Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Israel's Technion Targeted by DarkBit Ransomware's Campaign

Date of Publication	Admiralty Code	TA Number
February 17, 2023	A1	TA2023088

Summary

First appeared: February 12, 2023
Attack Region: Israel
Attack: The DarkBit ransomware is a newly emerged threat in the cybersecurity scene that has targeted Technion - Israel Institute of Technology, a prestigious academic institution in Israel. The attackers behind this assault are opposed to prejudice, fascism, and apartheid and have adopted the hashtag "#HackForGood" to promote their cause. The hackers demanded a ransom of 80 Bitcoin (BTC), which is valued at approximately USD $1,869,760.

Attack Regions

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

Attack Details

#1

A new ransomware variant called DarkBit has surfaced. It targets Windows operating systems and is written in Go binary. The creators of this ransomware appear to have geopolitical motivations. The primary portable executable (PE) module supports command-line options and is optimized for encrypting large files. Technion - Israel Institute of Technology (IIT) fell victim to a DarkBit ransomware attack.

#2

After being executed, the malware creates a Global mutex to guarantee that only one instance of the malware operates at a time. It then employs the CreateProcessW() API to execute vssadmin.exe and remove shadow copies on the victim's device. The ransomware encrypts different files throughout the attack, utilizing multithreading and Advanced Encryption Standard 256-bits (AES-256), and adds the ".Darkbit" file extension to denote encryption. Additionally, the ransomware adds a ransom note named 'RECOVERY_DARKBIT.txt' to all impacted directories.

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

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	TA0040 Impact	T1204 User Execution
T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery	T1082 System Information Discovery	T1083 File and Directory Discovery
T1189 Drive-by Compromise	T1090 Proxy	T1003 OS Credential Dumping	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1055 Process Injection	T1036 Masquerading	T1005 Data from Local System

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff
SHA1	30466ccd4ec7bcafb370510855da2cd631f74b7a
MD5	9880fae6551d1e9ee921f39751a6f3c0
URL	hxxp[:]//iw6v2p3cruy7tqfup3yl4dgt4pfibfa3ai4zgnu5df2q3hus3lm7c7ad[.]onion/support

Recent Breaches

https://www.technion.ac.il/land-page/

References

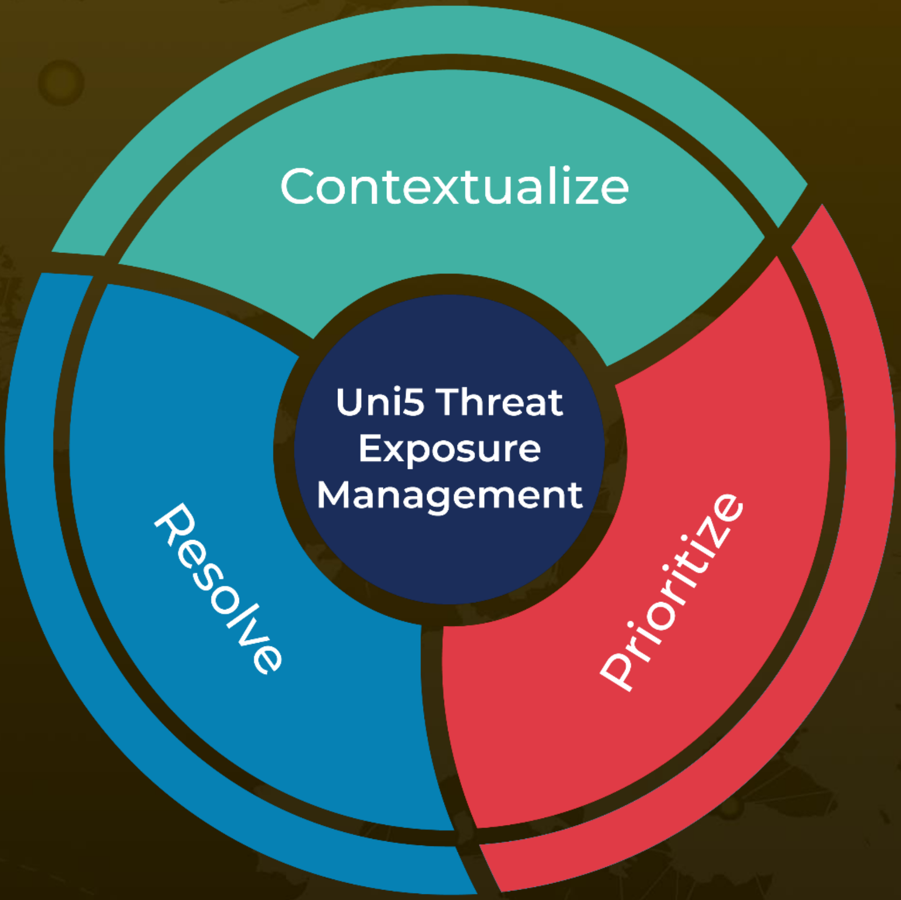
https://blogs.blackberry.com/en/2023/02/darkbit-ransomware-targets-israel

https://blog.cyble.com/2023/02/15/uncovering-the-dark-side-of-darkbit-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

February 17, 2023 • 1:11 AM

More at www.hivepro.com