Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Unveiling BunnyLoader 3.0 Enhanced Malware Capabilities

Date of Publication	Admiralty Code	TA Number
March 21, 2024	A1	TA2024110

Summary

Attack Began: February 11, 2024
Targeted Countries: Worldwide (excluding Russia)
Malware: BunnyLoader 3.0
Affected Platform: Windows
Attack: BunnyLoader 3.0, which has been active since September 2023, is a malicious malware variant known for its enhanced data theft and advanced keylogging capabilities. This modular malware provides attackers with flexibility and presents challenges in terms of detection. Despite its global targeting, it refrains from infecting systems in Russia. With its accessibility and growing features, BunnyLoader 3.0 poses a serious threat.

Attack Regions

Attack Details

#1 BunnyLoader 3.0 is a recent and concerning variant of the BunnyLoader malware. First discovered in September 2023, BunnyLoader is a Malware-as-a-Service (MaaS) that has been steadily evolving with new features and updates.

#2 This latest iteration, BunnyLoader 3.0, was released in February 2024 and boasts significant improvements over its predecessors. Key enhancements include completely rewritten modules for data theft, resulting in a smaller payload size and improved performance. One of the most concerning additions is BunnyLoader 3.0's advanced keylogging capabilities, allowing it to capture a wider range of sensitive information from victims.

#3 Another distinguishing feature of BunnyLoader 3.0 is its modular design. The malware separates its core functionality from additional malicious payloads, giving its operators more flexibility. They can choose to deploy the core functionality on its own or combine it with other malware payloads for a more comprehensive attack. This modularity also makes it more challenging for security researchers to detect and analyze BunnyLoader 3.0.

#4 A Denial of Service (DoS) module included as a new feature in BunnyLoader 3.0. This module allows attackers to remotely instruct infected devices to launch HTTP flood attacks against a target webserver, potentially overwhelming it with traffic and causing it to become unavailable to legitimate users.

#5 Interestingly, the malware's code includes a geo-restriction that prevents it from infecting systems located in Russia. The reasons behind this restriction are not entirely clear, but it may be an attempt to evade detection by Russian authorities or to avoid competition from other cybercriminals operating in that region.

#6 BunnyLoader 3.0 is a significant threat due to its ease of access and expanding functionality. The malware is available for purchase on cybercrime forums, making it accessible to a wide range of attackers. Its modular design and improved data theft capabilities make it a versatile tool for cybercriminals looking to steal sensitive information and deploy additional malware payloads on victim devices.

Recommendations

Strengthen Endpoint Security: Employ robust endpoint security solutions that include advanced threat detection mechanisms to identify and block BunnyLoader 3.0 and other evolving malware variants. Ensure that endpoint protection software is regularly updated to defend against new threats.

Deploy Network Monitoring Tools: Utilize network monitoring tools to detect and analyze suspicious network traffic patterns that may indicate the presence of BunnyLoader 3.0 or other malware infections. Monitor for unusual outbound connections and communication with known malicious domains.

Keep Software and Systems Updated: Maintain a proactive approach to patch management by ensuring that all software applications, operating systems, and firmware are promptly updated with the latest security patches and updates. Vulnerabilities in outdated software can be exploited by malware like BunnyLoader 3.0.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0005 Defense Evasion	TA0002 Execution	TA0003 Persistence
TA0010 Exfiltration	TA0011 Command and Control	TA0009 Collection	TA0006 Credential Access
T1132 Data Encoding	T1059 Command and Scripting Interpreter	T1113 Screen Capture	T1083 File and Directory Discovery
T1056.001 Keylogging	T1056 Input Capture	T1027 Obfuscated Files or Information	T1036 Masquerading
T1115 Clipboard Data	T1027.011 Fileless Storage	T1657 Financial Theft	T1555 Credentials from Password Stores
T1071.001 Web Protocols	T1071 Application Layer Protocol	T1048 Exfiltration Over Alternative Protocol	T1055 Process Injection

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3a64f44275b6ff41912654ae1a4af1d9c629f94b8062be441902aeff2d38af3e, 0f425950ceaed6578b2ad22b7baea7d5fe4fd550a97af501bca87d9eb551b825, 82a3c2fd57ceab60f2944b6fea352c2aab62b79fb34e3ddc804ae2dbc2464eef, 2ab21d859f1c3c21a69216c176499c79591da63e1907b0d155f45bb9c6aed4eb, c006f2f58784671504a1f2e7df8da495759227e64f58657f23efee4f9eb58216, 52b7cdf5402f77f11ffebc2988fc8cdcd727f51a2f87ce3b88a41fd0fb06a124, 5f09411395c8803f2a735b71822ad15aa454f47e96fd10acc98da4862524813a, cc2acf344677e4742b22725ff310492919499e357a95b609e80eaddc2b155b4b, ebc17dbf5970acb38c35e08560ae7b38c7394f503f227575cd56ba1a4c87c8a4, 2d39bedba2a6fb48bf56633cc6943edc6fbc86aa15a06c03776f9971a9d2c550, 2e9d6fb42990126155b8e781f4ba941d54bcc346bcf85b30e3348dde75fbeca1, 74c56662da67972bf4554ff9b23afc5bdab477ba8d4929e1d7dbc608bdc96994, fffdf51cdb54f707db617b29e2178bb54b67f527c866289887a7ada4d26b7563, 62f041b12b8b4e0debd6e7e4556b4c6ae7066fa17e67900dcbc991dbd6a8443f, 1a5ad9ae7b0dcdc2edb7e93556f2c59c84f113879df380d95835fb8ea3914ed8, c80a63350ec791a16d84b759da72e043891b739a04c7c1709af83da00f7fdc3a
IPv4	37.139.129[.]145, 37.139.129[.]145, 37.139.129[.]145, 37.139.129[.]145, 37.139.129[.]145, 185.241.208[.]83, 185.241.208[.]83, 185.241.208[.]83, 185.241.208[.]83, 195.10.205[.]23,

TYPE	VALUE
IPv4	172.105.124[.]34, 185.241.208[.]104, 134.122.197[.]80, 134.122.197[.]80, 134.122.197[.]80

References

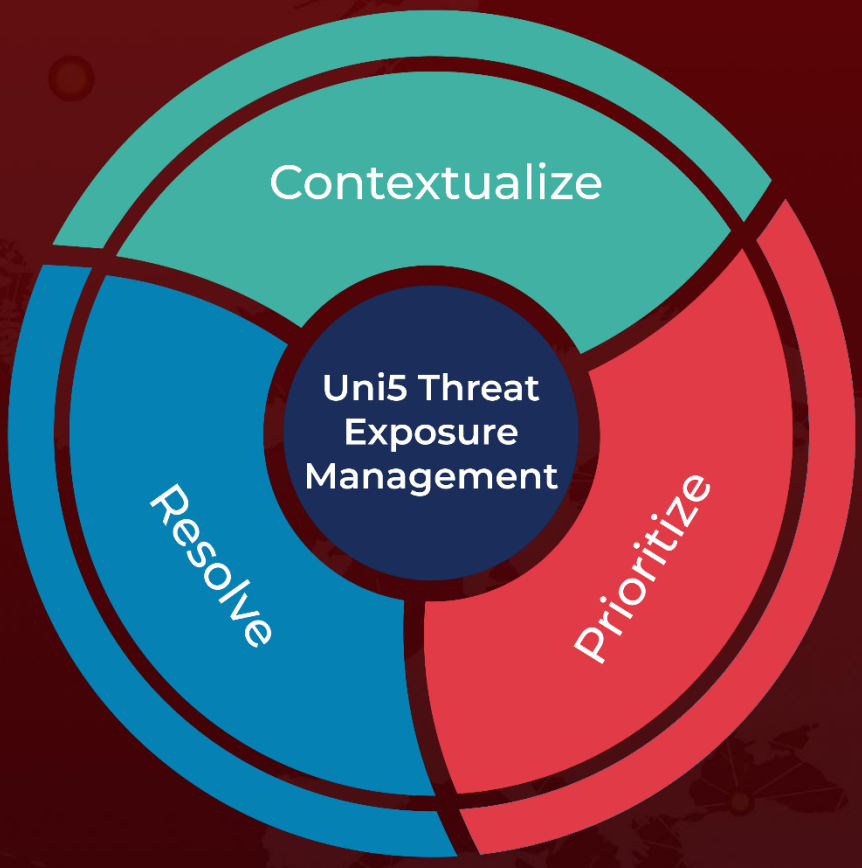
https://unit42.paloaltonetworks.com/analysis-of-bunnyloader-malware/

https://www.hivepro.com/threat-advisory/bunnyloader-the-new-malware-as-a-service-threat/

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

March 21, 2024 • 5:30 AM

More at www.hivepro.com