Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

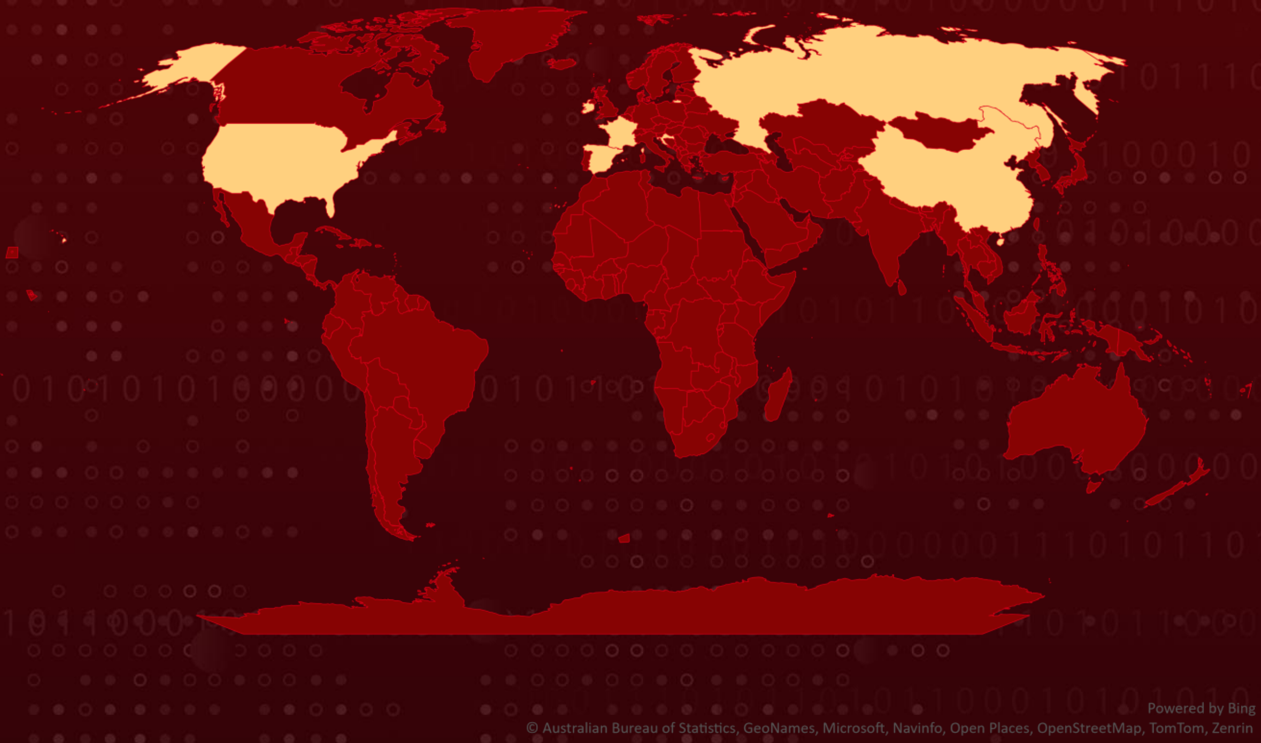
BlazeStealer Malware Uncovered in Python Packages on PyPI

Date of Publication	Admiralty Code	TA Number
November 09, 2023	A1	TA2023454

Summary

Attack Began: January 2023
Attack Region: US, China, Russia, Ireland, Hong Kong, Croatia, France, Spain
Malware: BlazeStealer
Attack: Python Package Index (PyPI) repository is infiltrated with number of malicious python packages. These packages masquerade as obfuscation tools, however they harbor BlazeStealer malware, which initiates a Discord bot that grants cybercriminals complete access to the victim's computer. The attack is aimed at the developer community, with the intention of stealing sensitive information and compromising the development ecosystem.

Attack Regions


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 Since 2023, attackers have been distributing malicious Python packages under the guise of legitimate obfuscation tools. When these packages are installed, the malicious payload, named "BlazeStealer," is activated. BlazeStealer is fetched from an external source, alongside another malicious script, and it triggers a Discord bot that provides the attackers with complete access to the victim's computer.

#2 Over the course of this entire year, till the past month, attackers have been releasing numerous packages with names like Pyobftoexe, Pyobfusfile, Pyobfexecute, Pyobfpremium, Pyobflite, Pyobfadvance, Pyobfuse, and the most recent, Pyobfgood, which was published in October. These packages disguise ulterior goals under the guise of useful tools, the attackers deliberately chose names similar to those of legitimate packages which programmers use to obfuscate their Python code.

#3 These modules comprise setup.py and init.py files, designed to fetch a Python script. These files are executed immediately upon installation. Utilizing the BlazeStealer malware, a Discord bot is activated enabling threat actors to collect a wide range of data, including passwords from screenshots and web browsers, execute arbitrary commands, encrypt files, and disable Microsoft Defender Antivirus on the compromised host.

#4 The attacker can render the computer inoperable by elevating CPU utilization, introducing a Windows Batch script into the startup directory to initiate system shutdown, and even causing a blue screen of death (BSoD) error. Open-source software is still a great place to innovate, but use caution while working with it. Developers should remain vigilant and thoroughly inspect packages before using them.

Recommendations

Download Packages from Official Websites: Always download software packages from the official website of the vendor or developer. Verify the website's URL to make sure it's the correct and official domain.

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.

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.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0006 Credential Access	TA0009 Collection	TA0010 Exfiltration	TA0040 Impact
T1608 Stage Capabilities	T1608.001 Upload Malware	T1059 Command and Scripting Interpreter	T1059.006 Python
T1140 Deobfuscate/Decode Files or Information	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1123 Audio Capture
T1113 Screen Capture	T1529 System Shutdown/Reboot	T1020 Automated Exfiltration	T1105 Ingress Tool Transfer
T1125 Video Capture	T1204 User Execution	T1562 Impair Defenses	T1562.001 Disable or Modify Tools
T1036 Masquerading	T1056 Input Capture	T1056.001 Keylogging	

Indicators of Compromise (IOCs)

TYPE	VALUE
Packages	Pyobftoexe, Pyobfusfile, Pyobfexecute, Pyobfpremium, Pyobflite, Pyobfadvance, Pyobfuse, Pyobfgood

TYPE	VALUE
URL	hxxps[:]//transfer[.]sh/get/wDK3Q8WOA9/start[.]py hxxps[:]//www[.]nirsoft[.]net/utils/webcamimagesave.zip
Discord Bot	MTE2NTc2MDM5MjY5NDM1NDA2MA.GRSNK7.OHxJIpJoZxopWpF_S3zy5v2g7k2vyiufQ183Lo

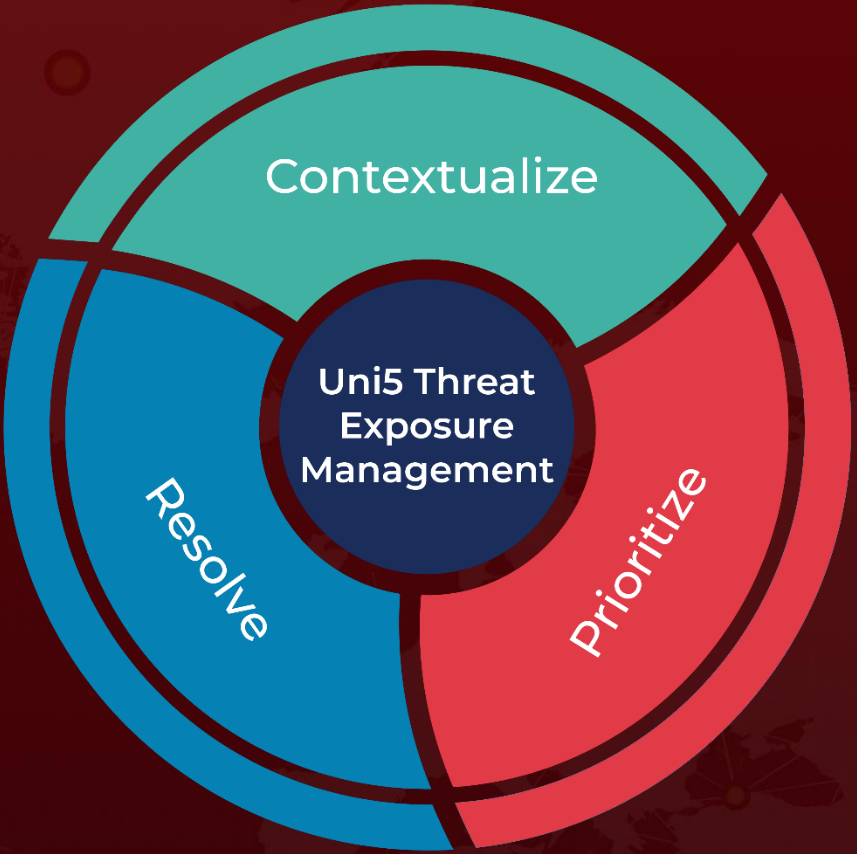
References

https://checkmarx.com/blog/python-obfuscation-traps/?

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 09, 2023 • 5:00 AM

More at www.hivepro.com