Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

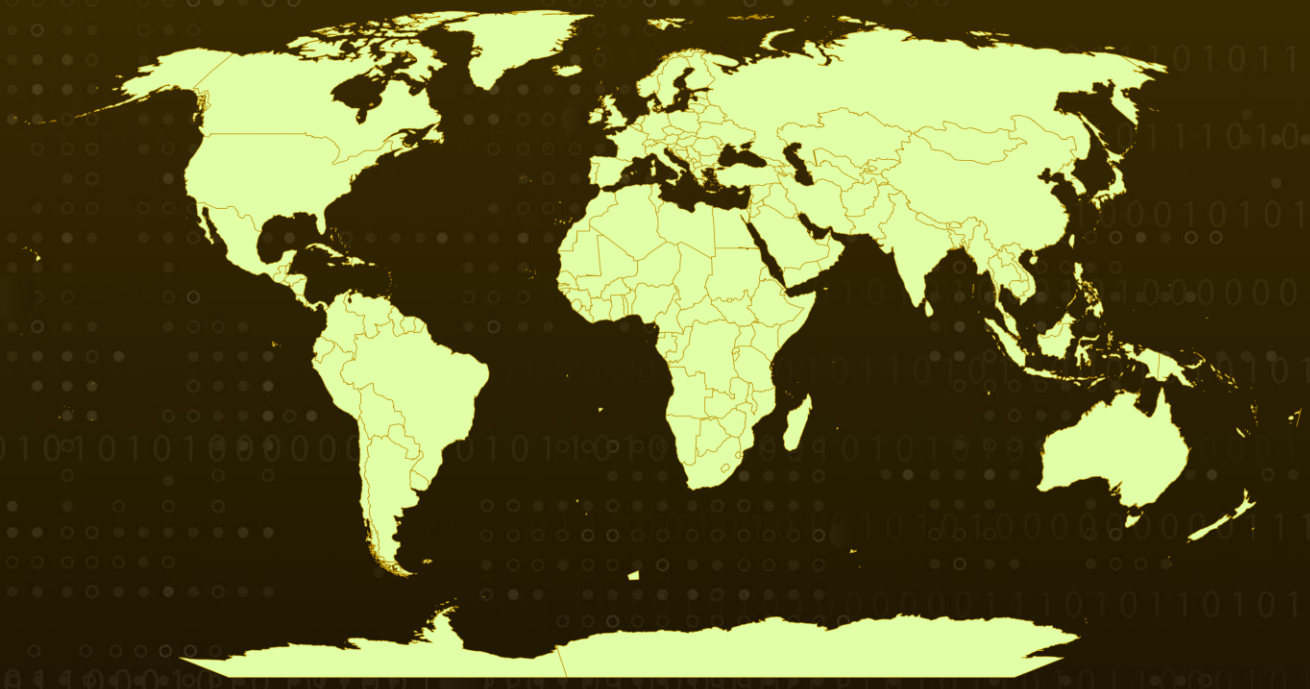
Evil Ant: The Python-Powered Ransomware

Date of Publication	Admiralty Code	TA Number
March 26, 2024	A1	TA2024117

Summary

First Appearance: January 2024
Malware: Evil Ant Ransomware
Attack Region: Worldwide
Attack: Evil Ant Ransomware, a sophisticated Python-based malware compiled with PyInstaller, operates covertly by hiding its console window and executing tasks discreetly. It aims to gain access to critical system functions and encrypt secured files.

Attack Regions



Attack Details

#1 Evil Ant Ransomware is a Python-based malware meticulously crafted and compiled using PyInstaller. This insidious ransomware operates surreptitiously by concealing its console window, executing tasks stealthily in the background via the Windows DLL API.

#2 Leveraging its capability to elevate user privileges to the administrator level, Evil Ant ransomware gains access to critical system functionalities, including altering system configurations and accessing secured files. Moreover, to thwart detection measures, it systematically incapacitates Windows Defender by executing a PowerShell command.

#3 Employing Fernet, a cryptography library in Python, Evil Ant ransomware generates an auto-generated encryption key to encrypt the contents of files residing within the victim's system, systematically encrypting all backup files with a .bak extension.

#4 Beyond its fundamental ransomware functionalities such as file encryption and ransom note display, Evil Ant boasts sophisticated anti-analysis features, refusing to operate within virtual machine environments.

#5 Notably, the ransomware alters the victim's desktop wallpaper, aiming to attract immediate victim attention and instill panic regarding the ransomware's pervasive impact. Upon completion of encryption processes, a distressing blue screen materializes, prompting the victim to remit payment in Bitcoin.

Recommendations

Robust Backup Strategies: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Continuous Monitoring and Analysis: Implement continuous monitoring and analysis of network traffic and system logs. This proactive approach can help identify anomalies and potential threats before they escalate.

Disable Unnecessary Services: Review and disable unnecessary services and features on systems to minimize potential attack vectors. Restrict user privileges to limit the impact of potential breaches.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0040** Impact
TA0010 Exfiltration	**T1059** Command and Scripting Interpreter	**T1574.002** DLL Side-Loading	**T1055** Process Injection
T1010 Application Window Discovery	**T1018** Remote System Discovery	**T1057** Process Discovery	**T1082** System Information Discovery
T1083 File and Directory Discovery	**T1497** Virtualization/Sandbox Evasion	**T1518.001** Security Software Discovery	**T1068** Exploitation for Privilege Escalation
T1041 Exfiltration Over C2 Channel	**T1486** Data Encrypted for Impact	**T1491.001** Internal Defacement	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	ac612b8f09ec1f9d87a16873f27e15f0
SHA1	066b96a82ac998a04897dc1bd25c2e1b6d075182
SHA256	355784fa1c77e09c0de0fcd277bfc9edb3920933f2003d2d1d1b84822f25697b
URL	hxxps[://]api[.]telegram[.]org/bot6893451039:AAGMOfYl9-RF8rfOKQUSizMAqvr28TKmgpY/sendMessage
Email	evilant[.]ransomware[@]gmail[.]com
Bitcoin address	3CLUhZqfXmM8VUHhR3zTgQ8wKY72cSn989

References

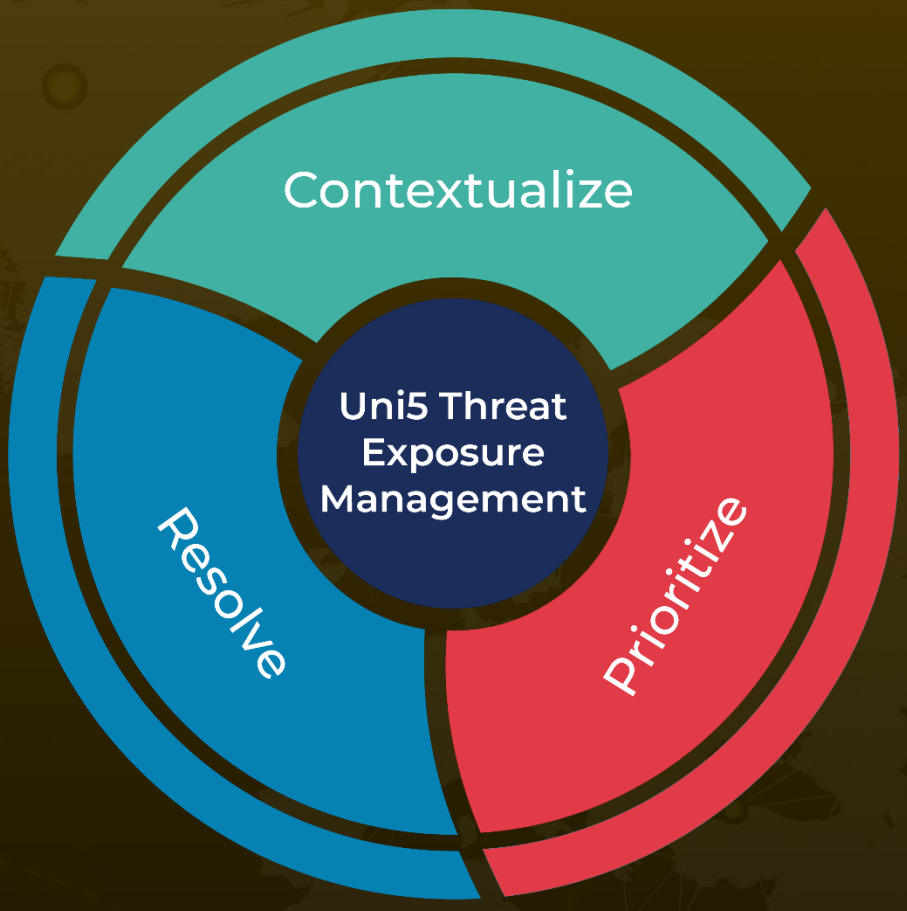
https://labs.k7computing.com/index.php/python-ciphering-delving-into-evil-ants-ransomwares-tactics/

https://www.broadcom.com/support/security-center/protection-bulletin/python-based-evilant-ransomware

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 26, 2024 • 5:15 AM

More at www.hivepro.com