UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00239

SYSJOKER BACKDOOR MULTI-PLATFORM MALWARE

DATE ISSUED: 18th January 2022

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Targeting Windows, Linux & MacOS the SysJoker Backdoor Malware establishes itself on machines and lies in wait for additional code to execute. It is suspected to be spread by malicious npm packages and is proving difficult to detect.

BREAKDOWN

Popular security tools such as VirusTotal are struggling to detect SysJoker with only 6 detections currently known for the Windows version of the new multi-platform malware as reported by Intezer. Those that have been identified used a .ts TypeScript file suffix. The malware is used to establish a backdoor which can then be used to execute further commands or run code remotely, allowing attackers to perform numerous attack types and establish persistence on a system. Npm packages and other popular public code repositories are becoming an increasingly popular method for attackers to distribute malware and after Intezer's analysis of an attack, this is the suspected mechanism being used to distribute SysJoker where it masquerades as a system update. During Intezer's analysis the Command and Control (C2) changed 3 times indicating the attacker is actively monitoring infected devices. These behaviours are similar across all three targeted platforms. After execution the malware "sleep" for a random period of time before creating a C:\ProgramData\SystemData\ directory and creating a copy of itself titled "igfxCUIService.exe" indicating that it is impersonating an Intel Graphics Common User Interface Service. The malware then harvests data in temporary text files which are moved to a JSON object written to another file and establishes persistence by adding a registry key entry "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run." It will then establish a connection to the C2 by decoding a sting retrieved from text file hosted on a Google Drive and from there is able to execute numerous command types and self-deletion actions.

REMEDIATION STEPS

- Use memory scanners to detect a SysJoker Payload in memory or EDR or SIEM functions. If compromise is detected:
    1. Kill related processes and delete persistence mechanisms including all related SysJoker files.
    2. Scan and clean the infected machine
    3. Conduct a thorough investigation to discover initial entry point.
    4. If a server is discovered to be compromised check the configuration status and password length for all publicly facing server – the longer the password, the stronger it is. Check all used software versions and possible known exploits. See Intezer resource below for more information.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/undetected-sysjoker-backdoor-malwarewindows-linux-macos/177532/
Intezer https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/