SECURITY ADVISORY

CYBER STASH

September, 2023

Deadglyph Malware

Context

In a recent cyber espionage event aimed at Middle Eastern government entities, a newly surfaced, highly advanced backdoor malware named 'Deadglyph' emerged, marking a significant and ominous development. The Deadglyph malware is designed with interchangeable parts, known as modules. These modules are like specialized tools that it can download from a central control center (C2). Each tool, or module, comes with specific instructions called shellcodes that the malware follows to carry out different tasks. This modular approach gives threat actors the flexibility to create new tools whenever they need them.

The sophistication and modular nature of the Deadglyph malware make it likely that other threat actors will adopt similar capabilities, seeking to replicate its effectiveness and customization features in cyberattacks. Organizations should remain vigilant and update their defenses to counter such emerging threats.

Mitigation

Effective mitigation strategies against Deadglyph Malware require a multi-faceted approach, including:

Adversary Behavior Detection: Monitor for unusual behavior patterns to detect adversary attacks early, gaining insights into their tactics.

Forensic Depth Analysis: Conduct static and dynamic analysis of operating system artifacts with a focus on detecting post-breach compromises, allowing for timely response and mitigation of security incidents.

Anomaly Analysis of Operating System Artifacts: Identify irregularities in operating system artifacts by stacking and comparing outliers, enabling automated detection for swift response to potential security breaches.

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.

Technical Details

Operational Summary

The operational indicators of Deadglyph Malware are:

Registry-Based Loader: Deadglyph initiates with a registry shellcode loader that retrieves shellcode from the Windows registry, which then loads the main Deadglyph component (Executor). Notably, only the initial loader is a file on the victim's system; the rest remains encrypted within a registry entry.

Infection Vector: While the exact method isn't clear, it's suspected that an installer component is responsible for introducing the malicious code to victims.

Orchestrator's Role: The Orchestrator, written in .NET, acts as Deadglyph's central component. It communicates with a remote server, executing commands often with the Executor. Its strong obfuscation makes it challenging to analyze; essentially, it serves as Deadglyph's control center.

Communication and Commands: Deadglyph uses two obfuscated modules, Timer and Network, for server communication. The Timer module performs tasks at specific intervals, while the Network module handles server communication. Deadglyph can self-uninstall if it loses server contact for an extended period.

Modules: Core Functionality: Deadglyph's core capabilities come from additional modules obtained from the server. Three identified modules shed light on its potential, but there could be up to fourteen modules. These modules include:

Process Creator (Module 0x69): Executes specific commands as new processes and sends results to Deadglyph's control centre.

Info Collector (Module 0x6C): Gathers extensive system information, including OS details and installed software.

Multistage Shellcode Downloader Chain: A complex chain, similar to Deadglyph's main threat, assists in its installation. It starts with a CPL file downloading shellcode, which is then injected into a host process, ultimately loading a .NET assembly acting as a shellcode downloader.

Technical Details

Tactics, Techniques and Procedures

The notable TTPs related to the Deadglyph Malware are:

T1059 (Command and Scripting Interpreter):

Deadglyph executes malicious files and scripts on the victim's system as part of its infection process.

T1060 (Registry Run Keys / Start up Folder):

The malware achieves persistence by creating or modifying registry keys or adding files to the startup folder.

T1053 (Scheduled Task):

Deadglyph may create scheduled tasks to ensure it runs at specified times or events, maintaining persistence.

T1041 (Exfiltration Over Command and Control Channel):

Deadglyph exfiltrates stolen data through encrypted command and control channels to remote servers controlled by threat actors.

T1014 (Rootkit):

Deadglyph employs rootkit capabilities to hide its presence and evade detection.

T1055 (Process Injection):

Process injection techniques are used to inject malicious code into legitimate processes, making detection more challenging.

T1003 (Credential Dumping):

Deadglyph may attempt to dump credentials from compromised systems to escalate privileges or move laterally within the network.

T1005 (Data from Local System):

The malware collects data from the local system, potentially including sensitive information, for exfiltration or further analysis.

Cyber Threat Intelligence

Deadglyph is attributed to the Stealth Falcon APT, also known as Project Raven or FruityArmor, a state-sponsored hacking group associated with the United Arab Emirates (UAE). This APT has a history of targeting activists, journalists, and dissidents over the past decade. Its shift towards using Deadglyph showcases a concerning evolution in their cyber arsenal.

References

Related IOC's

- https://github.com/eset/malware-ioc/tree/master/stealthfalcon

Public Intelligence

- https://www.eset.com/int/about/newsroom/press-releases/research/uae-linked-stealth-falcon-spies-with-sophisticated-new-backdoor-on-its-neighbors-eset-research-disco/
- https://www.bleepingcomputer.com/news/security/new-stealthy-and-modular-deadglyph-malware-used-in-govt-attacks/
- https://www.hackread.com/deadglyph-backdoor-stealth-falcon-apt-middle-east/
- https://thehackernews.com/2023/09/deadglyph-new-advanced-backdoor-with.html
- https://www.infosecurity-magazine.com/news/researchers-spot-novel-deadglyph/