Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

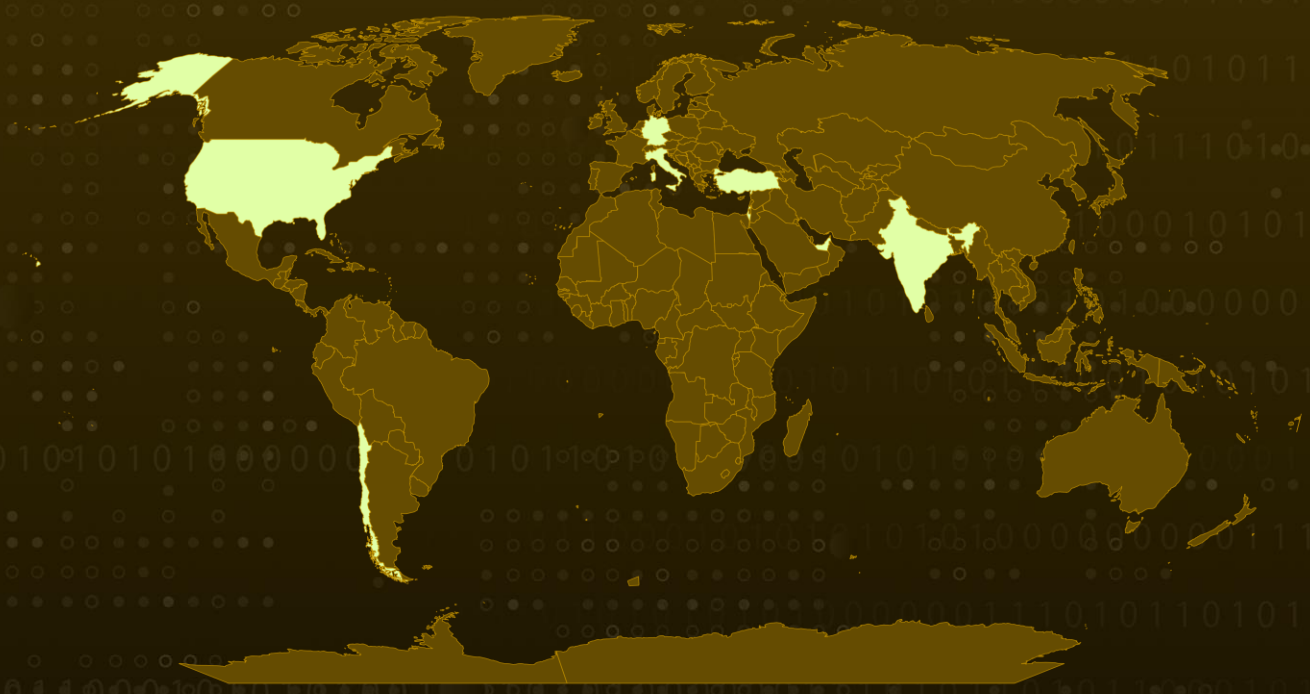
BlackMagic Ransomware disrupts the Israeli logistics sector

Date of Publication	Admiralty Code	TA Number
December 8, 2022	A1	TA2022287

Summary

First appearance: December 2022
Attack Region: Chile, Germany, India, Israel, Italy, Turkey, UAE, USA.
Targeted Industries: Logistics, Transportation.
Attack: Selling the exfiltrated victims' data equates to around 50 GB of data from Israeli transportation businesses.

Attack Regions



Attack Details

#1 The latest ransomware entity, known as "BlackMagic" has emerged. This gang targets its victims using a double extortion approach in which it initially exfiltrates the victim's data, followed by encryption, and has primarily targeted several firms in Israel's transportation and logistics niche.

#2 The ransomware payload comprises two files: "MicrosoftUpdate.dll" and "back.bmp." The ransomware DLL file is then loaded and operated, either manually or with the help of additional malware. This DLL file only exports one function called "Black," which is in charge of carrying out the processes of the BlackMagic ransomware.

#3 To evade detection via sandboxes, the malware repeatedly invokes the Sleep() method, terminates processes, and disables the task manager. After encrypting the victim's files, it renames them with the suffix ".BlackMagic." Drops a ransom note called "HackedByBlackMagic.txt" that consists of links to social media handles used to expose the victim's data rather than any crypto address for ransom payments.

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	TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control
TA0040 Impact	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1218 System Binary Proxy Execution
T1218.011 Rundll32	T1016 System Network Configuration Discovery	T1071 Application Layer Protocol	T1486 Data Encrypted for Impact
T1489 Service Stop	T1529 System Shutdown/Reboot	T1491 Defacement	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	bf647a66de004ae56ece7f18a8dfa0ed 7b1fd05e9db5369c5b7ef82080fd0ca8
SHA1	aeadbc1254da9c1ec70ddf18cd8b5cda78d8daf6 aea92bb857367e29183fe5c335a4c0cbda44eabf
SHA256	af80b807c797d4d5e8141f7d43f08e91181fb94029c84fd41786a883d09dc902 8f855ed4c2f17487bac5d5079437acd728ccd68d93b49ab2f5b6d6d2430da133
IP Address	5[.]230.70[.]49

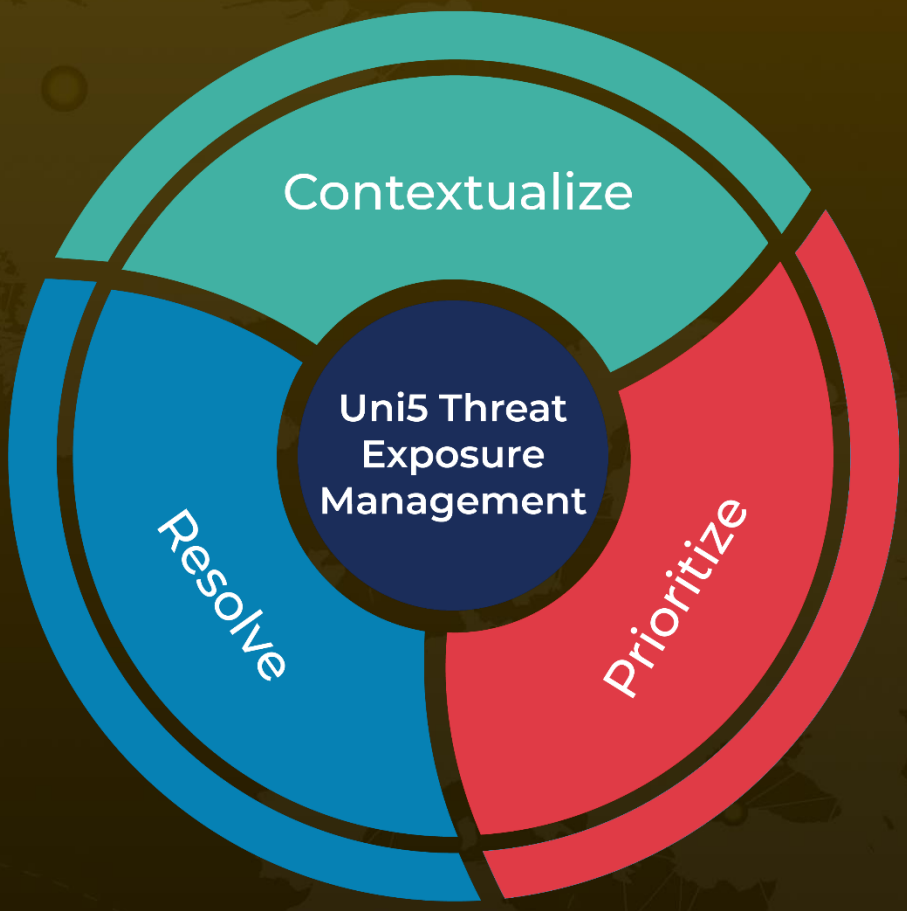
References

https://blog.cyble.com/2022/12/07/a-closer-look-at-blackmagic-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

December 8, 2022 . 12:49 AM

More at www.hivepro.com