Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

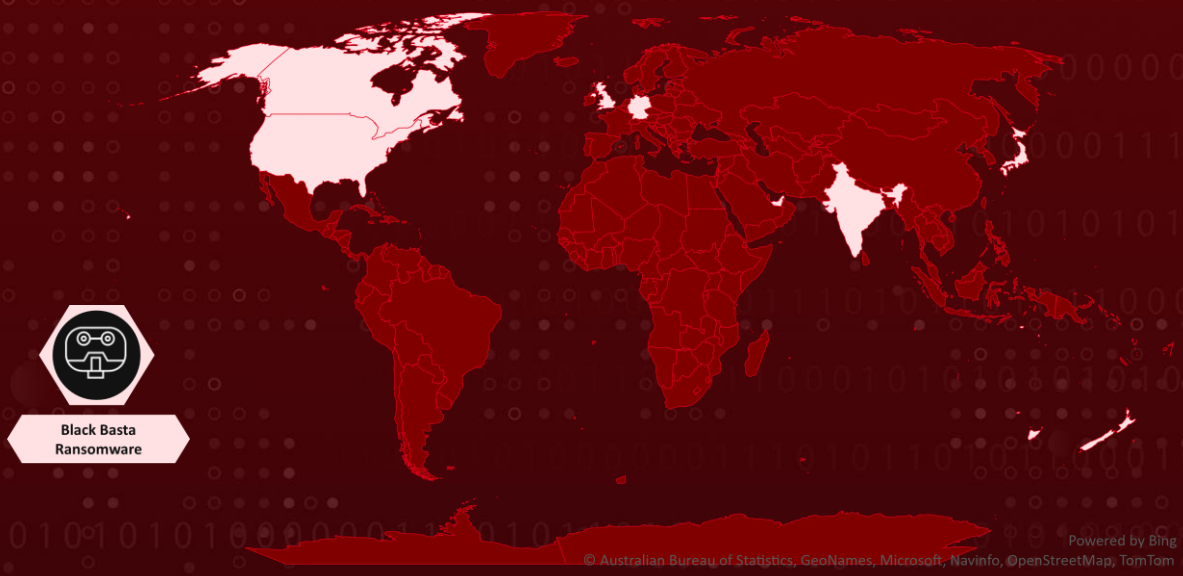
Black Basta Ransomware Invades US Firms with Qakbot Malware

Date of Publication	Admiralty Code	TA Number
November 24, 2022	A1	TA2022271

Summary

First seen: April 2022
Attack Region: Australia, Canada, Germany, India, Japan, New Zealand, Singapore, UAE, UK, USA
Targeted Industry: Automotive, Construction, Cosmetics, Energy, Healthcare, Heating, Manufacturing, Pharmaceuticals, Plumbing, Telecommunication, Transportation, Textile
Threat Actor: Black Basta Ransomware gang
Attack: Encrypts classified files and inhabits system recovery

Attack Regions



Attack Details

#1 In this latest spear-phishing campaign, the Black Basta ransomware gang employed QakBot malware, aka QBot or Pinkslipbot, to acquire an initial point of entry and migrate laterally through an organization's network to steal financial data from victims.

#2 The attack scenario starts with a QakBot infection and results in multiple machines loading Cobalt Strike leading to the deployment of Black Basta ransomware. To make recovery even more difficult, the threat actor disables DNS services, thereby locking the victim out of the network.

#3 The adversary moved laterally on multiple devices using Windows Management Instrumentation (WMI) to execute malicious instructions and harvest credentials before penetrating as many endpoints as possible using the obtained passwords. Black Basta encrypts the files and appends a random extension to each file, later the ransom letter named “readme.txt” will be dropped into the victim's system.

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
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	TA0040 Impact
T1566 Phishing	T1566.001 Spearphishing Attachment	T1204 User Execution	T1569 System Services
T1059 Command and Scripting Interpreter	T1547 Boot or Logon Autostart Execution	T1055 Process Injection	T1027 Obfuscated Files or Information
T1218 System Binary Proxy Execution	T1140 Deobfuscate/Decode Files or Information	T1562 Impair Defenses	T1010 Application Window Discovery
T1482 Domain Trust Discovery	T1135 Network Share Discovery	T1057 Process Discovery	T1018 Remote System Discovery
T1082 System Information Discovery	T1071 Application Layer Protocol	T1573 Encrypted Channel	T1486 Data Encrypted for Impact
T1489 Service Stop	T1490 Inhibit System Recovery	T1491 Defacement	

Indicator of Compromise (IOC)

TYPE	VALUE
Domains	jesofidiwi[.]com dimingol[.]com tevokaxol[.]com vopaxafi[.]com
IP Addresses	108.177.235[.]29 144.202.42[.]216 108.62.118[.]197
SHA1	75b2593da627472b1c990f244e24d4e971c939e7 3a852c006085d0ce8a18063e17f525e950bb914c 4202bf2408750589e36750d077746266176ac239

Recent Breaches

https://www.itmanage.co.jp/

https://imacorp.com/

https://metro.co.uk/

https://www.wilken.de/

https://www.property-tax.com/

https://www.cadeploy.com/

References

https://www.cybereason.com/blog/threat-alert-aggressive-qakbot-campaign-and-the-black-basta-ransomware-group-targeting-u.s.-companies

https://thehackernews.com/2022/11/black-basta-ransomware-gang-actively.html

https://www.trendmicro.com/en_us/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html

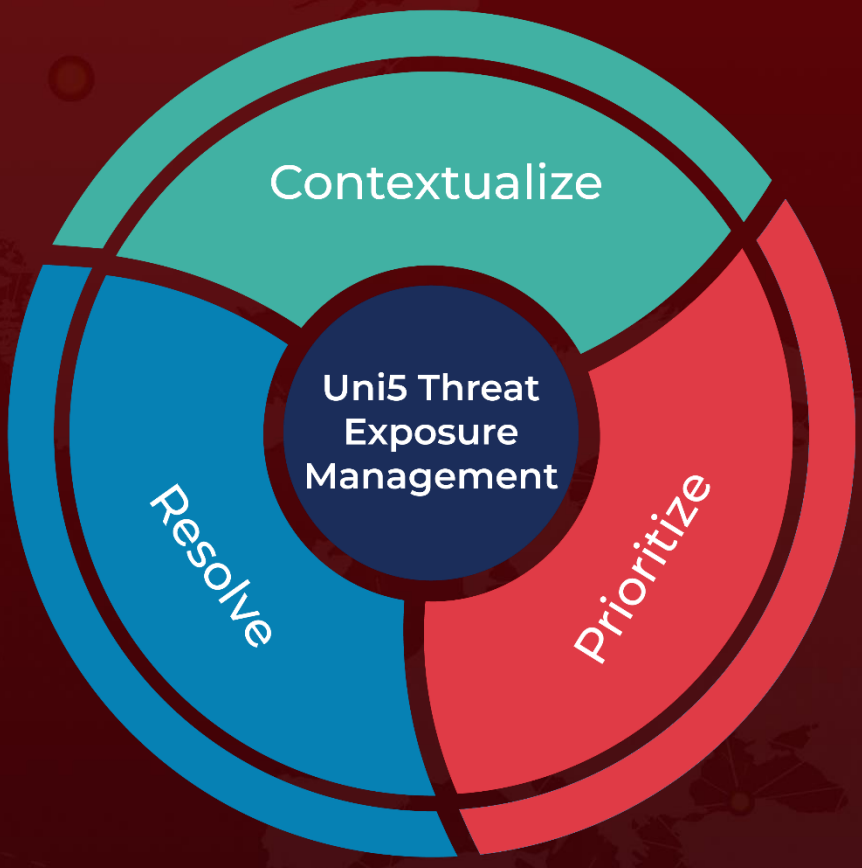
https://attack.mitre.org/software/S0650/

https://www.hivepro.com/50-firms-attacked-by-black-basta-ransomware-group/

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 24, 2022 . 3:14 AM

More at www.hivepro.com