers-exploit-windows-smartscreen-flaw-to-drop-darkgate-malware/