Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

Manjusaka- Cybercriminal's new attack framework weapon

Date of Publication	Admilarity Code	TA Number
August 4, 2022	A1	TA2022164

Summary

Manjusaka is a new attack framework that mimics Cobalt Strike and Sliver. The new malware family implants are written in the Rust programming language and are compatible with Windows and Linux. The command and control (C2) is built in GoLang and is ELF binary with a Chinese user interface(UI).

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**T1055** Process Injection	**TA0007** Discovery	**T1082** System Information Discovery
TA0011 Command and Control	**T1102** Web Service	**TA0006** Credential Access	**T1003** OS Credential Dumping
TA0002 Execution	**T1059** Command and Scripting Interpreter	**T1049** System Network Connections Discovery	**T1083** File and Directory Discovery
T1555 Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**TA0001** Initial Access	**T1566** Phishing

Technical Details

#1

The Manjusaka implant comprises several remote access trojan (RAT) features, including a specific file management module and a limited set of conventional functionality. Executing arbitrary operations, obtaining login information from browsers, Wi-Fi passwords, taking screenshots, and obtaining extensive system information are all supported functions.

#2

The ELF version of the implant gathers system-specific data from the endpoint, such as the global system data, which includes hostname, version, machine ID, kernel, network interfaces, user account details, and CPU activity details.

#3

Distribution of a malicious document(maldoc) to targets starts the infection chain, which results in the installation of Cobalt Strike beacons on the affected systems. The malicious document has a VBA macro that runs rundll32.exe in the first stage, downloads Metasploit shellcode, and then runs in memory during the second stage.

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	58a212f4c53185993a8667afa0091b1acf6ed5ca4ff8efa8ce7dae784c276927 8e7c4df8264d33e5dc9a9d739ae11a0ee6135f5a4a9e79c354121b69ea901ba6 54830a7c10e9f1f439b7650607659cdbc89d02088e1ab7dd3e2afb93f86d4915 8e9ecd282655f0afbdb6bd562832ae6db108166022eb43ede31c9d7aacbcc0d8 a8b8d237e71d4abe959aff4517863d9f570bba1646ec4e79209ec29dda64552f 3f3eb6fd0e844bc5dad38338b19b10851083d078feb2053ea3fe5e6651331bf2 0b03c0f3c137dacf8b093638b474f7e662f58fef37d82b835887aca2839f529b fb5835f42d5611804aaa044150a20b13dcf595d91314ebef8cf6810407d85c64 955e9bbcdf1cb230c5f079a08995f510a3b96224545e04c1b1f9889d57dd33c1
URLs	https[://]39[.]104[.]90[.]45/2WYz http[://]39[.]104[.]90[.]45/2WYz http[://]39[.]104[.]90[.]45/IE9CompatViewList.xml http[://]39[.]104[.]90[.]45/submit.php
IPV4	39[.]104[.]90[.]45

References

https://blog.talosintelligence.com/2022/08/manjusaka-offensive-framework.html

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

August 4, 2022 • 5:55 AM

More at www.hivepro.com