SECURITY ADVISORY

CYBER STASH

October, 2024

Latrodectus Malware: The Black Widow Threat

Context

Latrodectus, a newly identified and highly sophisticated malware, is rapidly capturing the attention of the cybersecurity community. Drawing its name from the notorious black widow spider, this malware employs stealthy and perilous tactics to infiltrate targeted systems. Latrodectus is associated with data exfiltration, credential theft, and ransomware attacks, with a pronounced focus on critical infrastructure sectors such as healthcare, financial institutions, and government agencies, underscoring an urgent need for heightened vigilance.

The methods employed by Latrodectus include advanced phishing campaigns, specifically aimed at high-ranking executives and system administrators. Its remarkable ability to evade detection enables it to siphon off sensitive data while delivering secondary payloads that amplify its destructive potential. The malware's evolving characteristics present significant challenges to conventional security measures.

The cybercriminal entities orchestrating Latrodectus are believed to operate on a global scale, driven by motives of financial gain and corporate espionage. Given its adaptable and persistent nature, Latrodectus is poised to remain a formidable threat to organizations managing sensitive information, necessitating ongoing and enhanced defensive strategies.

Mitigation

Defending against the Latrodectus malware requires a proactive and layered security approach to minimize the risk of data breaches and system compromise.

Restrict Unauthorized Software Installation: Limit user permissions to prevent the installation of unapproved applications, enhancing security against potential threats.

Block Access to High-Risk Infrastructure: Proactively restrict access to known high-risk IP addresses, ASNs, and TLDs to mitigate exposure to malicious activities.

Deploy Endpoint Detection and Response (EDR) Solutions: Implement EDR tools to provide real-time monitoring, threat detection, and automated response capabilities, enhancing overall incident response.

Technical Details

Latrodectus Malware Delivery

Latrodectus malware is typically delivered through sophisticated phishing campaigns that exploit social engineering techniques. These emails often contain HTML or PDF attachments that trick users into believing they are from trusted services like DocuSign. The attachments lead victims to malicious URLs, which initiate a series of redirects through compromised domains, culminating in the download of an obfuscated JavaScript file.

Attack Chain Unique Techniques

Initial Phishing Entry: The attack begins with phishing emails containing heavily obfuscated JavaScript files. These files redirect users through multiple URLs, employing URL shorteners and legitimate cloud services to obscure the final payload.

Payload Delivery: Once the obfuscation is bypassed, the JavaScript triggers the download of an MSI file that houses a 64-bit DLL. This DLL is executed through the legitimate rundll32.exe process, allowing the malware to operate stealthily and evade immediate detection.

C2 Communication: After establishing itself, the malware connects to a command and control (C2) server via encrypted channels and unusual ports. This communication allows attackers to remotely control the infected system, download additional malicious payloads, or exfiltrate sensitive data.

Obfuscation Techniques: Throughout the process, advanced obfuscation and junk code insertion are employed to complicate detection and analysis by traditional antivirus solutions.

Persistence Mechanisms: The malware ensures long-term control by modifying the Windows registry and creating scheduled tasks, enabling execution upon system reboot or at designated intervals.

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to Latrodectus :

Tactic	Technique Number	Technique	Description
Initial Access	(T1566)	Phishing: Spear Phishing	Distributed through phishing emails with malicious attachments or links to fake websites that can download malware.
Execution	(T1059)	Command and Scripting Interpreter: JavaScript	JavaScript file executes to install main malware components, often heavily obfuscated to evade detection.
Persistence	(T1053)	Scheduled Task/Job: Scheduled Task	Creates scheduled tasks to ensure persistence across system reboots or user logins.
Privilege Escalation	(T1068)	Exploitation for Privilege Escalation	Exploits vulnerabilities to gain elevated privileges on the compromised system.
Defense Evasion	(T1036)	Masquerading	Disguises itself as legitimate processes or files to evade detection by security tools.
Credential Access	(T1003)	Credential Dumping: LSASS Memory	Extracts credentials from the Local Security Authority Subsystem Service (LSASS) memory after installation.
Discovery	(T1083)	File and Directory Discovery	Performs reconnaissance to identify sensitive files and directories on the infected system.
Lateral Movement	(T1021)	Remote Services: Remote Desktop Protocol	Uses remote access capabilities to move laterally across the network after establishing a backdoor.
Command and Control	(T1071)	Application Layer Protocol: Web Protocols	Employs web-based protocols for command-and-control communication, potentially using encryption to obfuscate traffic.
Exfiltration	(T1041)	Exfiltration Over Command-and-Control Channel	Exfiltrates data and additional payloads through the same channel used for C2 communications.
Impact	(T1499)	Endpoint Denial of Service	Engages in activities that degrade the performance or availability of the infected system.

Cyber Threat Intelligence

Latrodectus, or "BlackWidow," was identified by Walmart researchers in October 2023 during an IcedID investigation. Developed by the LUNAR SPIDER group, it serves as a successor to IcedID and is used by threat actors TA577 and TA578. Acting as a loader, it downloads additional malware, including credential-stealing tools like Lumma Stealer and remote access agents like Brute Ratel C4 (BRC4).

Detected via phishing, malvertising, and SEO poisoning, Latrodectus often masquerades as legitimate DLLs. It spreads through JavaScript, BAT files, and ISO files, disguised as fake business communications. After a hiatus during "Operation Endgame," it re-emerged in June 2024, using a fake IRS website to distribute payloads.

References

IOCs:

- https://threatfox.abuse.ch/browse/malware/win.unidentified_111/

Initial Stage URLs

- hxxps://delview[.]com/MobileDefault[.]aspx?reff=hxxps://cutt[.]ly/seU8MT6t#_fZ0NmW
- hxxps://cutt[.]ly/seU8MT6t#_fZ0NmW
- hxxps://digitalpinnaclepub[.]com/?3
- hxxps://storage[.]googleapis[.]com/braided-turbine-435813-n7[.]appspot[.]com/VA8PBxartt/Document-20-17-57.js
- hxxp://194[.]54[.]156[.]91/dsa.msi
- hxxp://gertioma[.]top/o.jpg

Public Intelligence:

- https://www.logpoint.com/en/blog/latrodectus-the-wrath-of-black-widow/
- https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/analyzing-latrodectus-the-new-face-of-malware-loaders/
- https://thehackernews.com/2024/10/bumblebee-and-latrodectus-malware.html
- https://www.securityweek.com/latrodectus-malware-increasingly-used-by-cybercriminals/
- https://www.forcepoint.com/blog/x-labs/inside-latrodectus-malware-phishing-campaign