Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

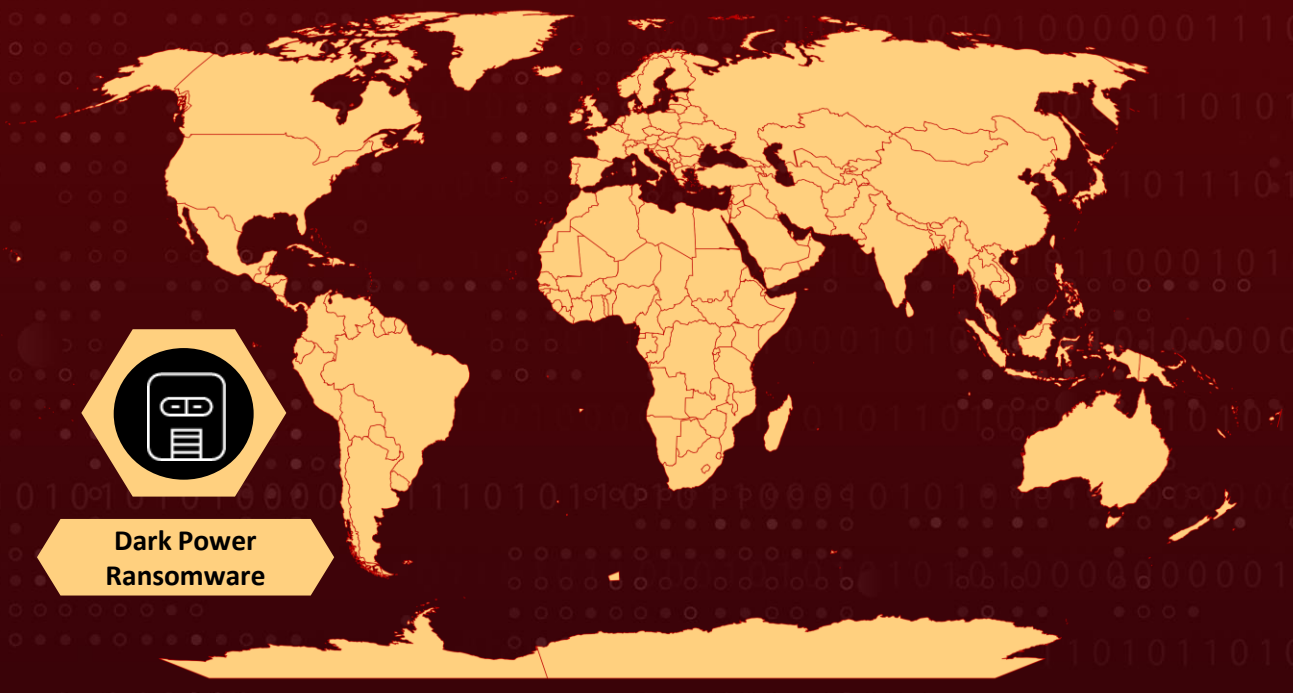
New Dark Power Nim-based Ransomware Targeted Attacks Globally

Date of Publication	Admiralty Code	TA Number
March 27, 2023	A1	TA2023160

Summary

First Appearance: January 29, 2023
Target Countries: Worldwide
Malware: Dark Power ransomware
Target Sector: All industries
Attack: New Dark Power ransomware gang uses Nim programming language to create malware that encrypts specific services and processes, excludes crucial system files, clears logs, and generates a ransom note in every folder.

Attack Regions



Attack Details

#1 The Dark Power ransomware gang is a new group that is using the Nim programming language to create their malware. The ransomware uses the AES CRT encryption algorithm and encrypts strings within the malware, making it harder for defenders to create a generic detection rule.

#2 The ransomware also targets specific services and processes on the victim's machine, including backup and anti-malware services, to increase the chances of the victim paying the demanded ransom. It also excludes certain files and folders that are crucial for the system to remain operational, and clears system logs to hide their tracks.

#3 The ransomware generates a ransom note in every folder it encrypts, and the gang has a victim naming and shaming website where they publish non-paying victims' stolen data. The Dark Power ransomware gang claims to have victims across the globe in countries such as Algeria, the Czech Republic, Egypt, France, Israel, Peru, Turkey, and the USA. The group does not seem to have a specific sector to target.

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	TA0007 Discovery	TA0010 Exfiltration
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
T1047 Windows Management Instrumentation	T1070 Indicator Removal	T1070.001 Clear Windows Event Logs	T1027 Obfuscated Files or Information
T1082 System Information Discovery	T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery	T1489 Service Stop
T1623 Command and Scripting Interpreter	T1057 Process Discovery	T1140 Deobfuscate/Decode Files or Information	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	33c5b4c9a6c24729bb10165e34ae1cd2315cfce5763e65167bd58a57fde9a389 11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394
SHA1	9bddcce91756469051f2385ef36ba8171d99686d
MD5	df134a54ae5dca7963e49d97dd104660

References

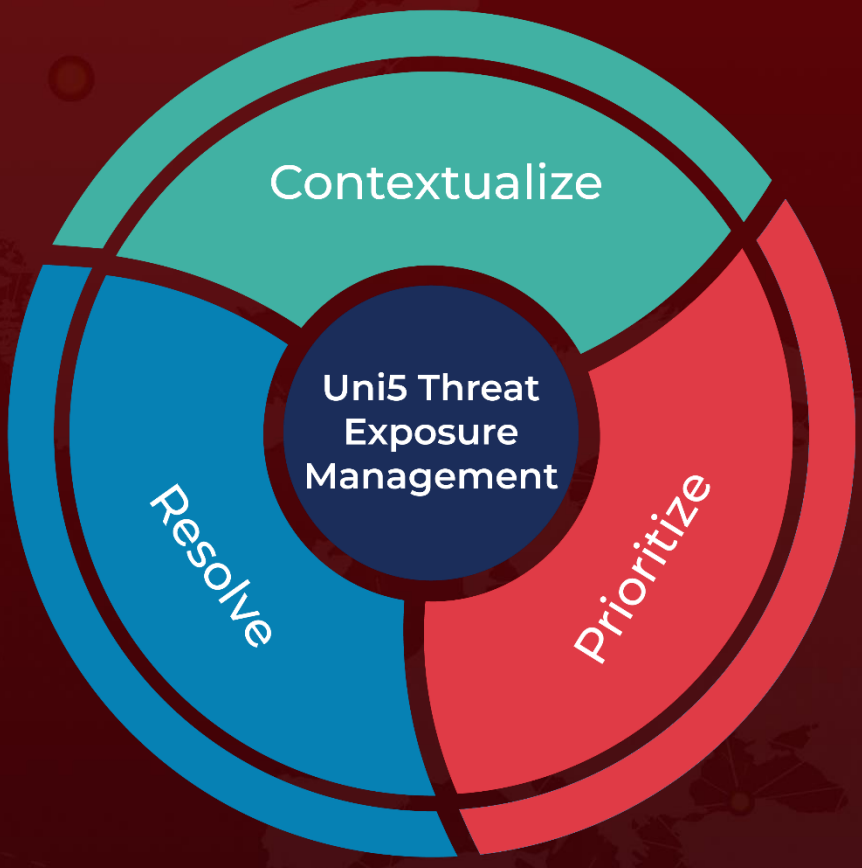
https://www.trellix.com/en-us/about/newsroom/stories/research/shining-light-on-dark-power.html

https://twitter.com/DailyDarkWeb/status/1633821362178658306

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 27, 2023 • 12:30 AM

More at www.hivepro.com