Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

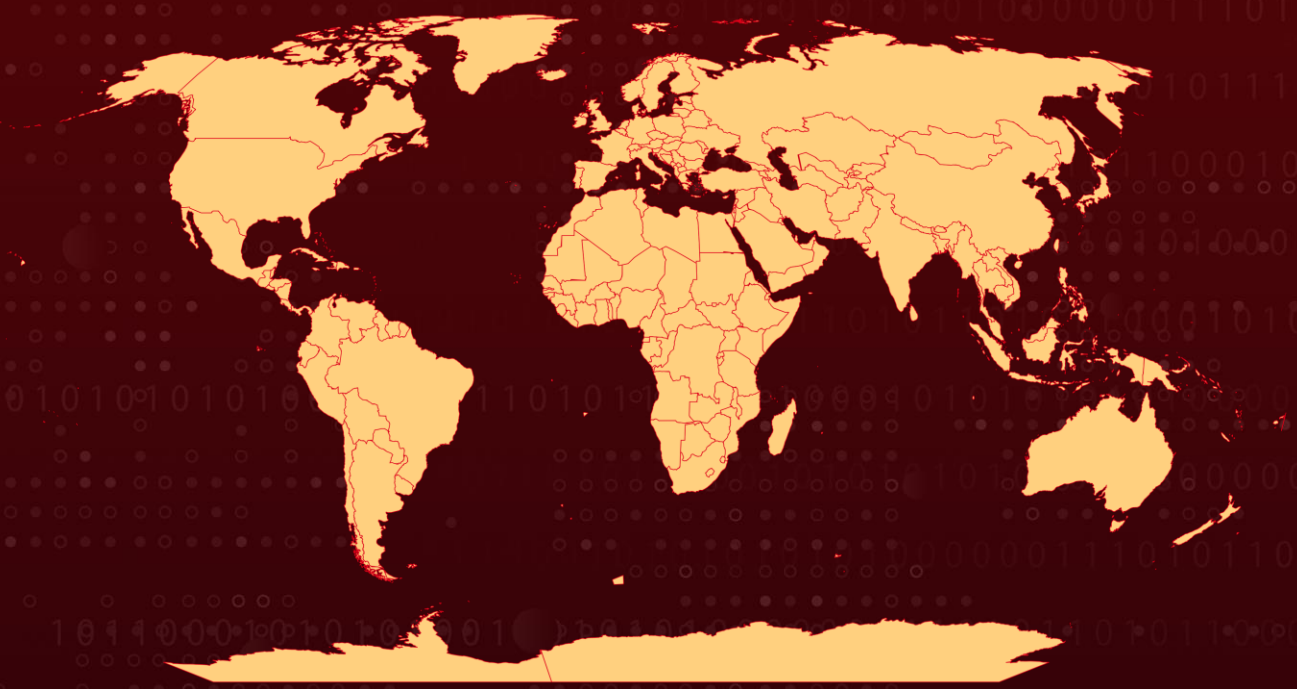
BunnyLoader: The New Malware-as-a-Service Threat

Date of Publication	Admiralty Code	TA Number
October 5, 2023	A1	TA2023398

Summary

First Appearance: September 4, 2023
Attack Region: Worldwide
Affected Platforms: Windows
Malware: BunnyLoader
Attack: BunnyLoader is a Malware-as-a-Service threat, boasting advanced features like anti-sandbox techniques, keylogging, stealing data, cryptocurrency wallets and remote command execution, posing risks to infected systems.

Attack Regions



Attack Details

#1 A new Malware-as-a-Service (MaaS) threat called "BunnyLoader" being sold on various forums. BunnyLoader is a malicious software loader written in C/C++ and is sold for $250. It offers a range of features and functionalities, including downloading and executing second-stage payloads, stealing browser credentials and system information, and more.

#2 The malware is rapidly evolving, with frequent updates and bug fixes. It employs various anti-sandbox techniques to avoid detection, including checking for specific modules, querying system information, and detecting sandbox usernames. If a sandbox is identified, BunnyLoader displays a misleading error message.

#3 BunnyLoader communicates with a command-and-control (C2) server, where it can receive tasks and commands. The C2 panel allows attackers to manage tasks such as downloading and executing additional malware, keylogging, stealing credentials, manipulating clipboard content to steal cryptocurrency, and running remote commands on infected machines.

#4 Upon execution, BunnyLoader maintains persistence on the infected system and hides itself. It creates registry values, a mutex, and performs various checks to avoid running in a virtualized environment. It also checks for Docker containers and blacklisted sandbox usernames.

#5 BunnyLoader can steal information related to web browsers, cryptocurrency wallets, VPNs, and messaging applications. Stolen data is stored in a folder named "BunnyLogs" in the Appdata\Local directory, compressed as a ZIP archive, and exfiltrated to the C2 server.

#6 The malware also includes a clipper module that monitors the victim's clipboard for cryptocurrency addresses and replaces them with addresses controlled by the attacker. It can target multiple cryptocurrencies, including Bitcoin, Monero, Ethereum, Litecoin, Dogecoin, ZCash, and Tether.

#7 BunnyLoader performs various types of download and execute tasks, including downloading files from URLs provided by the C2 server and executing them. It can also perform fileless execution by injecting downloaded payloads into existing processes. The malware includes a "Heartbeat" mechanism to inform the C2 server that the infected system is online.

Recommendations

Network Segmentation: Segment your network to limit lateral movement if BunnyLoader infects one part of your network. This can help prevent the malware from spreading to critical systems.

Regular Software Updates: Ensure that all operating systems, software applications, and security solutions are kept up-to-date with the latest patches and updates. This helps eliminate vulnerabilities that adversaries may exploit to deploy malware like BunnyLoader.

Endpoint Security: Use robust endpoint protection solutions that include antivirus, anti-malware, and behavior-based detection to safeguard individual devices from malware and other threats.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0001 Initial Access	TA0005 Defense Evasion	TA0009 Collection
TA0040 Impact	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0002 Execution
TA0008 Lateral Movement	TA0006 Credential Access	T1056.001 Keylogging	T1056 Input Capture
T1115 Clipboard Data	T1560.002 Archive via Library	T1560 Archive Collected Data	T1497 Virtualization/Sandbox Evasion
T1539 Steal Web Session Cookie	T1528 Steal Application Access Token	T1055.012 Process Hollowing	T1055 Process Injection
T1112 Modify Registry	T1543 Create or Modify System Process	T1547 Boot or Logon Autostart Execution	T1102 Web Service

T1053 Scheduled Task/Job	T1041 Exfiltration Over C2 Channel	T1133 External Remote Services	T1190 Exploit Public-Facing Application
T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	37[.]139[.]129[.]145
MD5	Dbf727e1effc3631ae634d95a0d88bf3, Bbf53c2f20ac95a3bc18ea7575f2344b, 59ac3eacd67228850d5478fd3f18df78

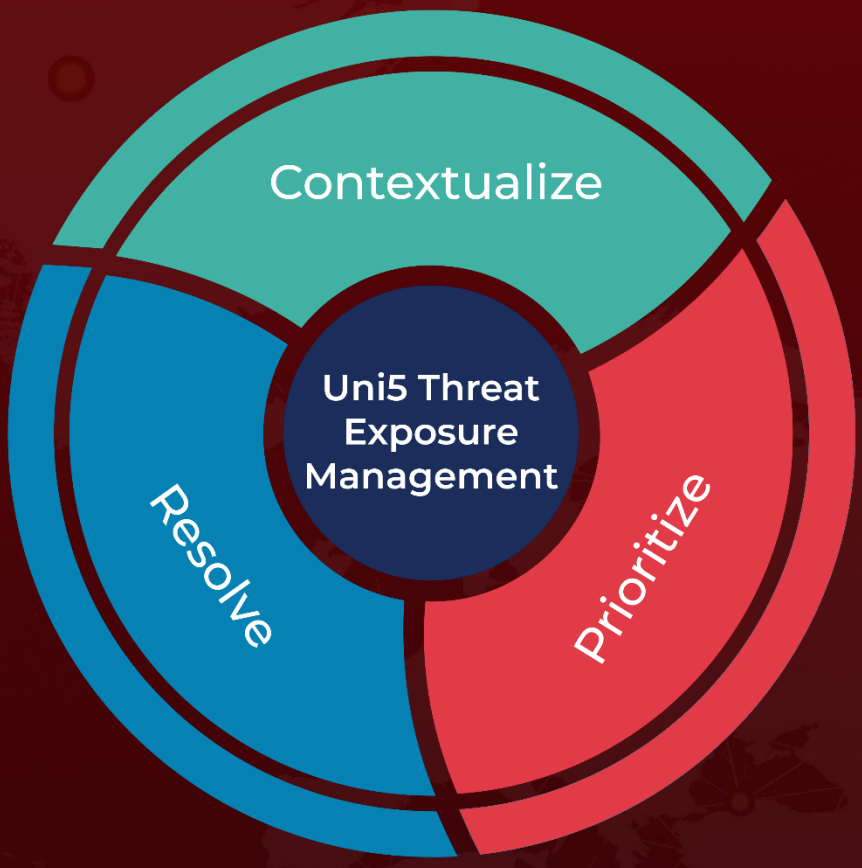
References

https://www.zscaler.com/blogs/security-research/bunnyloader-newest-malware-service

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

October 5, 2023 . 6:30 AM

More at www.hivepro.com