Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Newly Discovered PoweRAT Malware Distributed through PyPI

Date of Publication	Admiralty Code	TA Number
January 12, 2023	A1	TA2023022

Summary

First appeared: December 22, 2022
Attack Region: Worldwide
Attack: New Malware named PoweRAT combines Stealer and RAT Capabilities

Attack Regions

Attack Details

#1

A newly discovered malware called “PoweRAT" combines a stealer and a RAT (remote access tool). The malware is being distributed through the Python Package Index (PyPI), a repository of software for the Python programming language. The malware can steal sensitive information such as login credentials and cryptocurrency wallets, as well as give attackers remote access to the infected computer.

#2

The attack chain is complex and uses novel techniques to hide the malicious code being executed. The malware is present in multiple packages like pyrologin, easytimestamp, discorder, discord-dev, style.py, and pythonstyles which all start in the setup.py file, meaning that anyone who pip installs any of these packages triggers the deployment of malware on their machine. The malware uses a variety of techniques such as exec on encoded strings, PowerShell commands, and the installation of invasive packages to control and monitor mouse and keyboard input and capture screen contents. It also uses a fully-fledged flask app with 17 routes and over 30 helper functions in a hidden window style.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5’s Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the ’Potential MITRE ATT&CK TTPs’ & ‘Indicators of Compromise (IoC)’ on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0008 Lateral Movement	TA0009 Collection	T1113 Screen Capture	T1059 Command and Scripting Interpreter
T1021 Remote Services	T1547 Boot or Logon Autostart Execution	T1560 Archive Collected Data	T1195 Supply Chain Compromise

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	5397800c26dc73bd3dfbd91aa88964244bc8d8dc9cc533fe25f9457d317354f9 5904cf32df705d6e5c9ad730ee425382922e5bd13d1d67212342e374d57f71c3 ede874db1e28252914553871ff9528544894e1785e8b6cd093ebe586c8472997 d0a42a9a0897e762da6b2d3796d03934dc8c2f6d7d2308dc65231497399df145 96a2b383be58f0896d50ca93e23009729f1decfa84b6a837190dd6795227b6c6 eeef39f59c56eca1198a05f272fa27da0ba745657a59c07c13939120513495ba

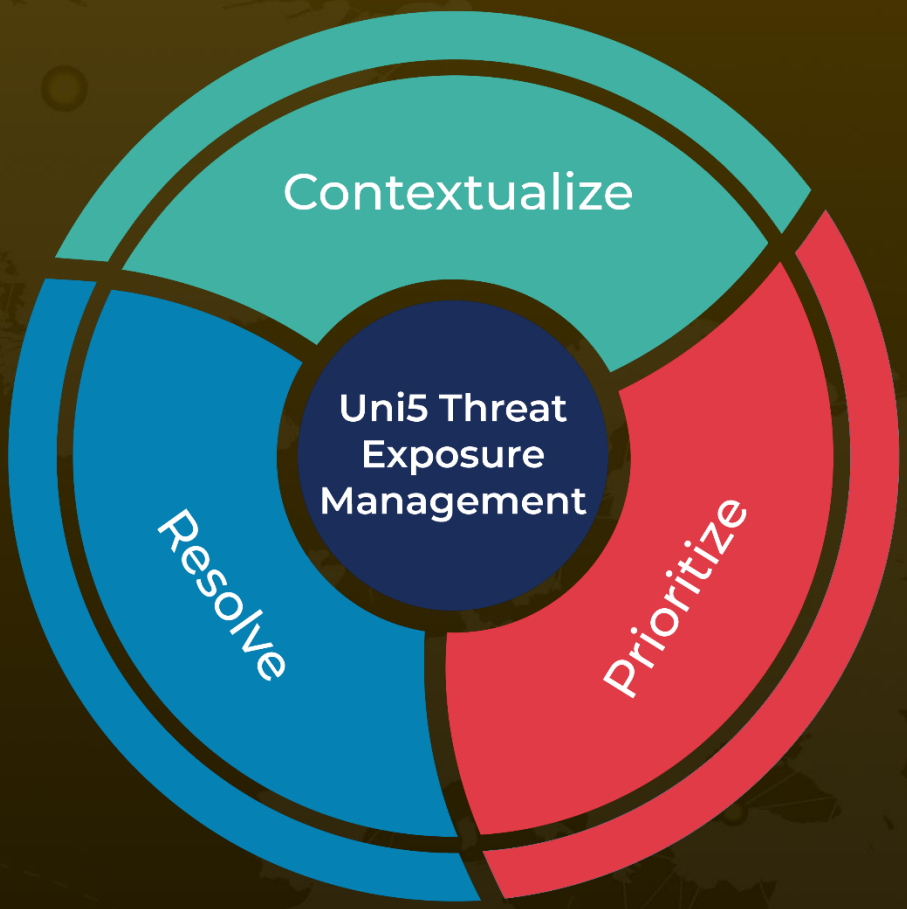
References

https://blog.phylum.io/a-deep-dive-into-powerat-a-newly-discovered-stealer/rat-combo-polluting-pypi

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

January 12, 2023 . 2:15 AM

More at www.hivepro.com