UPDATE: Black Basta Threat Actor Emerges as a Major Threat to the Healthcare Industry

Threat Bulletins | TLP:WHITE | Alert ID : 2c4e32a6 | May 10, 2024, 06:06 PM

UPDATE:

On May 10, 2024, new indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) were made available through a joint Cybersecurity Advisory (CSA) from the Cybersecurity and Infrastructure Security Agency (CISA). Health-ISAC is sharing the updated information for overall awareness and action. The Health-ISAC bulletin, plus this CSA serves as a reminder of the recent Black Basta ransomware activity whose actors have encrypted and stolen data from at least 12 of the 16 critical infrastructure sectors, including the Healthcare and Public Health (HPH) Sector.

The tactics, techniques, and procedures identified in the Black Basta ransomware operation include:

Initial Access

Black Basta affiliates primarily use spearphishing [T1566] to obtain initial access. According to cybersecurity researchers, affiliates have also used Qakbot during initial access.

Starting in February 2024, Black Basta affiliates began exploiting ConnectWise vulnerability CVE-2024-1709 [CWE-288] [T1190]. In some instances, affiliates have been observed abusing valid credentials [T1078].

Discovery and Execution

Black Basta affiliates use tools such as SoftPerfect network scanner (netscan[.]exe) to conduct network scanning. Cybersecurity researchers have observed affiliates conducting reconnaissance using utilities with innocuous file names such as Intel or Dell, left in the root drive C[:]\ [T1036].

Lateral Movement

Black Basta affiliates use tools such as BITSAdmin and PsExec, along with Remote Desktop Protocol (RDP), for lateral movement. Some affiliates also use tools like Splashtop, Screen Connect, and Cobalt Strike beacons to assist with remote access and lateral movement.

Privilege Escalation and Lateral Movement

Black Basta affiliates use credential scraping tools like Mimikatz for privilege escalation. According to cybersecurity researchers, Black Basta affiliates have also exploited ZeroLogon (CVE-2020-1472, [CWE-330]), NoPac (CVE-2021-42278 [CWE-20] and CVE-2021-42287 [CWE-269]), and PrintNightmare (CVE-2021-34527, [CWE-269]) vulnerabilities for local and Windows Active Domain privilege escalation [T1068].

Exfiltration and Encryption

Black Basta affiliates use RClone to facilitate data exfiltration prior to encryption. Prior to exfiltration, cybersecurity researchers have observed Black Basta affiliates using PowerShell [T1059.001] to disable antivirus products, and in some instances, deploying a tool called Backstab, designed to disable endpoint detection and response (EDR) tooling [T1562.001]. Once antivirus programs are terminated, a ChaCha20 algorithm with an RSA-4096 public key fully encrypts files [T1486]. A .basta or otherwise random file extension is added to file names and a ransom note titled readme[.]txt is left on the compromised system. To further inhibit system recovery, affiliates use the vssadmin[.]exe program to delete volume shadow copies [T1490].

For additional information, including a tabled version of the TTPs identified, please see the full report here.

Indicators of Compromise:

For Health-ISAC members who have implemented the Health-ISAC Indicator Threat Sharing (HITS) program, the IOCs initially shared may have been ingested into your environment via the H-ISAC WHITE STIX/TAXII feed. These IOCs should be purged from your environment and automated network defenses.

For visibility into the full list of IOCs available in the Cybersecurity Advisory (AA24-131A), please see the full report here.

Additional Information

Original Alert: May 10, 2024

The notorious ransomware group, Black Basta, has recently accelerated attacks against the healthcare sector. Health-ISAC is urging all Healthcare and Public Health (HPH) sector entities to review this threat bulletin and follow the recommended actions below.

Black Basta emerged in early 2022 and quickly became one of the most active ransomware-as-a-service (RaaS) threat actors. They use double extortion tactics, encrypting victims' data and threatening to leak sensitive information on their public leak site on Tor, named Basta News. The group has allegedly extorted over 100 million dollars since its emergence, making it one of the most prolific active ransomware strains.

The threat actor is financially motivated and has opportunistically targeted the healthcare sector as a part of their malicious operations. In the past month, at least two healthcare organizations, in Europe and in the United States, have fallen victim to Black Basta ransomware and have suffered severe operational disruptions. Taking these latest developments into consideration, Health-ISAC has assessed that Black Basta represents a significant threat to the healthcare sector. Members are strongly advised to keep an eye on the threat actor and their tactics, techniques and procedures (TTPs).

Black Basta's malware, written in C++, targets both Windows and Linux systems. It encrypts data using ChaCha20 and RSA-4096 and attempts to delete shadow copies and backups.

The group has been linked to the defunct Conti threat actor group due to similarities in their operations. There are suspicions that the group is also linked to another actor FIN7 due to similarities in their tools and TTPs. The level of sophisticated TTPs deployed by the group corresponds to a more mature operation which could be explained by connections to the more established threat actors like Conti and FIN7.

The threat actor is using spearphishing attacks and has also been seen buying compromised credentials through Initial Access Brookers (IABs) to obtain means of initial access.

In some of the previous attacks the group also used the following vulnerabilities to breach organizations:

- ConnectWise ScreenConnect authentication bypass vulnerability - CVE-2024-1709, and path-traversal vulnerability - CVE-2024-1708
- Microsoft Windows common log file system driver elevation of privilege vulnerability - CVE-2022-35803
- Vmware OpenSLP vulnerability - CVE-2021-21974
- Fortra GoAnywhere MFT pre-authentication command injection vulnerability CVE-2023-0669

Black Basta uses advanced techniques to evade detection by security solutions and hinder file recovery from backups. These include obfuscation and polymorphism, Living Off the Land (LotL), anti-analysis and sandbox detection, memory execution, disabling security solutions, and deleting backups. These techniques make it difficult for antivirus solutions to detect and prevent file recovery without the decryption key. The ransomware also uses legitimate system tools AnyDesk, AteraAgent and Splashtop, and processes to move laterally into the network, and execute malicious actions. Other common tools identified being used by the Black Basta affiliates in the infection chain are Qakbot (aka QBot), SystemBC, Mimikatz, Cobalt Strike, and Rclone.

Organizations are advised to remain vigilant to any suspicious activity in their environments, and to apply recommendations from the following section.

More technical analysis, as well as mapped TTPs are available in Kroll's analysis: Black Basta - Technical Analysis.

Recommendations

- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.
- Regularly update software and operating systems to patch vulnerabilities.
- Implement strong email security measures to prevent phishing attacks.
- Limit account access privileges across organizations.
- Use a combination of antivirus, anti-malware, and firewall solutions to protect against threats.
- Regularly back up data and ensure backups are isolated and immutable.
- Conduct cybersecurity awareness training for employees to recognize and report suspicious activities such as phishing attempts.
- Monitor networks for suspicious activity and have an incident response plan in place.
- Create and implement a business continuity plan to ensure minimal operational disruptions in case of a ransomware incident.

Threat Indicator(s)

SHA256

96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be

d73f6e240766ddd6c3c16eff8db50794ab8ab95c6a616d4ab2bc96780f13464d

0554eb2ffa3582b000d558b6950ec60e876f1259c41acff2eac47ab78a53e94a

0a8297b274aeab986d6336b395b39b3af1bb00464cf5735d1ecdb506fef9098e

723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224

e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757

7ad4324ea241782ea859af12094f89f9a182236542627e95b6416c8fb9757c59

17879ed48c2a2e324d4f5175112f51b75f4a8ab100b8833c82e6ddb7cd817f20

5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa

9a55f55886285eef7ffabdd55c0232d1458175b1d868c03d3e304ce7d98980bc

58ddbea084ce18cfb3439219ebcf2fc5c1605d2f6271610b1c7af77b8d0484bd

62e63388953bb30669b403867a3ac2c8130332cf78133f7fd4a7f23cdc939087

a7b36482ba5bca7a143a795074c432ed627d6afa5bc64de97fa660faa852f1a6

90ba27750a04d1308115fa6a90f36503398a8f528c974c5adc07ae8a6cd630e7

37a5cd265f7f555f2fe320a68d70553b7aa9601981212921d1ac2c114e662004

fafaff3d665b26b5c057e64b4238980589deb0dff0501497ac50be1bc91b3e08

462bbb8fd7be98129aa73efa91e2d88fa9cafc7b47431b8227d1957f5d0c8ba7

86a4dd6be867846b251460d2a0874e6413589878d27f2c4482b54cec134cc737

69192821f8ce4561cf9c9cb494a133584179116cb2e7409bea3e18901a1ca944

3090a37e591554d7406107df87b3dc21bda059df0bc66244e8abef6a5678af35

39939eacfbc20a2607064994497e3e886c90cd97b25926478434f46c95bd8ead

acb60f0dd19a9a26aaaefd3326db8c28f546b6b0182ed2dcc23170bcb0af6d8f

d15bfbc181aac8ce9faa05c2063ef4695c09b718596f43edc81ca02ef03110d1

88c8b472108e0d79d16a1634499c1b45048a10a38ee7990544146l3cc9dccccc

3c50f6369f0938f42d47db29a1f398e754acb2a8d96fd4b366246ac2ccbe250a

360c9c8f0a62010d455f35588ef27817ad35c715a5f291e43449ce6cb1986b98

5b2178c7a0fd69ab00cef041f446e04098bbb397946eda3f6755f9d94d53c221

17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90

b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9

5942143614d8ed34567ea472c2b819777edd25c00b3e1b13b1ae98d7f9e28d43

42f05f5d4a2617b7ae0bc601dd6c053bf974f9a337a8fcc51f9338b108811b78

51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e

1c1b2d7f790750d60a14bd661dae5c5565f00c6ca7d03d062adcecda807e1779

3337a7a9ccdd06acdd6e3cf4af40d871172d0a0e96fc48787b574ac93689622a

fff35c2da67eef6f1a10c585b427ac32e7f06f4e4460542207abcd62264e435f

ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e

05ebae760340fe44362ab7c8f70b2d89d6c9ba9b9ee8a9f747b2f19d326c3431

f039eaaced72618eaba699d2985f9e10d252ac5fe85d609c217b45bc8c3614f4

350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd

0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298

df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415

07117c02a09410f47a326b52c7f17407e63ba5e6ff97277446efc75b862d2799

d3683beca3a40574e5fd68d30451137e4a8bbaca8c428ebb781d565d6a70385e

882019d1024778e13841db975d5e60aaae1482fcf86ba669e819a68ce980d7d3

Domain(s)

welausystem[.]net

septcntr[.]com

businessprofessionalllc[.]com

currentbee[.]net

maluisepaul[.]com

animalsfast[.]net

myfinancialexperts[.]com

audsystemecll[.]net

fy9[.]39d9030e5d3a8e2352daae2f4cd3c417b36f64c6644a783b9629147a1[.]afd8b8a4615358e0313bad8c544a1af0d8efcec0e8056c2c8eee96c7[.]b06d1825c0247387e38851b

simorten[.]com

treeauwin[.]net

getfnewssolutions[.]com

airbusco[.]net

startupmartec[.]net

recentbeelive[.]com

kolinileas[.]com

specialdrills[.]com

bluenetworking[.]net

fy9[.]36c44903529fa273afff3c9b7ef323432e223d22ae1d625c4a3957d57[.]015c16eff32356bf566c4fd3590c6ff9b2f6e8c587444ecbfc4bcae7[.]f71995aff9e6f22f8daffe9d2ad9

buygreenstudio[.]com

topglobaltv[.]com

investmendvisor[.]net

monitorsystem[.]net

withclier[.]com

recentbee[.]net

adslsdfdsfmo[.]world

trailcocompany[.]com

taskthebox[.]net

onedogsclub[.]com

consulheartinc[.]com

unitedfrom[.]com

brendonline[.]com

trackgroup[.]net

magentoengineers[.]com

my[.]2a91c002002[.]588027fa[.]dns[.]realbumblebee[.]net

trailgroupl[.]net

kekeoamigo[.]com

technologgies[.]com

tomlawcenter[.]com

protectionek[.]com

ionoslaba[.]com

artstrailman[.]com

artstrailreviews[.]com

erihudeg[.]com

modernbeem[.]net

reelsysmoona[.]net

constrtionfirst[.]com

monitor-websystem[.]net

limitedtoday[.]com

businesforhome[.]com

wellsystemte[.]net

otxcosmeticscare[.]com

jenshol[.]com

startupbuss[.]com

rasapool[.]net

startuptechnologyw[.]net

investmentgblog[.]net

artspathgroupe[.]net

otxcarecosmetics[.]com

webnubee[.]com

cloudworldst[.]net

gartenlofti[.]com

0gpw[.]588027fa[.]dns[.]realbumblebee[.]net

investmentrealtyhp[.]net

usaglobalnews[.]com

jessvisser[.]com

startupbusiness24[.]net

childrensdolls[.]com

securecloudmanage[.]com

artspathgroup[.]net

allcompanycenter[.]com

trailshop[.]net

stockinvestlab[.]net

getfnewsolutions[.]com

nebraska-lawyers[.]com

auuditoe[.]com

caspercan[.]com

ontexcare[.]com

softradar[.]net

clearsystemwo[.]net

garbagemoval[.]com

karmafisker[.]com

buyblocknow[.]com

thetrailbig[.]net

startupbizaud[.]net

dns[.]trailshop[.]net

masterunix[.]net

xkpal[.]d6597fa[.]dns[.]blocktoday[.]net

wipresolutions[.]com

seohomee[.]com

trailcosolutions[.]com

oneblackwood[.]com

mytrailinvest[.]net

dns[.]artspathgroupe[.]net

wardeli[.]com

investrealtydom[.]net

steamteamdev[.]net

prettyanimals[.]net

thesmartcloudusa[.]com

unougn[.]com

realbumblebee[.]net

IP(s)

88[.]198[.]198[.]90

5[.]183[.]130[.]92

46[.]161[.]27[.]151

95[.]181[.]173[.]227

64[.]176[.]219[.]106

185[.]220[.]101[.]149

155[.]138[.]246[.]122

207[.]126[.]152[.]242

188[.]130[.]218[.]39

185[.]220[.]100[.]240

80[.]239[.]207[.]200

185[.]219[.]221[.]136

66[.]249[.]66[.]18

83[.]243[.]40[.]10

116[.]203[.]186[.]178

5[.]78[.]115[.]67

183[.]181[.]86[.]147

46[.]8[.]10[.]134

185[.]7[.]214[.]79

46[.]8[.]16[.]77

107[.]189[.]30[.]69

188[.]130[.]137[.]181

Reference | References

sectrio
Fortinet
incibe
HHS
Kroll
Reuters
CISA

Tags

White, Black Basta

Linked Alert(s)

1b76422a

For Questions or Comments:

Please email us at toc@h-isac.org