Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

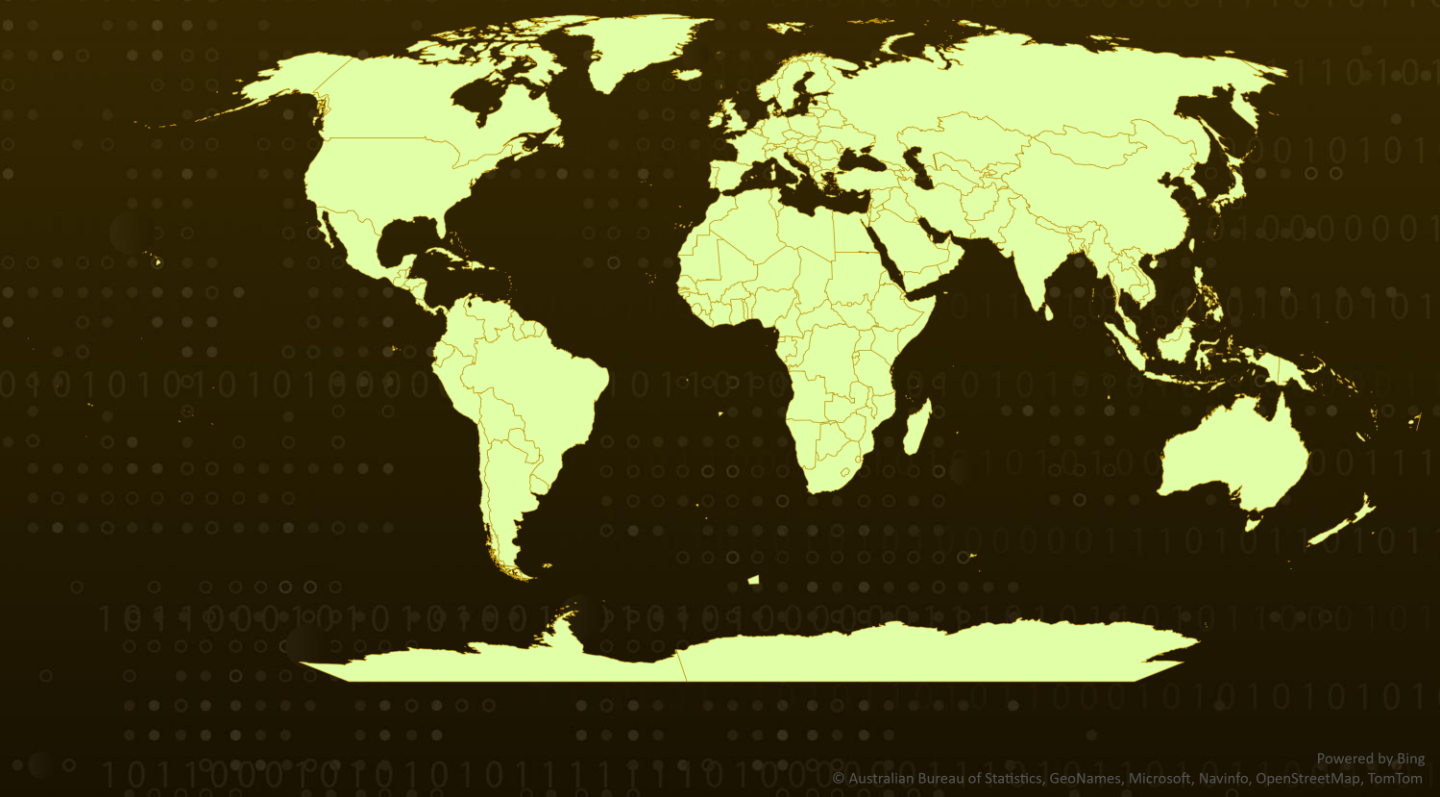
# Fickle Stealer's Dynamic Attack Strategies

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| June 21, 2024 | A1 | TA2024239 |

# Summary

**First Seen:** May 2024
**Malware:** Fickle Stealer
**Affected Browser:** Google Chrome, Microsoft Edge, Brave, Vivaldi, and Mozilla Firefox
**Attack Region:** Worldwide
**Attack:** Fickle Stealer, a Rust-based information stealer, has emerged as a major cybersecurity threat. This sophisticated malware employs a versatile targeting approach and uses four distinct distribution methods.

## Attack Regions



# Attack Details

**#1** A sophisticated Rust-based information stealer known as Fickle Stealer emerged in May 2024. This malware is disseminated through multiple strategies and is versatile in selecting its targets.

**#2** Fickle Stealer's code is highly intricate, employing four distinct distribution techniques: VBA dropper, VBA downloader, link downloader, and executable downloader. Its primary objective is to harvest sensitive information from compromised systems.

**#3** Several distribution methods utilize PowerShell scripts to bypass User Account Control (UAC) and execute Fickle Stealer. Additionally, the malware is engineered to transmit details about the victim such as country, city, IP address, operating system version, computer name, and username to a Telegram bot operated by the attacker.

**#4** The payload of Fickle Stealer is shielded by a packer that masquerades as a legitimate executable and performs a series of anti-analysis checks to detect if it is running in a sandbox or virtual machine environment. The malware extracts information from cryptocurrency wallets, web browsers based on the Chromium and Gecko engines, and other applications.

**#5** Fickle Stealer conducts a thorough search for sensitive data in common installation directories and their parent paths. It receives a dynamic target list from its command-and-control (C2) server, allowing for frequent updates as new variants of the malware are developed.

# Recommendations

**Behavior-Based Detection:** Use endpoint detection and response (EDR) solutions that can detect unusual behaviors indicative of a stealer like Fickle, such as unauthorized access attempts or anomalous system activities.

**Implement Network Segmentation:** Segment your network to isolate critical systems and sensitive data from general user access and potential malware spread. Use intrusion detection and prevention systems (IDPS) to monitor and analyze network traffic for abnormal behavior.

**Exercise Caution with Unsolicited Emails:** Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

**Content Filtering and Application Control:** Enforce application control to prevent unauthorized app installations and executions, reducing the risk of downloading and running malicious files. This integrated strategy safeguards against downloadable threats by proactively blocking access to harmful content and preventing the execution of malicious code.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0001** Initial Access | **TA0002** Execution | **TA0003** Persistence | **TA0004** Privilege Escalation |
| **TA0005** Defense Evasion | **TA0006** Credential Access | **TA0007** Discovery | **TA0011** Command and Control |
| **TA0010** Exfiltration | **T1566** Phishing | **T1059** Command and Scripting Interpreter | **T1059.001** PowerShell |
| **T1068** Exploitation for Privilege Escalation | **T1548** Abuse Elevation Control Mechanism | **T1548.002** Bypass User Account Control | **T1543** Create or Modify System Process |
| **T1036** Masquerading | **T1027** Obfuscated Files or Information | **T1027.002** Software Packing | **T1562** Impair Defenses |
| **T1555** Credentials from Password Stores | **T1087** Account Discovery | **T1497** Virtualization/Sandbox Evasion | **T1041** Exfiltration Over C2 Channel |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| File Path | C:\Users\Public\prepares.dat |
| IPv4 | 144[.]208[.]127[.]230,<br>185[.]213[.]208[.]245,<br>138[.]124[.]184[.]210 |
| URL | hxxps:// github[.]com/SkorikJR |
| SHA256 | 1b48ee91e58f319a27f29d4f3bb62e62cac34779ddc3b95a0127e67f2e141e59,<br>ad57cc0508d3550caa65fcb9ee349c4578610970c57a26b7a07a8be4c8b9bed9,<br>8e87ab1bb9870de9de4a7b409ec9baf8cae11deec49a8b7a5f73d0f34bea7e6f,<br>9ffc6a74b88b66dd269d006dec91b8b53d51afd516fe2326c6f9e3ed81d860ae,<br>48e2b9a7b8027bd03ceb611bbfe48a8a09ec6657dd5f2385fc7a75849bb14db1,<br>6f9f65c2a568ca65326b966bcf8d5b7bfb5d8ddea7c258f58b013bc5e079308b,<br>2236ffcf2856d5c9c2dedf180654cf318596614be450f6b24621dc13d7370dbf,<br>8d3ccfafc39830ee2325170e60a44eca4a24c9c4dd682a84fa60c961a0712316,<br>3ad1c2273ee77845117c0f7f55bf0050b0bcea52851d410520a694252b7bb187,<br>7034d351ce835d4905064d2b3f14adb605374a4a6885c23390db9eddd42add86,<br>c6c6304fea3fd6f906e45544b2e5119c24cda295142ed9fafd2ec320f5ff41cc,<br>97e5ac8642f413ba4b272d3cb74cba3e890b7a3f7a7935e6ca58944dbb9bfe54,<br>011992cfa6abaeb71d0bb6fc05f1b5623b5e710c8c711bca961bf99d0e4cae38,<br>5fbd700bd77d3f632ba6ce148281c74a20391a40c7984f108f63a20dc442f8d6,<br>d9dcae235891f206d1baabfcbd79cb80337b5e462adef9516b94efc696b596b7,<br>679e9ba645e17cceeff14be7f5f7dff8582d68eba5712c5928a092e1eec55c84, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 4d78793719d14f92f5bb9ecc7c2fa9e51c1bf332de26aa7746f35d7e42362db8,<br>d55611fce7fcdd6b49066b194196577ee12bffa98400b724d013fc3a1e254f34,<br>346e18b7ce2e3c3c5412dacdc8034a7566dee12ea0aafc6b82f196dcba2453f8,<br>20e1d7af698e3e2f5092815be1a0415019511da99550fdcc050741f4b47551fa,<br>f71069aed94e4b13d70bd9ee7b2a8fc8580c4339aa9ba9d8baf15abf95d6f673,<br>94ee2227696da3049ff67592834b4b6f98186f91e6d1cd1eeec44f24b9df754b,<br>24e44d000a61de06b63b532ef237d9f41aa897f4d9f46f8abaf9e654074a65af,<br>a04677fe4ba06b66f698e4969b749174d30477283d97b5eaee16ffeb305d9c0a,<br>7b9e09227b036428a41dd46b6d6e354bb0c3822ce201c1a14d083116916e078d,<br>0494077ac65aa278680002f3b73c61c8896303668c62139a9db5a042923fd0ce,<br>47e4142fa6ab10a2d7dc0423d41f9bdbb3ced0f4fae5c58b673386d11dd8c973,<br>46caee016da4b460f7c242e19a88e8dc7544ded7d2528b0b9e918a7be64b5ceb,<br>b05736874d383ed2e8dcc9d392f2c04e0fd545b8880620499d720c44adb18822,<br>bf8b8f964d1c67aee82ad01528423077ef5e6c65de6d95e446c9343868849350,<br>4602d8f9e2150744e89958d813354696abe6800ee55ef70c48db3134e964a13a,<br>70363b97f955e5d30fb8d3a8d2a439303f88707420c05f051f87e0458fdfffc2,<br>62ff72aa8a8c5bccdf6c789952ee054a0d0d479e417fa20ea73a936e17bdf043,<br>5f24168581cdaef32e60a62ba7123917bbe65f2f8410d759f345587eb406be40,<br>effb85aaef61cd8918d66513da1573365be2743ec263be4029a6b827e3ecc1c6,<br>b57caa40f680d468bbf811e798ef9881d6158fb3462dd9bedb4658d17aed44a5,<br>26fa0ccc5c7b7733ee6ffc2c70edef067b6764387ef1b16cb8005f28c34a3d84,<br>f080d7803ce1a1b9dc72da6ddf0dd17e23eb8227c497f09aa7dfd6f3b5be3a66,<br>93db0d88966519e76db4995a3b67ca548e4aa9675806295a790eedf585e0aa2f, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 9f7591c9d9bc66029e6a341a4fb8828361fc14b1918f9e35506c608359fa1eec, e9bc44cf548a70e7285499209973faf44b7374dece1413dfcdc03bf25a6c599c, a641d10798be5224c8c32dfaab0dd353cd7bb06a2d57d9630e13fb1975d03a53, 9ce52929765433ff8bf905764d7b83c4c3fcbefb4f12eabcf16ee3dddcd3759d, b7bdb0cc90b11c4738c2af218a1a53e4c65b6c91c6067c224164b8fcfc3eed8c, f878a88b7dda1155fe939abe0500e32d5fba34569ca933bccb5603d9e0e96cc0, bfe2d817e20ecff45cc92b7b8f4e1cd0482b48a769940402eaa5b31cbfb9b908, 09b47fd0e1fcab827d1a723f9db7e402502ec91e57b7217ed85094abd98bc637, 978400108aa16e464b1fbc300bc270bc89193e3c3890d5e9373b3034b592b4da, e394f96ee040508063606343b1ad2158e266dcbd8beb3ba4a23936d1957e5ad6 |

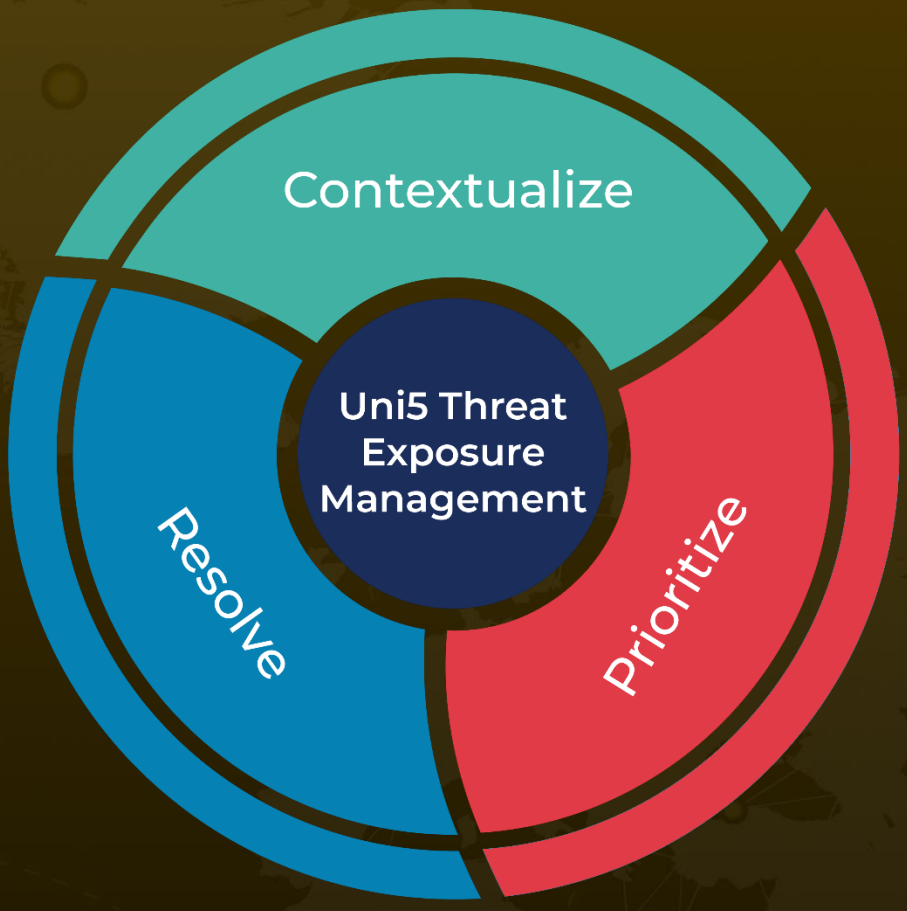
## References

https://www.fortinet.com/blog/threat-research/fickle-stealer-distributed-via-multiple-attack-chain

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**June 21, 2024 • 6:30 AM**



More at www.hivepro.com