SECURITY ADVISORY

CYBER STASH

February, 2024

Stealthy Deployment of Remcos RAT

Context

The advent of a fresh variant of the IDAT loader, frequently utilized by cybercriminals for malware dissemination, presents a formidable obstacle for both standard and advanced defense mechanisms. This latest iteration harnesses steganography, a technique for camouflaging data within apparently benign files, to clandestinely deploy the Remcos Remote Access Trojan (RAT). Steganography amplifies the stealth attributes of the payload, rendering it notably arduous for conventional security measures to identify.

The Remcos RAT facilitates various malicious activities, including remote monitoring and data exfiltration. IDAT utilizes sophisticated evasion techniques, such as dynamic loading of Windows API functions and obfuscation of API calls, to avoid detection. Upon execution, IDAT extracts the hidden payload from a PNG image file, decrypts it, and executes it in memory, injecting additional modules into legitimate processes. The final stage involves decrypting and executing the Remcos RAT, enabling covert data theft and surveillance.

Mitigation strategies include deploying robust security controls to reduce exposure and educating users about the risks of opening files from untrusted sources.

Mitigation

Defending against the Remcos RAT necessitates more than just patching vulnerabilities. It involves actively blocking emerging threat infrastructures, memory analysis, while also enhancing user awareness.

Forensic-Depth Memory Analysis: Incorporate regular memory-based forensic analysis across all systems into your threat hunting strategy to unveil malicious fileless executables

Blocking Network Traffic: Implement proactive network traffic blocking measures, including the restriction of suspicious IPs, domains, and connections from high-risk Autonomous System Numbers, Top-Level Domains, and countries.

User Security Awareness Training: Provide user awareness training to educate employees on the risks of opening files or images from unknown sources. Enforce policies restricting interaction with untrusted content and consider implementing email filtering systems to detect

Technical Details

The sophisticated evolution of the IDAT loader showcases an intricate blend of cutting-edge techniques designed to evade detection and unleash potent cyber threats. Utilizing steganography, this latest iteration conceals the Remcos RAT payload within innocuous files or images, laying the groundwork for a stealthy infiltration of victim systems.

Upon execution, the loader adeptly extracts and executes the concealed payload, granting attackers unfettered access and control, thereby unleashing a cascade of malicious activities including remote surveillance, data exfiltration, and the execution of arbitrary commands facilitated by the Remcos RAT.

IDAT's arsenal is fortified with advanced evasion tactics, including the dynamic loading of Windows API functions, meticulous HTTP connectivity tests, strategic process blocklisting, and intelligent syscall manipulation, all orchestrated to circumvent traditional detection mechanisms. Further obscuring its tracks, API calls are shrouded within the code and dynamically resolved at runtime using encrypted keys interwoven within the attack chain, ensuring the operation remains covert and undetected.

Upon execution, IDAT orchestrates a meticulously choreographed sequence: extracting the encoded payload nestled within a seemingly benign PNG image file, seamlessly decrypting it, and orchestrating its execution within the memory space. This intricate process, unfolding across multiple stages, culminates in the injection of additional modules into unsuspecting legitimate processes such as Explorer.exe and DLL files like PLA.dll, further camouflaging its nefarious activities amidst the legitimate system operations.

The climax of this sophisticated assault unveils the decryption and activation of the Remcos RAT, an insidious backdoor malware heralding covert data theft and pervasive victim surveillance. Notably, IDAT's threat landscape extends beyond the Remcos RAT, as it serves as a conduit for disseminating other potent malware strains like Danabot, SystemBC, and RedLine Stealer. However, the exact extent of their involvement remains shrouded in uncertainty, with Morphisec indicating their presence in separate attacks or potentially intertwined within the fabric of the specific incident in Finland.

Tactics, Techniques and Procedures

The notable TTPs related to the IDAT's delivery of Remcos RAT are:

T1027.003 - Steganography: The adversary employs steganography techniques to conceal malicious payloads within legitimate files or images, evading detection by traditional security measures. In this context, steganography is used to hide the Remcos RAT within a PNG image, facilitating its delivery via the IDAT loader.

T1073 - DLL Side-Loading: In this scenario, the adversary leverages the IDAT loader to facilitate the execution of additional malicious DLL files by exploiting vulnerable legitimate processes such as Explorer.exe. By side-loading malicious DLLs into trusted applications, the adversary evades detection mechanisms and gains persistence on the compromised system. This tactic aligns with the broader objective of establishing a foothold and executing unauthorized code within the target environment, illustrating the adversary's intent to maintain access for further exploitation.

T1055.012: Process Hollowing: This technique involves creating a new process in a suspended state and then replacing its memory with the malicious code. IDAT may use this technique during the injection of additional modules into legitimate processes.

Cyber Threat Intelligence

In a recent discovery, the hacking collective identified as 'UAC-0184' has been observed employing sophisticated techniques to infiltrate the systems of a Ukrainian entity operating in Finland. Their modus operandi involves the use of steganographic image files as a delivery mechanism for the notorious Remcos RAT.

This latest activity, detected by analysts at Morphisec in early January 2024, underscores a concerning escalation in the group's operations. It highlights their capability to expand their target landscape beyond Ukraine, targeting organizations affiliated with their strategic objectives. This development underscores the evolving threat landscape and the need for heightened vigilance and robust cybersecurity measures to thwart such malicious activities.

References

Related IOC's & Yara Rules:

- https://otx.alienvault.com/pulse/643f7c31ec6660e495778454
- https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/

Public Intelligence:

- https://www.bleepingcomputer.com/news/security/new-idat-loader-version-uses-steganography-to-push-remcos-rat/
- https://thehackernews.com/2024/02/new-idat-loader-attacks-using.html
- https://www.cybersecurity-help.cz/blog/3826.html

Act now to protect your business!

Contact CyberStash today to learn about eclipse.xdr and our round-the-clock managed detection and response service.