Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

New Python-Based Fileless Malware Named 'PyLoose' Targeting Cloud Environments

Date of Publication	Admiralty Code	TA Number
July 13, 2023	A1	TA2023297

Summary

First appeared: June 22, 2023
Attack Region: Worldwide
Affected Platform: Various cloud platforms and hosting providers that support Jupyter Notebook deployments, such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and others
Targeted Industries: Cloud Technology
Malware: PyLoose
Attack: A new fileless attack called PyLoose targets cloud workloads by loading an XMRig Miner directly into memory using Python code and the memfd technique. This evasive attack highlights the need for advanced security solutions and precautions like avoiding public exposure of services and constraining system command execution.

Attack Regions

Attack Details

#1

A new Python-based fileless malware called PyLoose has been targeting cloud workloads. This attack involves Python code that loads an XMRig Miner directly into memory using the memfd Linux fileless technique. It is the first publicly documented Python-based fileless attack targeting cloud workloads, and approximately 200 instances of the attack for crypto mining have been found.

#2

Fileless attacks targeting cloud workloads are not frequently reported. The last known activity was reported over two years ago when TeamTNT used the Ezuri tool written in Go for loading a fileless payload. These attacks are evasive as they do not rely on writing payloads to disk, making them difficult to detect with traditional security solutions.

#3

The PyLoose attack involves a simple Python script that contains a compressed and encoded XMRig miner. The script was uploaded to VirusTotal with zero detections. The attack flow starts with initial access through a publicly accessible Jupyter Notebook service that failed to restrict system command execution. The attacker downloads the fileless payload into the Python runtime's memory using an HTTPS GET request, bypassing disk storage. The script then decodes and decompresses the XMRig miner, loading it into memory via the memfd file descriptor.

#4

The in-memory XMRig execution connects to the MoneroOcean mining pool. Fileless attacks are preferred by threat actors due to their evasiveness and difficulty in detection and investigation. The memfd fileless execution technique is utilized to execute payloads without writing them to disk, bypassing traditional security tools. The attacker used an open data-sharing service to host the Python payload and adapted the fileless execution technique.

Recommendations

Secure access and authentication to Jupyter Notebook services. This can be achieved by avoiding public exposure and implementing proper access controls. Utilize strong authentication methods such as complex passwords or security tokens to prevent unauthorized access. Consider implementing a centrally managed identity platform with multi-factor authentication (MFA) for enhanced security.

Harden the execution environment of Jupyter Notebook. Configure the environment to restrict the execution of system commands and limit the usage of potentially risky Python modules like "os" and "subprocess." Regularly update and patch the Jupyter Notebook software to address any known security vulnerabilities and ensure a secure execution environment.

Deploy advanced security solutions to detect and prevent fileless attacks. Utilize security solutions that employ runtime behavior-based analysis and memory monitoring techniques to identify suspicious activities. Implement endpoint detection and response (EDR) solutions capable of detecting fileless attacks and malicious behavior in memory. Consider using security solutions powered by machine learning and artificial intelligence to proactively detect and block emerging threats.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0011 Command and Control	TA0005 Defense Evasion	TA0002 Execution
T1105 Ingress Tool Transfer	T1102 Web Service	T1140 Deobfuscate/Decode Files or Information	T1027.002 Software Packing
T1027 Obfuscated Files or Information	T1620 Reflective Code Loading	T1496 Resource Hijacking	T1059.006 Python
T1071.001 Web Protocols	T1071 Application Layer Protocol	T1132.001 Standard Encoding	T1132 Data Encoding

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	d422493b47e4798717f2b05a482c97ef9e6b74b9, eba82ed21b329b0955ab87b2397a949628349b3f
SHA256	25232290fa9fa5529240a4e893ce206dfdcfc28d0b3a1b89389f7270f1046822, 935ee206846223e6d2db3f62d05101c0bea741e7b43e1b73c1eb008f947d5ff1
MD5	059f83f8969b09c29c95b17452718ea3, fec5b820594579f1088db47583d2c62d
IPV4:PORT	51[.]75[.]64[.]249[:]20128
DNS	gulf[.]moneroocean[.]stream, Pool[.]sabu-sabu[.]ml, pool[.]xiao[.]my[.]id
Monero wallet address	85DS3ShGZwtFffeQUrDK8Db12qwCcaCHofNcZdjMkjTCfWiRv9WLe4cR2W97eGnRXwBxDhTK7BbbE2Z7t4gjXRz1VLPmhn7

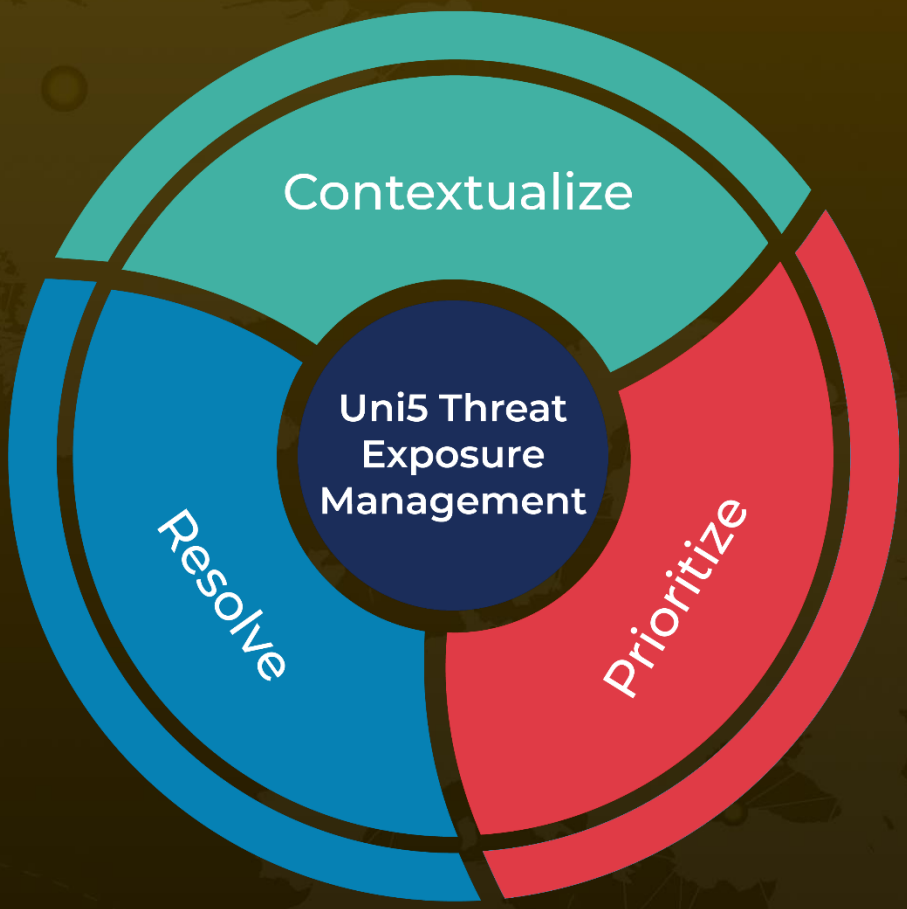
References

https://www.wiz.io/blog/pyloose-first-python-based-fileless-attack-on-cloud-workloads

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

July 13, 2023 • 5:30 AM

More at www.hivepro.com