Hive Pro®

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

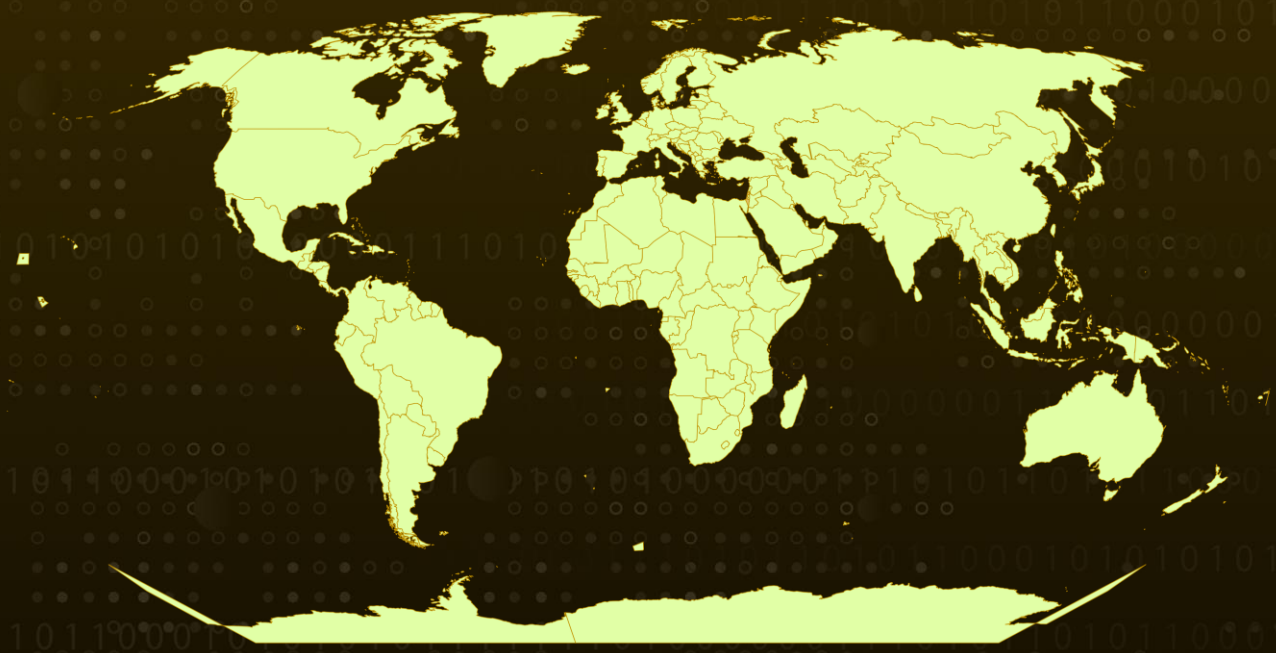
# Jupyter Infostealer Returns with New Addition to Its Arsenal

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| November 07, 2023 | A1 | TA2023448 |

# Summary

**First appeared:** Late 2020
**Attack Region:** Worldwide
**Targeted Industry:** Education and Health sectors
**Malware:** Jupyter Infostealer (aka Yellow Cockatoo, Solarmarker, Polazert)
**Attack:** Jupyter Infostealer is a malware variant initially discovered in late 2020. Since then, it has undergone continued evolution, altering its delivery methods and techniques to avoid detection and establish persistence on compromised systems. New variants of the Jupyter Infostealer are aimed at evading detection and ensuring persistence, allowing attackers to compromise their victims in a stealthy manner.

## Attack Regions



# Attack Details

**#1** Jupyter Infostealer is a malware variant that was initially identified in late 2020. This malware uses various techniques, including manipulated search engine optimization (SEO) tactics and malvertising, as an initial access vector. It deceives users who are searching for popular software into downloading it from untrustworthy websites. Jupyter Infostealer is known for its ability to harvest credentials and its use of encrypted C2 communication to exfiltrate sensitive data.

**#2** Jupyter, the information-stealing malware, has surfaced back with subtle but significant changes that enable it to stealthily create a long-lasting presence on infected systems. The malware used in these recent waves of Jupyter Infostealer assaults changes PowerShell commands and adds private key signatures in an attempt to pass for a genuine signed file and avoid detection.

**#3** Jupyter Infostealer can be distributed in a number of ways, just like the majority of other malware. Phishing emails, drive-by downloads, and rogue websites are common delivery techniques. When users click on fraudulent ads or visit compromised websites, they could unintentionally download Jupyter Infostealer. Popular online browsers like Firefox, Chrome, and Edge are frequently the targets of malware.

**#4** The recent iterations of Jupyter Infostealer have become more sophisticated, utilizing various certificates to sign the malware, creating a false appearance of legitimacy. However, these fake installers activate the infection chain when executed. These installers initiate an interim payload that utilizes PowerShell to connect to a remote server. Finally, the remote server decodes and launches the Jupyter Infostealer malware, allowing it to stealthily compromise the target system.

**#5** Indeed, Jupyter Infostealer has demonstrated a remarkable ability to adapt and evolve over time. The changes implemented in its techniques aim to enhance its evasion capabilities, making it more challenging to detect by security systems and allowing it to maintain its stealthy presence on compromised systems.

# Recommendations

**Robust Endpoint Security:** Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

**Remain vigilant:** It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

**Implement Behavioral Analysis:** Deploy advanced security solutions that employ behavioral analysis and monitoring on the host for detection of unusual activities and anomalies in the system. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

**Email Security Measures:** Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to sandbox suspicious or untrusted URLs.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence | TA0004<br>Privilege Escalation |
| TA0005<br>Defense Evasion | TA0006<br>Credential Access | TA0007<br>Discovery | TA0009<br>Collection |
| TA0011<br>Command and Control | TA0010<br>Exfiltration | T1566<br>Phishing | T1204<br>User Execution |
| T1204.002<br>Malicious File | T1059<br>Command and Scripting Interpreter | T1059.001<br>PowerShell | T1055<br>Process Injection |
| T1547<br>Boot or Logon Autostart Execution | T1547.001<br>Registry Run Keys / Startup Folder | T1564<br>Hide Artifacts | T1564.003<br>Hidden Window |

| | | | |
|---|---|---|---|
| **T1620** Reflective Code Loading | **T1027** Obfuscated Files or Information | **T1027.011** Fileless Storage | **T1036** Masquerading |
| **T1070** Indicator Removal | **T1070.004** File Deletion | **T1112** Modify Registry | **T1082** System Information Discovery |
| **T1083** File and Directory Discovery | **T1552** Unsecured Credentials | **T1552.001** Credentials In Files | **T1105** Ingress Tool Transfer |
| **T1005** Data from Local System | **T1071** Application Layer Protocol | **T1071.001** Web Protocols | **T1041** Exfiltration Over C2 Channel |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| IP | 146.70.101[.]83, 224.0.0[.]251, 78.135.73[.]176, 146.70.71[.]13, 239.255.255[.]250, 91.206.178[.]10, 185.243.112[.]60, 146.70.121[.]88 |
| SHA256 | 820eda2078723e7f1c09d0e6d3641ea822c2b36c981cb5bfa4e445733664c087, 95a96d21f89b5e73ad41c5af5381f54a2697abd0c8490b4fd180ad88e9677452, 32e0c3db78cdeaa026b8b9ed9c3e4f599eb5d9cb4184aaacae8ec94a0c1be438, ad7098b4882cdd187a2c2bdf87f6e4cb6c76017975a135cf9c9dcd49ce1f30d7, c083bf80cfc91f4e3c696bab27760163b9b7621ff4e1230b8129d44b52ccf79a, 39102fb7bb6a74a9c8cb6d46419f9015b381199ea8524c1376672b30fffd69d2, fee1e684cc9588c9aea22c48e9745d0f3150479b2c094c0de598247487fc3f89, 7d57b32e3753a28d2e106392fef0c02ec549062f607563732a64abb4ad949fde |

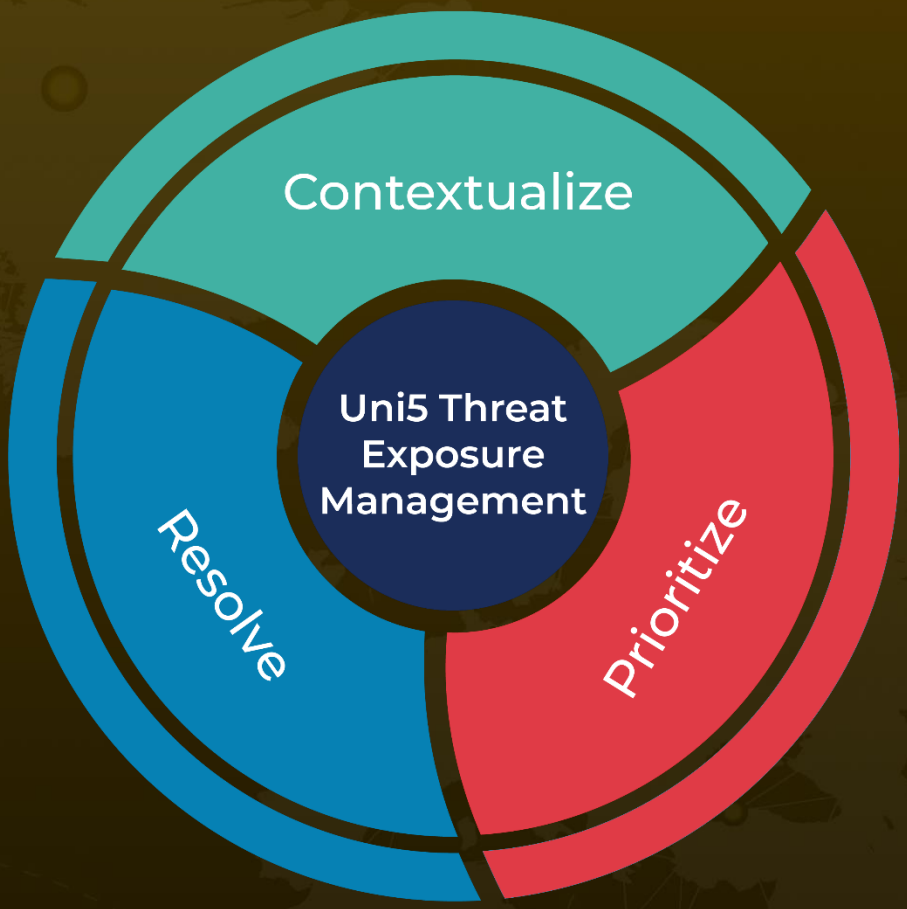
# References

https://blogs.vmware.com/security/2023/11/jupyter-rising-an-update-on-jupyter-infostealer.html

# 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

**November 07, 2023 • 4:00 AM**



More at www.hivepro.com