KPMG Cyber Threat Intelligence Platform

BunnyLoader 3.0 – Digging into Digital Havoc

TLP : Clear

KPMG. Make the Difference.

BunnyLoader is a rapidly evolving Malware-as-a-Service (MaaS) that was initially recognized in September 2023 for its capability to steal credentials, information, and cryptocurrency. The latest version, BunnyLoader 3.0, was introduced by its developer, "Player", on February 2024, this expands on previous versions by adding Denial-of-Service (DoS) functionality for launching HTTP flood attacks against targeted URLs. The threat actor claims that the payloads have been enhanced with completely rewritten modules for improved performance, reduced payload size, and advanced keylogging capabilities.

The attack begins with an undocumented dropper, which may be delivered via various means like phishing emails with malicious attachments. Upon execution, the dropper installs the PureCrypter payload, which splits into two branches: one drops the PureLogs loader and stealer, while the other delivers BunnyLoader, which installs Meduza malware. During execution, BunnyLoader evades detection by decompressing and decrypting itself directly in memory. BunnyLoader establishes persistence by modifying registry keys or creating scheduled tasks to survive reboots and maintain access. It connects to its C2 server to retrieve instructions and additional payloads using a new modular structure. BunnyLoader uses an updated communication protocol, sending encrypted HTTP parameters with RC4 encryption to ensure secure and less detectable data transmission. It utilizes the stealer module to harvest credentials, while the keylogger records keystrokes, saving them to log files. By communicating with the C2 server every two seconds, it continually receives updates and instructions, ensuring its persistent presence.

BunnyLoader's rapid evolution and sophisticated approach make it easy for anyone worldwide to fall prey to its tactics, highlighting the urgent need for cyber resilience and awareness.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

BunnyLoader 3.0 – Digging into Digital Havoc

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
91.92.254[.]31	185.241.208[.]83
91.92.247[.]212	172.105.124[.]34
195.10.205[.]23	134.122.197[.]80
37.139.129[.]145	185.241.208[.]104

Indicators of Compromise: Hashes
9dae516b7ad2b51d1c06b68486ace79b
66ff4001f31b4ee0098e16c82b8532a2
616b48133c6af2445736435912d4a586
5bf25368a2614b9f12a3e6eda517c626
fd2d8b60aa33d5e893f8968ca38dc3f7
baaccddc8a452b4dfcc2ba0847a0a178
38aecdfd279d1a2a6b0615d10cb0efd9
051a4f06117e95526261257d2ed02892
d1af6fa15fc5bfe005609d122ba5f3c2
70f25c6ebbc8977f8ca79c70cfdef28d
51162a09c37f256ca46c685958db09fd
2f05a56a349dce85119e7fda9e8047ac
99310a4915617e321b4d65b443da7029
160e743ef32c8ef11b06c71a69acb980
194118c43c65faad06bf5ff6cd9b52a2
121e8ad4193710ce80f9df6710d275bb
dbf727e1effc3631ae634d95a0d88bf3
bbf53c2f20ac95a3bc18ea7575f2344b
59ac3eacd67228850d5478fd3f18df78
a335e0d3035e8da489877d7a07b987ad56489072

KPMG

KPMG Cyber Threat Intelligence Platform

BunnyLoader 3.0 – Digging into Digital Havoc

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
89d64456367ea5887c75d4d53fcaf19fdf5c4a6b
0a0702e7f6a75d047ae1b3cec8fc40b6e5f75992
a0add337a3838a962fa392455dfb3105a847d8e8
89be14bcbfc249a7cd9cc53d0d4857fefd168994
02e18bb8f170f692e76164720025c4e7bc92b15f
0ebc02ad46db642fd1ac586eb807f720a50686f1
d321877d036a4d64e9e47cc8b6f49ceca3984b1b
4f2583874778a12a00f114d6af3e1c8cfc02323a
88940df22e5753072da61701d9023743fddf8f89
047e89fb82b54aba7e9e5a18c32692b23f5a1700
2f5afa9af299cba599c57fd99319268db803b31b
aea7d8951f76a7994042a09f2ad0409ba866faf8
7463a0f440a483285c6af813a69e3d70288029a6
7bdf85b3968747acf21d37df5e56d54f8a0c7e62
975e2ca86686e6f53362a78d914b4ad8c0ad5c1f
c02d2a18eca78b91b4c4e9e7a45c8d17c8c5bbca
059d27dbb4777ed1f17b2aa42c0e7c19ad29b304
cdc11d2244321b850fad88a92e704a8ce2255ca7
3a64f44275b6ff41912654ae1a4af1d9c629f94b8062be441902aeff2d38af3e
0f425950ceaed6578b2ad22b7baea7d5fe4fd550a97af501bca87d9eb551b825
82a3c2fd57ceab60f2944b6fea352c2aab62b79fb34e3ddc804ae2dbc2464eef
2ab21d859f1c3c21a69216c176499c79591da63e1907b0d155f45bb9c6aed4be
c006f2f58784671504a1f2e7df8da495759227e64f58657f23efee4f9eb58216
52b7cdf5402f77f11ffebc2988fc8cdcd727f51a2f87ce3b88a41fd0fb06a124
5f09411395c8803f2a735b71822ad15aa454f47e96fd10acc98da4862524813a
cc2acf344677e4742b22725ff310492919499e357a95b609e80eaddc2b155b4b

KPMG

KPMG Cyber Threat Intelligence Platform

BunnyLoader 3.0 – Digging into Digital Havoc

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
ebc17dbf5970acb38c35e08560ae7b38c7394f503f227575cd56ba1a4c87c8a4
2d39bedba2a6fb48bf56633cc6943edc6fbc86aa15a06c03776f9971a9d2c550
2e9d6fb42990126155b8e781f4ba941d54bcc346bcf85b30e3348dde75fbeca1
74c56662da67972bf4554ff9b23afc5bdab477ba8d4929e1d7dbc608bdc96994
fffdf51cdb54f707db617b29e2178bb54b67f527c866289887a7ada4d26b7563
62f041b12b8b4e0debd6e7e4556b4c6ae7066fa17e67900dcbc991dbd6a8443f
1a5ad9ae7b0dcdc2edb7e93556f2c59c84f113879df380d95835fb8ea3914ed8
c80a63350ec791a16d84b759da72e043891b739a04c7c1709af83da00f7fdc3a
454bd68088f17718527b300134cae3eed1c7db3ba7ed9e08d291ef7729229a79
90e6ebc879283382d8b62679351ee7e1aaf7e79c23dd1e462e840838feaa5e69
9b8efc369c7ff541f885c605c462c7d5a16acfbdfef3b28adc4e5418e890142f