Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

Ransomware Black Basta uses tools related to FIN7

Date of Publication	Admiralty Code	TA Number
November 4, 2022	A1	TA2022246

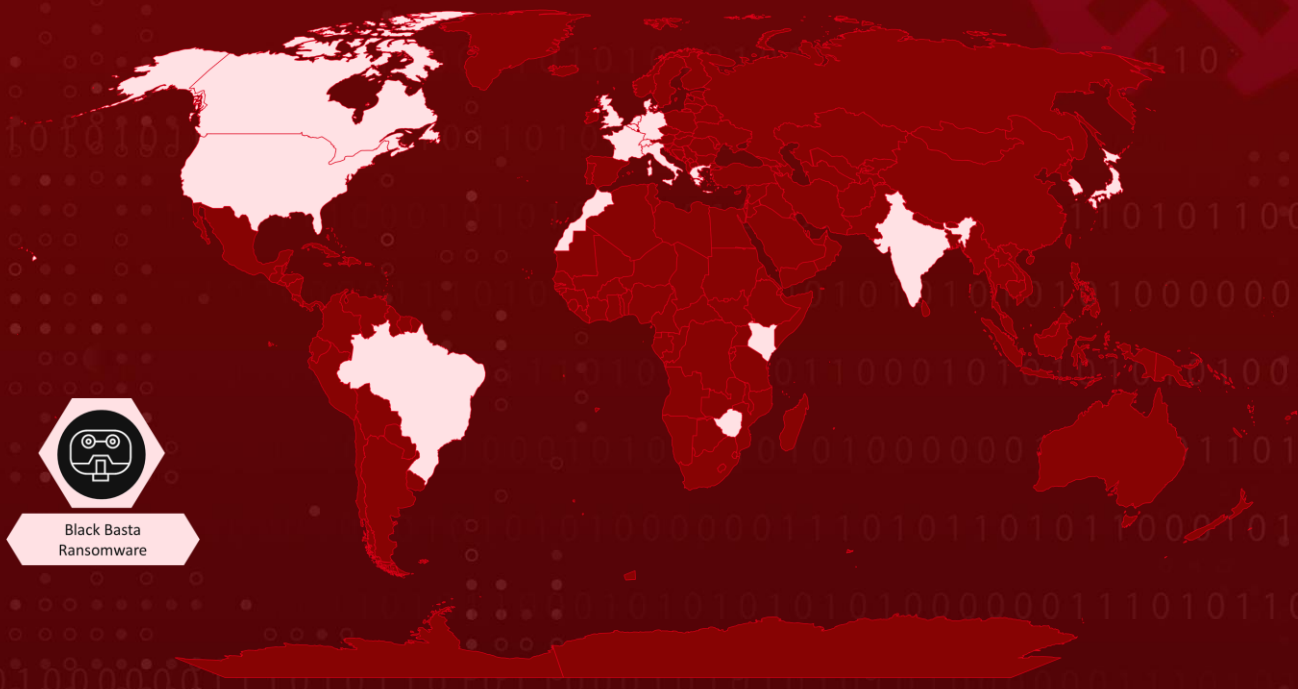
Summary

Black Basta is deploying a ransomware payload by exploiting Microsoft flaws and using an Endpoint Detection and Response(EDR) defense evasion tool created by FIN7. Black Basta is a relatively new ransomware group that emerged in April 2022 and has infected more than 120 victims to date.

CVEs

CVE	NAME	PATCH
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (Follina)	✓
CVE-2021-42287	Active Directory Domain Services Elevation of Privilege Vulnerability (NoPac)	✓
CVE-2021-42278	Active Directory Domain Services Elevation of Privilege Vulnerability (NoPac)	✓
CVE-2021-34527	Windows Print Spooler Remote Code Execution Vulnerability (PrintNightmare)	✓
CVE-2020-1472	Netlogon Elevation of Privilege Vulnerability (ZeroLogon)	✓

Actor Map



Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**TA0040** Impact	**T1059** Command and Scripting Interpreter	**T1059.005** Visual Basic Script
T1059.007 JavaScript	**T1027** Obfuscated Files or Information	**T1027.005** Indicator Removal from Tools	**T1027.006** HTML Smuggling
T1027.002 Software Packing	**T1569** System Services	**T1070** Indicator Removal on Host	**T1070.004** File Deletion
T1482 Domain Trust Discovery	**T1135** Network Share Discovery	**T1069** Permission Groups Discovery	**T1069.001** Local Groups
T1016 System Network Configuration Discovery	**T1049** System Network Connections Discovery	**T1033** System Owner/User Discovery	**T1010** Application Window Discovery

T1082 System Information Discovery	**T1005** Data from Local System	**T1071** Application Layer Protocol	**T1041** Exfiltration Over C2 Channel
T1102 Web Service	**T1090** Proxy	**T1505** Server Software Component	**T1566** Phishing
T1566.001 Spearphishing Attachment	**T1566.002** Spearphishing Link	**T1204** User Execution	**T1204.001** Malicious Link
T1204.002 Malicious File	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1053** Scheduled Task/Job
T1053.005 Scheduled Task	**T1543** Create or Modify System Process	**T1543.003** Windows Service	**T1574** Hijack Execution Flow
T1574.001 DLL Search Order Hijacking	**T1490** Inhibit System Recovery	**T1218** Signed Binary Proxy Execution	**T1218.010** Regsvr32
T1218.011 Rundll32	**T1112** Modify Registry	**T1055** Process Injection	**T1055.012** Process Hollowing
T1562 Impair Defenses	**T1562.009** Safe Boot Mode	**T1622** Debugger Evasion	**T1555** Credentials from Password Stores
T1555.003 Credentials from Web Browsers	**T1003** OS Credential Dumping	**T1057** Process Discovery	**T1018** Remote System Discovery
T1573 Encrypted Channel	**T1486** Data Encrypted for Impact		

Technical Details

#1 Black Basta infection begins when the attacker sends Qakbot by email and macro-based MS Office documents exploiting Follina (CVE-2022-30190).

#2 Then it tries a variety of exploits to gain privilege escalation at the local and domain levels. ZeroLogon (CVE-2020-1472), NoPac (CVE-2021-42287, CVE-2021-42278), and PrintNightmare (CVE-2021-34527) are some of the exploits they have been using.

#3 The threat actor then uses a custom Remote Access Trojan as well as scripts to kill services and processes to maximize the ransomware impact, delete the shadow copies and kill certain security solutions.

#4 Black Basta group then used malware such as DICELOADER, CARBANAK, Cobalt Strike, POWERTRASH, and BIRDDOG to invade detection.

Indicator of Compromise (IOC)

TYPE	VALUE
IPV4	185[.]217.1.23 159[.]223.236.110 193[.]29.13.159 193[.]29.13.216 193[.]29.13.170 190[.]123.44.126 190[.]123.44.130 185[.]125.206.218 95[.]179.161.101 69[.]46.15.147 87[.]247.152.249 185[.]107.80.78 177[.]54.145.139 109[.]248.149.137 109[.]170.6.150 78[.]128.112.217 45[.]153.241.167 78[.]128.112.217 209[.]250.236.75

TYPE	VALUE
SHA1	0b06b000f0dd8d89e7300fa333cba33f90aa8e62 31c0be28f46b86670c3d08d3c4f6ee8793cabbbe 48bf9b838ecb90b8389a0c50b301acc32b44b53e 5ebacb20f62fae0dd610d874583d13fac5024309 f48b84a91e90ad96f652e777c05e41157eb0c666 2b93cc96825ec27525b9caa918073387eea13538 fd6277f31d7a40d8ece67130f6b0dd69bb58db82 5ed592a6713d36c26139b7d386c97a251b9f2ccb 885e07e95661282000d843bfd87295718d08ee05 2c25eefd5a8c1df0346deefb705f80c3c4775e8f 84a594fc02731009fdf444a3e4134b1b7a928626 fbb59ffa0f882cc2971d72b8556bfe3b9cce060c 3b2a0d2cb8993764a042e8e6a89cbbf8a29d47d1 1860e9423d55720a44e7814e757b10d880e1d9af 93cf40f95ab91a0e33b405c0c49025dab7ceb496 a0c3ba7679a36976bbbbad6c08758054ba49af8b 0b879c224e3ae5be0b6d3fcca28e27bd26ed7114 20486b47aa29334b368fe80bd815181aa59d5db4 877da581a05917591cfa905d2a3981f03c1389fc 3112a39aad950045d6422fb2abe98bed05931e6c d76188d82e1c09c7703e30ab9b64a0c42f68a67b
Domain	courtlincolnglave.com jardinoks.com widisusez.com purestealconstruction.com groundworkseasy.com
Command Line	c:\windows\sysnative\nltest.exe /domain_trusts /all_trusts wmic /namespace:\\root\SecurityCenter2 PATHAntiVirusProduct GET /value wmic /namespace:\\root\SecurityCenter2 PATHAntiSpywareProduct GET /value wmic /namespace:\\root\SecurityCenter2 PATHFirewallProduct GET /value
regkey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run/NSM HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run/MSN HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SentinelHealth HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\PandaHealth

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42287

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42278

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472

Recent Breaches

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

https://www.cadeploy.com/

https://diamondmowers.com/

https://edc3global.com/

http://www.alrotransport.com/

https://www.jmrodgers.com/

https://www.bootz.be/nl/Home.aspx

References

https://assets.sentinelone.com/sentinellabs22/sentinellabs-blackbasta

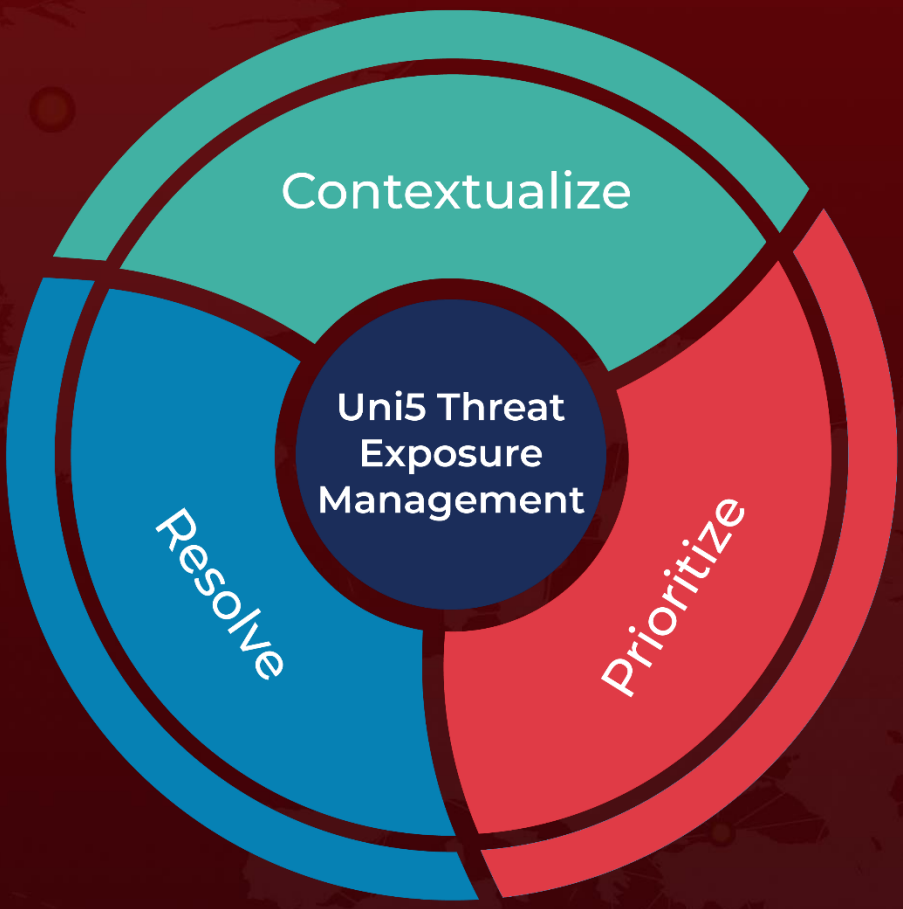
https://otx.alienvault.com/pulse/6363be4e63994f523414639c/

https://www.cynet.com/blog/orion-threat-alert-qakbot-ttps-arsenal-and-the-black-basta-ransomware/

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 4, 2022 • 6:00 AM

More at www.hivepro.com