Hive Pro

Threat Level

Red

CISA: AA24-131A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

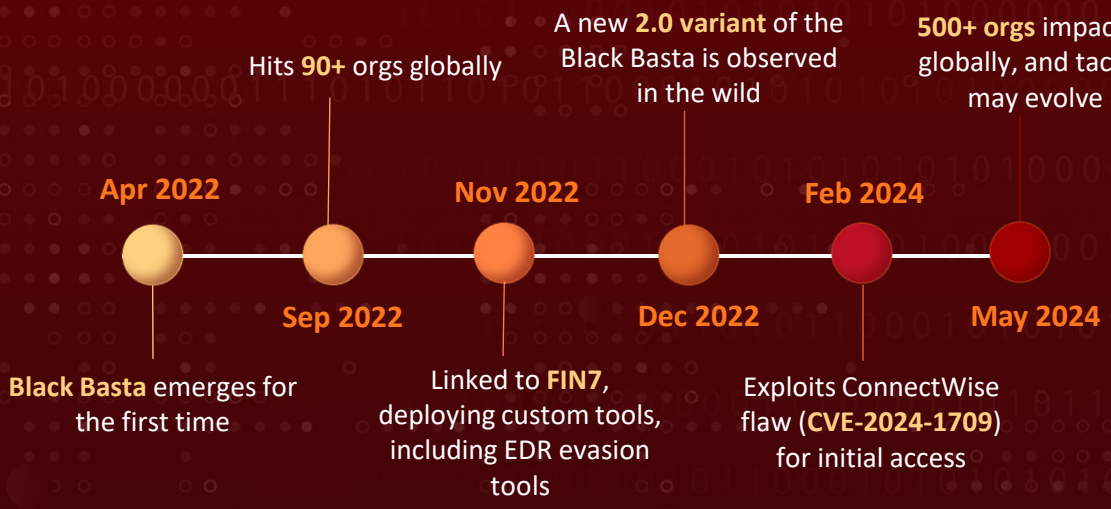
Black Basta Ransomware Impacts Over 500 Organizations Worldwide

Date of Publication	Admiralty Code	TA Number
May 14, 2024	A1	TA2024185

Summary

First Appearance: April 2022
Malware: Black Basta Rasnomware, Qakbot
Targeted Countries: Worldwide
Targeted Industries: Critical infrastructure sectors, including Healthcare
Affected Platforms: Windows, Linux, macOS, and Vmware ESXi
Attack: Black Basta ransomware, a highly impactful Ransomware-as-a-Service (RaaS) variant, targets critical sectors globally, affecting over 500 organizations. They use phishing, exploits, and Qakbot to gain access, steal data, encrypt systems, and threaten public data leaks if a ransom isn't paid.

Attack Timeline



Attack Regions

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect	✗	✓	✓
CVE-2020-1472	ZeroLogon (Microsoft Netlogon Privilege Escalation Vulnerability)	Microsoft Netlogon	✗	✓	✓
CVE-2021-42278	NoPac (Microsoft Active Directory Domain Services Privilege Escalation Vulnerability)	Microsoft Active Directory Domain Services	✗	✓	✓
CVE-2021-42287	NoPac (Microsoft Active Directory Domain Services Privilege Escalation Vulnerability)	Microsoft Active Directory Domain Services	✗	✓	✓
CVE-2021-34527	PrintNightmare (Windows Print Spooler Remote Code Execution Vulnerability)	Windows Print Spooler	✓	✓	✓
CVE-2022-30190	Follina (Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability)	Microsoft Windows Support Diagnostic Tool (MSDT)	✓	✓	✓

Attack Details

#1

Black Basta is a sophisticated ransomware strain that first appeared in April 2022. They target various organizations, including critical infrastructure like healthcare providers, and have impacted over 500 organizations worldwide as of May 2024. It appears to have strong affiliations with current and former members from groups such as Conti, FIN7, and/or BlackMatter. Operating as a Ransomware as a Service (RaaS), Black Basta maintains a dark website and provides affiliates with a specific control panel for configuration and generating custom binaries.

#2 Black Basta primarily impacted a wide range of businesses and critical infrastructure in North America, Europe, and Australia. It is a cross-platform ransomware that is compatible with Windows and Linux VMware ESXi systems. Written in the C++ programming language and uses common tactics to gain access to systems, such as phishing emails, exploiting software vulnerabilities like ConnectWise (CVE-2024-1709), and then spreads through the banking Trojan Qakbot.

#3 Black Basta then employs a double extortion scheme. They demand a ransom payment to decrypt the stolen data threatening to publicly leak it if the ransom is not paid. Their tactics involve privilege escalation through tools like Mimikatz and the exploitation of vulnerabilities like ZeroLogon and PrintNightmare. Data exfiltration is facilitated by RClone, with encryption using ChaCha20 and RSA-4096.

#4 The exfiltrated data is sent to a cloud service, after which the ransomware encrypts files with the ".basta" extension. The group even attempts to disable security software, complicating victims' system recovery efforts. Healthcare organizations are particularly targeted due to their size and access to sensitive information

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with Black Basta ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. Black Basta affiliates often exploit known vulnerabilities to gain initial access to systems. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.

Conduct Regular Data Backups and Test Restoration: Implement a robust data backup strategy that includes regular backups of critical data and systems. Ensure backups are stored offline or in a secure, isolated environment to prevent them from being compromised in the event of an attack. Regularly test the restoration process to verify the integrity and availability of backups. In the event of a Black Basta ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0003 Persistence	TA0004 Privilege Escalation	TA0002 Execution
TA0042 Resource Development	TA0008 Lateral Movement	TA0011 Command and Control	TA0043 Reconnaissance
TA0010 Exfiltration	TA0040 Impact	TA0007 Discovery	T1588 Obtain Capabilities
T1566 Phishing	T1190 Exploit Public-Facing Application	T1078 Valid Accounts	T1036 Masquerading
T1562.001 Disable or Modify Tools	T1562 Impair Defenses	T1490 Inhibit System Recovery	T1486 Data Encrypted for Impact
T1573.002 Asymmetric Cryptography	T1573 Encrypted Channel	T1059 Command and Scripting Interpreter	T1588.005 Exploits
T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation	T1567.002 Exfiltration to Cloud Storage	T1567 Exfiltration Over Web Service
T1021.001 Remote Desktop Protocol	T1021 Remote Services	T1059.003 Windows Command Shell	T1027 Obfuscated Files or Information

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298, d3683beca3a40574e5fd68d30451137e4a8bbaca8c428ebb781d565d6a70385e, 88c8b472108e0d79d16a1634499c1b45048a10a38ee799054414613cc9dccccc,

TYPE	VALUE
SHA256	4bdda7dd3bbe1f9cb0a7d42f6947ba0f6442e52758bd2638541f9409b573d5c9, 58ddbea084ce18cfb3439219ebcf2fc5c1605d2f6271610b1c7af77b8d0484bd, 39939eacfbc20a2607064994497e3e886c90cd97b25926478434f46c95bd8ead, 5b2178c7a0fd69ab00cef041f446e04098bbb397946eda3f6755f9d94d53c221, 51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e, d15bfbc181aac8ce9faa05c2063ef4695c09b718596f43edc81ca02ef03110d1, 5942143614d8ed34567ea472c2b819777edd25c00b3e1b13b1ae98d7f9e28d43, 05ebae760340fe44362ab7c8f70b2d89d6c9ba9b9ee8a9f747b2f19d326c3431, a7b36482ba5bca7a143a795074c432ed627d6afa5bc64de97fa660faa852f1a6, 86a4dd6be867846b251460d2a0874e6413589878d27f2c4482b54cec134cc737, 07117c02a09410f47a326b52c7f17407e63ba5e6ff97277446efc75b862d2799, 96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be, 1c1b2d7f790750d60a14bd661dae5c5565f00c6ca7d03d062adcecda807e1779, 360c9c8f0a62010d455f35588ef27817ad35c715a5f291e43449ce6cb1986b98, 0554eb2ffa3582b000d558b6950ec60e876f1259c41acff2eac47ab78a53e94a, 9a55f55886285eef7ffabdd55c0232d1458175b1d868c03d3e304ce7d98980bc, 62e63388953bb30669b403867a3ac2c8130332cf78133f7fd4a7f23cdc939087, 7ad4324ea241782ea859af12094f89f9a182236542627e95b6416c8fb9757c59, 350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd, 90ba27750a04d1308115fa6a90f36503398a8f528c974c5adc07ae8a6cd630e7, fafaff3d665b26b5c057e64b4238980589deb0dff0501497ac50be1bc91b3e08, acb60f0dd19a9a26aaaefd3326db8c28f546b6b0182ed2dcc23170bcb0af6d8f, d73f6e240766ddd6c3c16eff8db50794ab8ab95c6a616d4ab2bc96780f13464d, f039eaaced72618eaba699d2985f9e10d252ac5fe85d609c217b45bc8c3614f4, 723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224,

TYPE	VALUE
SHA256	ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e, fff35c2da67eef6f1a10c585b427ac32e7f06f4e4460542207abcd62264e435f, df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415, 462bbb8fd7be98129aa73efa91e2d88fa9cafc7b47431b8227d1957f5d0c8ba7, 3c50f6369f0938f42d47db29a1f398e754acb2a8d96fd4b366246ac2ccbe250a, 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa, 37a5cd265f7f555f2fe320a68d70553b7aa9601981212921d1ac2c114e662004, 3090a37e591554d7406107df87b3dc21bda059df0bc66244e8abef6a5678af35, 17879ed48c2a2e324d4f5175112f51b75f4a8ab100b8833c82e6ddb7cd817f20, 42f05f5d4a2617b7ae0bc601dd6c053bf974f9a337a8fcc51f9338b108811b78, 882019d1024778e13841db975d5e60aaae1482fcf86ba669e819a68ce980d7d3, e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757, 0a8297b274aeab986d6336b395b39b3af1bb00464cf5735d1ecdb506fef9098e, 69192821f8ce4561cf9c9cb494a133584179116cb2e7409bea3e18901a1ca944, 3337a7a9ccdd06acdd6e3cf4af40d871172d0a0e96fc48787b574ac93689622a, 17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90, b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9, b6a4f4097367d9c124f51154d8750ea036a812d5badde0baf9c5f183bb53dd24, f21240e0bf9f0a391d514e34d4fa24ecb997d939379d2260ebce7c693e55f061, 8501e14ee6ee142122746333b936c9ab0fc541328f37b5612b6804e6cdc2c2c6, 034b5fe047920b2ae9493451623633b14a85176f5eea0c7aadc110ea1730ee79, 8C68B2A794BA3D148CAE91BDF9C8D357289752A94118B5558418A36D95A5A45F, 3c65da7f7bfdaf9acc6445abbedd9c4e927d37bb9e3629f34afc3380586804407, 808c96cb90b7de7792a827c6946ff48123802959635a23bf9d98478ae6a259f9,

TYPE	VALUE
SHA256	3a8fc07cadc08eeb8be342452636a754158403c3d4ebff379a4ae66f8298d9a6, 4ac69411ed124da06ad66ee8bfbcea2f593b5b199a2c38496e1ee24f9d04f34a, 819cb9bcf62be7666db5666a693524070b0df589c58309b067191b30480b0c3a, c26a5cb62a78c467cc6b6867c7093fbb7b1a96d92121d4d6c3f0557ef9c881e0, d503090431fdd99c9df3451d9b73c5737c79eda6eb80c148b8dc71e846233401f
MD5	4c897334e6391e7a2fa3cbcbf773d5a4, 2642ec377c0cee3235571832cb472870, b3fe23dd4701ed00d79c03043b0b952e
Filenames	C:\Users\Public\Audio\Jun.exe, C:\Users\Public\Audio\esx.zip, C:\Users\Public\Audio\7zG.exe, C:\Users\Public\Audio\7z.dll, C:\Users\Public\db_Usr.sql, C:\Users\Public\Audio\db_Usr.sql, C:\Users\Public\Audio\hv2.ps1, C:\Users\Public\7zG.exe, C:\Users\Public\7z.dll, C:\Users\Public\BitLogic.dll, C:\Users\Public\NetApp.exe, C:\Users\Public\DataSoft.exe, C:\Users\Public\BitData.exe, C:\Users\Public\DigitalText.dll, C:\Users\Public\GeniusMesh.exe, \Device\Mup\{redacted}\C$\Users\Public\Music\PROCEXP.sys, \Device\Mup\{redacted}\C$\Users\Public\Music\DumpNParse86.exe, \Device\Mup\{redacted}\C$\Users\Public\Music\POSTDump.exe, \Device\Mup\{redacted}\C$\Users\Public\Music\DumpNParse.exe, C:\Users\Public\socksps.ps1, C:\Users\Public\Thief.exe, C:\Users\All Users\{redacted}\GWT.ps1, C:\Program Files\MonitorIT\GWT.ps1, Comment: alias for cmd.exe, C:\Users\Public\eucr.exe, C:\Windows\DS_c1.dll, C:\Windows\DS_c1.dll, C:\Windows\DS_c1.dll, C:\Windows\DS_c1.dll, C:\Windows\DS_c1.dll, C:\Windows\DS_c1.dll, *\instructions_read_me.txt

TYPE	VALUE
Domains	trailshop[.]net, realbumblebee[.]net, recentbee[.]net, investrealtydom[.]net, webnubee[.]com, artspathgroup[.]net, buyblocknow[.]com, currentbee[.]net, modernbeem[.]net, startupbusiness24[.]net, magentoengineers[.]com, childrensdolls[.]com, myfinancialexperts[.]com, limitedtoday[.]com, kekeoamigo[.]com, nebraska-lawyers[.]com, tomlawcenter[.]com, thesmartcloudusa[.]com, rasapool[.]net, artspathgroupe[.]net, specialdrills[.]com, thetrailbig[.]net, consulheartinc[.]com, otxcosmeticscare[.]com, otxcarecosmetics[.]com, artstrailman[.]com, ontexcare[.]com, trackgroup[.]net, businessprofessionalllc[.]com, securecloudmanage[.]com, oneblackwood[.]com, buygreenstudio[.]com, startupbuss[.]com, onedogsclub[.]com, wipresolutions[.]com, recentbeelive[.]com, trailcocompany[.]com, trailcosolutions[.]com, artstrailreviews[.]com, usaglobalnews[.]com, topglobaltv[.]com, startupmartec[.]net, technologgies[.]com, jenshol[.]com, simorten[.]com, investmentgblog[.]net, protectionek[.]com, Table 11: Suspected Black Basta Domains, airbusco[.]net, allcompanycenter[.]com,

TYPE	VALUE
Domains	animalsfast[.]net, audsystemecll[.]net, auuditoe[.]com, bluenetworking[.]net, brendonline[.]com, businesforhome[.]com, caspercan[.]com, clearsystemwo[.]net, cloudworldst[.]net, constrtionfirst[.]com, erihudeg[.]com, garbagemoval[.]com, gartenlofti[.]com, getfnewsolutions[.]com, getfnewssolutions[.]com, investmendvisor[.]net, investmentrealtyhp[.]net, ionoslaba[.]com, jessvisser[.]com, karmafisker[.]com, kolinileas[.]com, maluisepaul[.]com, masterunix[.]net, monitor-websystem[.]net, monitorsystem[.]net, mytrailinvest[.]net, prettyanimals[.]net, reelsysmoona[.]net, seohomee[.]com, septcntr[.]com, softradar[.]net, startupbizaud[.]net, startuptechnologyw[.]net, steamteamdev[.]net, stockinvestlab[.]net, taskthebox[.]net, trailgroupl[.]net, treeauwin[.]net, unitedfrom[.]com, unougn[.]com, wardeli[.]com, welausystem[.]net, wellsystemte[.]net, withclier[.]com
IPv4	66[.]249[.]66[.]18, 66[.]249[.]66[.]18, 66[.]249[.]66[.]18, 95[.]181[.]173[.]227, 207[.]126[.]152[.]242, 72[.]14[.]196[.]50,

TYPE	VALUE
IPv4	72[.]14[.]196[.]192, 72[.]14[.]196[.]2, 72[.]14[.]196[.]226, 46[.]161[.]27[.]151, 207[.]126[.]152[.]242, 185[.]219[.]221[.]136, 64[.]176[.]219[.]106, 5[.]78[.]115[.]67, 207[.]126[.]152[.]242, 46[.]8[.]16[.]77, 185[.]7[.]214[.]79, 185[.]220[.]100[.]240, 107[.]189[.]30[.]69, 5[.]183[.]130[.]92, 185[.]220[.]101[.]149, 188[.]130[.]218[.]39, 188[.]130[.]137[.]181, 46[.]8[.]10[.]134, 155[.]138[.]246[.]122, 80[.]239[.]207[.]200, 183[.]181[.]86[.]147, 34[.]149[.]120[.]3, 104[.]21[.]40[.]72, 34[.]250[.]161[.]149, 88[.]198[.]198[.]90, 151[.]101[.]130[.]159, 35[.]244[.]153[.]44, 35[.]212[.]86[.]55, 34[.]251[.]163[.]236, 34[.]160[.]81[.]203, 34[.]149[.]36[.]179, 104[.]21[.]26[.]145, 83[.]243[.]40[.]10, 35[.]227[.]194[.]51, 35[.]190[.]31[.]54, 34[.]120[.]190[.]48, 116[.]203[.]186[.]178, 34[.]160[.]17[.]71

Recent Breaches

https://active-pcb.com
https://ayesa.com
https://azdel.com
https://bdcm.com
https://cavotec.com
https://cmactrans.com
https://doyon.com

https://fluenthome.com
https://gai-it.com
https://hymer-alu.de
https://ids-michigan.com
https://macphie.com
https://swisspro.ch
https://synlab.com
https://teaspa.it
https://thelawrencegroup.com
https://true.co.uk
https://www.olsonsteel.com

Patch Links

https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

https://screenconnect.connectwise.com/download

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42278

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42287

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a

https://www.cisa.gov/news-events/alerts/2024/05/10/cisa-and-partners-release-advisory-black-basta-ransomware

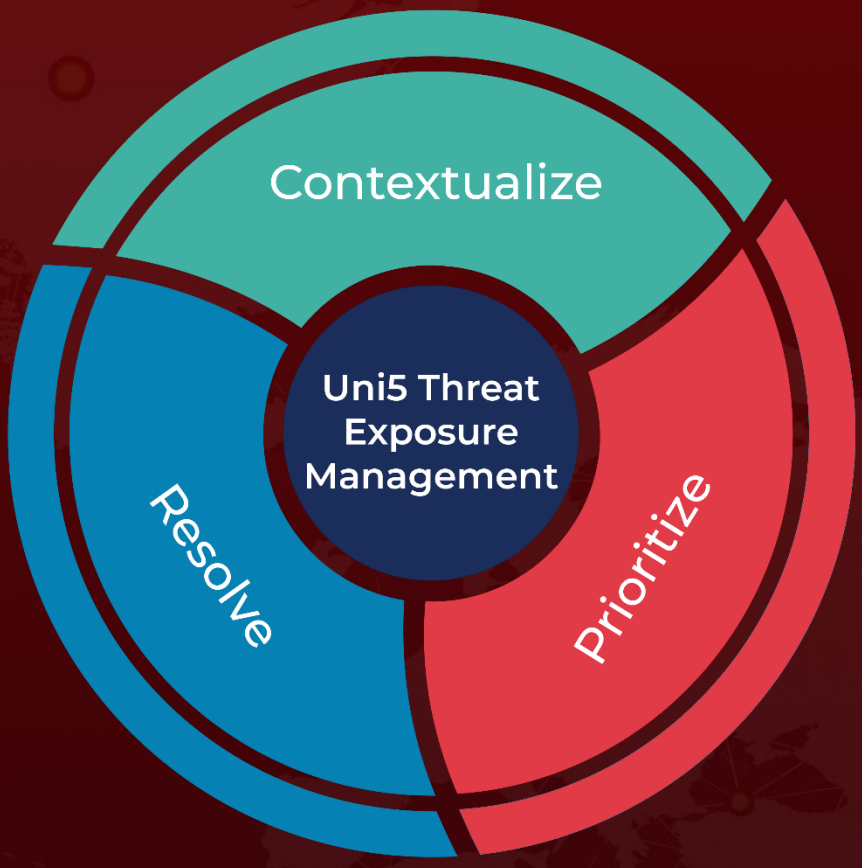
https://www.hivepro.com/threat-advisory/ransomware-black-basta-uses-tools-related-to-fin7/

https://www.hivepro.com/threat-advisory/critical-vulnerabilities-in-screenconnect-under-active-exploitation/

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

May 14, 2024 • 6:30 AM

More at www.hivepro.com