Good for Evil: DeepBlueMagic Ransomware Group Abuses Legit Encryption Tools

varonis.com/blog/deepbluemagic-ransomware

A group known as "DeepBlueMagic" is suspected of launching a ransomware attack against Hillel Yaffe Medical Center in Israel, violating a loose "code of conduct" that many ransomware groups operate under.

The incident resulted in cancellation of non-urgent elective procedures and the hospital was forced to switch to alternative systems to continue patient care.

This is not the first time that a healthcare institution has been targeted, and undoubtedly not the last given that some may consider them a soft target. The disruption caused by these financially-motivated cyber attacks could result in a loss-of-life situation by delaying or preventing critical care.

The attack employed a "living off-the land" technique, using legit encryption tools to evade detection.

This post will explore this tactic in-depth and provide recommendations for detecting abuse of legitimate encryption tools by threat actors.

Initial Access

Official details of this incident are limited, but early indications suggest that the suspected threat actor, known as 'DeepBlueMagic', gained initial access by exploiting a known Pulse Secure VPN vulnerability.

The exploitation of network infrastructure is consistent with previously reported DeepBlueMagic activity, an unsurprising revelation given that many ransomware operators favor tried-and-tested exploits to acquire user credentials and/or gain privileged access to victim networks.

This incident should act as yet another reminder as to why it is important to ensure that network infrastructure devices, all too often deployed and forgotten about, are included in robust patch management programs.

Encryption Phase

The exact tactics, techniques, and procedures (TTP) utilized in this incident are unknown at this time but would likely include some element of privilege escalation, lateral movement, and reconnaissance to identify and access suitable hosts for encryption.

As is common in the encryption phase of ransomware attacks, the threat actor attempts to thwart recovery by deleting volume shadow copy data using the Windows native tool vssadmin.exe.

While not explicitly observed here, it is also common for ransomware operators to terminate processes and services associated with backup and security tools, to evade detection and further thwart recovery, as well as any application servers, such as SQL, to ensure that files are not locked open.

Once these target hosts have been identified, DeepBlueMagic appears to favor the use of off-the-shelf encryption tools rather than using their own, or an affiliate, ransomware threat.

The 'living off the land' technique, along with the use of reputable third-party applications, offers several advantages to the threat actor while posing an interesting problem for defenders: how to determine nefarious use versus legitimate behavior.

In this specific incident, and again consistent with previous DeepBlueMagic ransomware attacks, it is understood that Microsoft's native disk encryption utility 'BitLocker' is used alongside Jetico's 'BestCrypt', the latter having both large government and private sector users according to their website.

In addition to being easily deployable within a victim network, it is unlikely that endpoint security solutions will detect or alert on these legitimate utilities.

Defenders will be reliant on the need to detect behavioral activity, both prior to the encryption phase, such as unusual user logon activity and privilege escalation, and during the encryption phase, such as the unexpected execution of these utilities or anomalous disk and file operations.

Notably, the use of BestCrypt and BitLocker has previously been observed in ransomware attacks with anecdotal reports suggesting their use in an attack against a French hospital in April 2021 that was loosely attributed to a ransomware group known as 'TimisoaraHackerTeam' (THT) based on their historical use of these TTP.

That said, most reports of activity attributed to THT date from 2018 and therefore it is perhaps more likely that DeepBlueMagic is an evolution of the group, or has simply adopted the same TTP, and has an apparent focus on targeting the healthcare sector.

Jetico BestCrypt

The use of BestCrypt appears to be favored when the threat actor encounters a host with multiple partitions or volumes with the legitimate application being copied to a local folder named **c:\crypt** based on screenshots obtained from the Hillel Yaffe Medical Center incident.

At this point, it is unclear if the threat actor using some 'portable' version of the application, simply running the 'BestCrypt Volume Encryption Manager' executable (**bcfmgr.exe**) alongside its dependencies, or if they are installing the full package. A supporting device driver appears to be required and, upon installation, would require the target host to be rebooted.

While it is possible that the threat actor may have discovered a workaround for this device driver requirement, any unexpected driver installation and reboot should be considered highly suspicious.

Once operational, the threat actor can use the BestCrypt graphical user interface (GUI) (Figure 1), or more likely execute **bcfmgr.exe** using the command-line parameters, to select target volumes for encryption, encryption method, and a presumably victim specific passphrase.

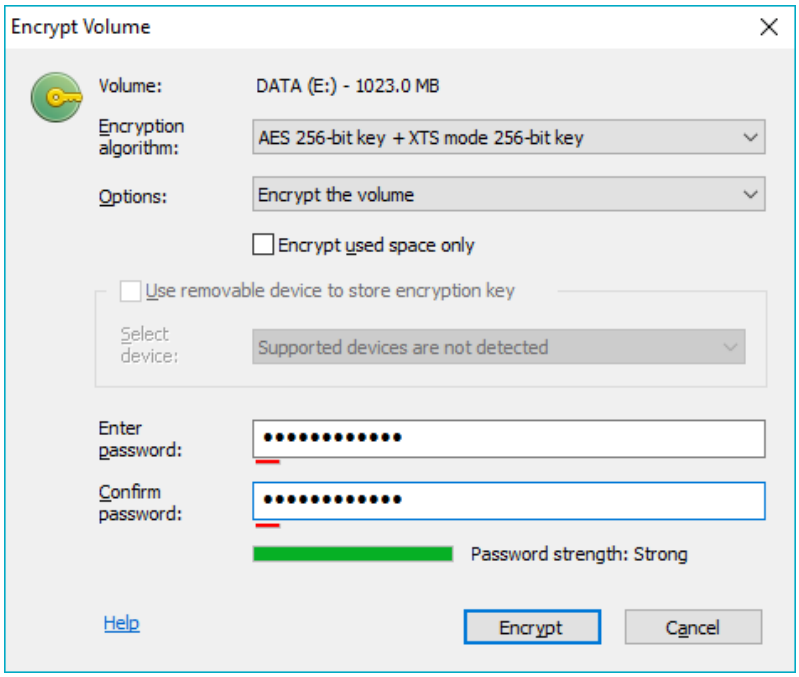

Figure 1 - BestCrypt GUI [Image source: Jetico Inc.]

Although previous reports of ransomware activity involving BestCrypt suggest that only a portion of the volume is encrypted, we were unable to find a suitably robust method of partial encryption within the application and therefore it would presumably require the threat actor to interrupt the encryption process at some arbitrary point. If this were the case, the encrypted volume, and data, would presumably be in an unpredictable condition thus making it difficult to successfully restore. The result would be more destructive or disruptive in nature and would not align with the traditional modus operandi of a ransomware group in which the victim needs to 'trust' that they will get their data back upon payment.

Additionally, it is understood that the system drive is not encrypted, and therefore, post-reboot, Windows will still boot but the victim would not be able to access their data.

BitLocker

While BestCrypt appears to be favored, the threat actor appears to fall back on to the use of Microsoft's data protection tool BitLocker when encountering single volume hosts, albeit containing both a boot drive and system drive as is expected on modern Windows deployments.

Natively available within Microsoft Windows 10 (Education, Enterprise and Professional) and Windows Server 2016 onwards, BitLocker typically requires Trusted Platform Module (TPM) hardware to be present although this limitation can be bypassed through the configuration of a Group Policy Object (GPO) (Figure 2).

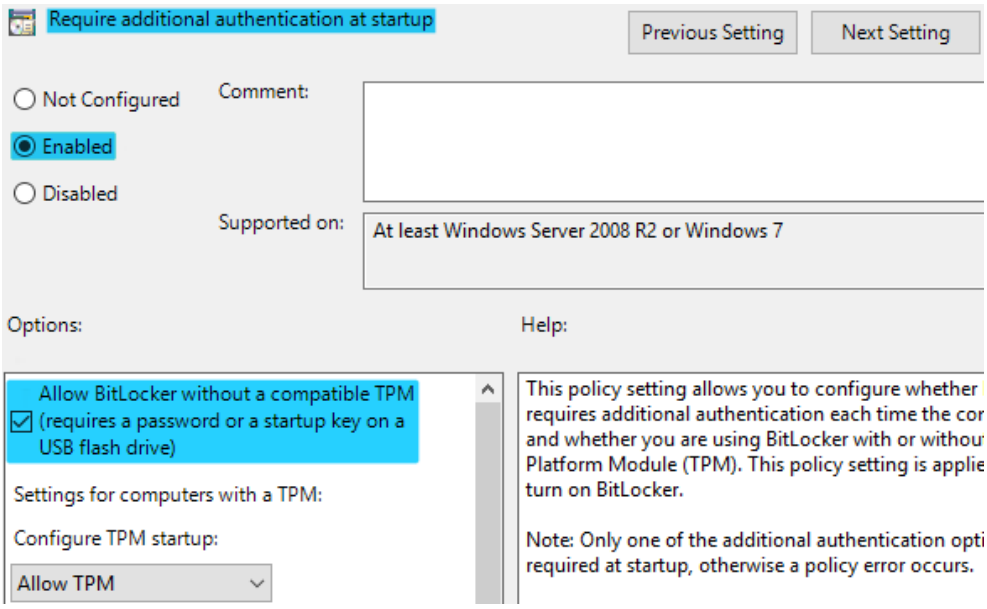

Figure 2 - Allowing BitLocker without a TPM (GPO configuration)

Once any preparatory steps have been made, BitLocker can be manually enabled through the Windows Control Panel (**'System and Security' > 'BitLocker Drive Encryption'**) or, more likely for an attacker automating their process, via the command line utility **manage-bde** (Figure 3) which also supports the configuration of a remote machin e.

```
>manage-bde
BitLocker Drive Encryption: Configuration Tool version 10.0.19041
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

manage-bde[.exe] -parameter [arguments]

Description:
    Configures BitLocker Drive Encryption on disk volumes.

Parameter List:
    -status     Provides information about BitLocker-capable volumes.
    -on         Encrypts the volume and turns BitLocker protection on.
    -off        Decrypts the volume and turns BitLocker protection off.
    -pause      Pauses encryption, decryption, or free space wipe.
    -resume     Resumes encryption, decryption, or free space wipe.
    -lock       Prevents access to BitLocker-encrypted data.
    -unlock     Allows access to BitLocker-encrypted data.
    -autounlock Manages automatic unlocking of data volumes.
    -protectors Manages protection methods for the encryption key.
    -SetIdentifier or -si
                Configures the identification field for a volume.
    -ForceRecovery or -fr
                Forces a BitLocker-protected OS to recover on restarts.
    -changepassword
                Modifies password for a data volume.
    -changepin  Modifies PIN for a volume.
    -changekey  Modifies startup key for a volume.
    -KeyPackage or -kp
                Generates a key package for a volume.
    -upgrade    Upgrades the BitLocker version.
    -WipeFreeSpace or -w
                Wipes the free space on the volume.
    -ComputerName or -cn
                Runs on another computer. Examples: "ComputerX", "127.0.0.1"
    -? or /?    Displays brief help. Example: "-ParameterSet -?"
    -Help or -h Displays complete help. Example: "-ParameterSet -h"
```

Figure 3 - BitLocker command line configuration

Given that the threat actor only appears to use BitLocker on single drive hosts, we suspect that the BitLocker key would be temporarily saved to C:\, likely having a BEK file extension, (Figure 4) using the following manage-bde command:

manage-bde -protectors -add c: -TPMAndStartupKey c:

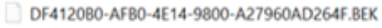

Figure 4 - BitLocker key

Furthermore, it would be possible for a threat actor with domain administrator privileges to both push the BitLocker GPO configuration across the domain alongside logon or start scripts containing the appropriate command line or PowerShell commands.

Having enabled encryption for the target host, the threat actor appears to save and presumably exfiltrate the BitLocker key before potentially clearing the TPM to ensure that it is not saved locally. After doing so, the victim would be prompted to insert a USB drive containing the BitLocker key upon rebooting (Figure 5), effectively locking them out.

Figure 5 - BitLocker password prompt

Although not observed, this password prompt is clearly different from the BestCrypt prompt (Figure 6) that would be presented if the threat actor were to encrypt the system volume using BestCrypt rather than BitLocker.

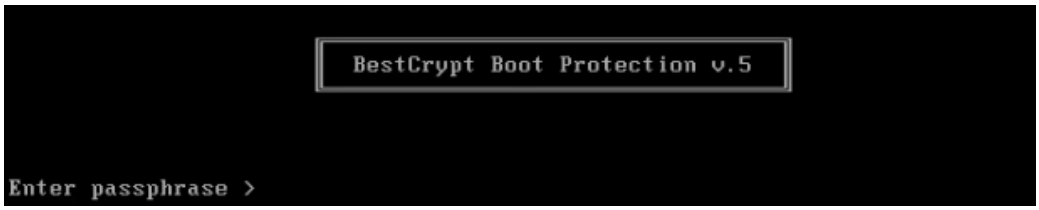

Figure 6 - BestCrypt passphrase prompt

Recommendations

- Given that many ransomware groups continue to gain initial access to victim networks by exploiting known vulnerabilities, organizations should ensure that all devices, not only servers and workstations, are subject to patch management processes.
- The abuse of legitimate tools prevents their detection as 'malicious binaries' and therefore the unexpected presence or execution of either BestCrypt or BitLocker should be investigated as a matter of urgency.
- Organizations not knowingly using BestCrypt should consider searching for the presence of the files identified in the indicators of compromise (IOC) section as well as proactively blocking and/or monitoring for any unexpected execution.
- In the case of BitLocker, System event log entries originating from 'BitLocker-API', 'BitLocker-DrivePreparationTool', 'BitLocker-Driver' and/or 'BitLocker-Driver-Performance' may provide an indication of unauthorized or unexpected use.
- Privileged activity, such as the installation of device drivers, along with unexpected reboots should also be considered suspicious especially when observed on servers.
- As always, organizations should monitor for the unexpected execution of legitimate Windows utilities commonly used in ransomware attacks such as net.exe, taskkill.exe, vssadmin.exe, and wmic.exe.

- Organizations should also prevent access to common administrative tools and script interpreters to prevent misuse by threat actors.

Varonis has seen success in the battle against ransomware on many fronts.

Noisy file system behavior is easy for Varonis to spot because of how closely our platform watches and analyzes data access activity. Most human-operated ransomware groups, however, don't encrypt files right away - they take over multiple systems, steal data, and leave backdoors before they trigger mass encryption.

Luckily, Varonis can alert you to early signs of compromise by ransomware gangs and APTs with behavior-based threat models for each phase of the kill chain. Beyond detection, Varonis can dramatically reduce your attack surface by automatically identifying and removing excessive access to data.

Indicators of Compromise (IOC)

BestCrypt

In this incident, screenshots indicate that the legitimate BestCrypt files were saved to **c:\crypt** including the executable **bcfmgr.exe** (SHA256: e904aaedabd6ab729470dd178c798b45503e8624d3b825e98fb6587deeec6e90).

Additionally, sources indicate that a self-extracting archive potentially named UnPack.exe (SHA256: 35d3b9b4f14fb313014dbc5cae08a3a3a5c460a31dc21c246143ee55d468651b) was used to deliver the following legitimate BestCrypt files in addition to supporting libraries.

Note: These are provided to assist defenders in hunting for unauthorized usage rather than suggesting that the files themselves are malicious, Jetico BestCrypt is a legitimate application.

Filename (SHA256)

- BCUpdate.exe (ceec3cbb3a97c6be2c0446fcd74134ab8feec66f985bc50f17fb41350494c6ef)
- bc_3des.sys (30e190d598d6a3fe301ccd6970d37389fb626f514243a2af42d65620520193a1)
- bc_3des.sys (453cb70ca57ca437e0e45ad068846b5f367afa9036edcab6d8ad6fda0f0c8fe3)
- bc_3des.sys (4ce5c92a5933c8493294d6a31eecc1b4a8db0398279ec8a9ec27cae931cdcd3f)
- bc_3des.sys (bab12d44c3e2d0ed28c5f8f850986d4c72730a1d008e66b91a433bb7bf1dd808)
- bc_3des.sys (d7daae86bbc0b5db0ff0ae07cdd685864b5cf1c5902dae5663860c1c6c75d8f9)
- bc_3des.sys (f8a1b45e6cd063b9c0d544d554e69b0b8b79bced30985ee8ce2362013f82f583)
- bc_bf128.sys (3cb8fcdb10e320b5d6d48438d2fc717c9295dc4253bdf7a90f16b3c9db41dafe)
- bc_bf128.sys (7e9264000ac21bcc04deaa4a47da9e6632d7324acf92794775a8604d2766a939)
- bc_bf128.sys (840ebfb4a88a7271734349364a5a2c8270022b0a0dd3ce8e055f95901e884384)
- bc_bf128.sys (b84b53f3e99ad24b362fce0d10bbead428a978b997d4f8b96284025cf3d58536)
- bc_bf128.sys (d89cdc36d4da9359aa1845fc34a89e65ede6fa8e03acdf50169f6c50776a81e8)
- bc_bf128.sys (f3b4feba20663cd875bc63a24989f3fd43447059c7018f3ba687168aeb2ef4e8)
- bc_bf448.sys (19d179136c04642bc54e45f824854cb9d67672cc5f61e49bc8a03c27b455e88f)
- bc_bf448.sys (3cc7c9ead9665c3f150adee12c7085ecff58e999cb1ffe286e04b608a928687b)
- bc_bf448.sys (524bfaff4e3cd362967d484cba187d8909873b37b6fbe284720176a4b914c04e)
- bc_bf448.sys (c715c91c8b553e37440a72d00f8c9760160b340141e5a846c53a847c1aba79de)
- bc_bf448.sys (cf6d47f6d25a932cd08ca9b1c614a4e68fa0f2b802a2e78959f9de35a54c61a5)
- bc_bf448.sys (d84750a28da5d13419dfc8d0641f85943079b9d0b464fd5170f27b8b236a350f)
- bc_bfish.sys (1853725d3c251f4775b193c39a210283f3f273b3eae358996ff7cc77d8e46d13)
- bc_bfish.sys (9ea8d6bac8076f44f54f6c2614c2bd9259646ade5df30ad3942da4ae4f579535)
- bc_bfish.sys (ab0138604500a7767b2f765fd1807dd2e33ece74c9c3ecd8482d593b5cdac8ec)
- bc_bfish.sys (b6bcaa5e5e736feb5f6c581645b6f4a7ffbd56819d59dbcfaea55ff423ebf9d7)

- bc_bfish.sys (c7440bbe4771c47d1054f85617745fbf488d60f1ade22c553d26ef9527bf397c)
- bc_bfish.sys (c99e3694a8cbc757fbe940216c3858c5d3129fa6982b8653c78f929a5fb293e5)
- bc_camellia.sys (4404cf4a71698c170bff526b2dfbb6ae22ff57fc2f21ed0a56def987b905c2e6)
- bc_camellia.sys (4b9cc8d8d1d507d65e33a52fb2fe323f8e58809ef65fa8793709cffdcedbe050)
- bc_camellia.sys (7361d4b1dbde4bf0d0e4becabef73a7aeff721e7ddba21d9b0c591d8d427f81b)
- bc_camellia.sys (bbfc2285d1ea17528afabf7a9680a4e5a857fe5fd14257beca0a672c7f8694a7)
- bc_camellia.sys (dc3028fb2417ec25de4ec31df6fc94ead36a95fe5f07495d13f22cc71aeb77f2)
- bc_cast.sys (329c360344b1f80c15c018199467a064fc847de32b11ed46f7d144557a95420d)
- bc_cast.sys (42619f2c8ac56ec5f2d8ba6696b63e0dae8479b0ca231eb862cd963a96eeaa63)
- bc_cast.sys (5d7b7c8f10f1ae473457979c8c779a5e62cb85ec9b29f3047abdd5000fc717f1)
- bc_cast.sys (621c35c436f7ebc7a193a2124b53106ba5e4a0a86726e70c71310734a6558709)
- bc_cast.sys (69f38b76dbd744ea934b9813fb20713ed8093749a5fd920d0f8bf4fdd372fff1)
- bc_cast.sys (b9ac821597ab93896f004d9331a80453f85876ea30e2dd92f81c9299bac418f3)
- bc_des.sys (3a2b81f77f287f9ed3130fcacb8fafbeba21938ef23c65692c27471bfb454977)
- bc_des.sys (7c72a8665f752b76d0939fc575eb9974dbea02c009197c01cb28a39ff54cd4b1)
- bc_des.sys (8887032687d6d0fcbba084f5c46e10b7364a9b29323d65aaaf12c9dfc18b06d3)
- bc_des.sys (e6b9d13e78102c045c3038ece1fad9f530303aab5af1dc75473c39bb8d051d2a)
- bc_des.sys (f01c6109a0fe6cfdd4010c6ffcb07f7ac2c05643b494a45766ffa08682b707d7)
- bc_des.sys (facb945844312ae6b40bbf5cf42cc046603ea025a7a566d1ca794fc2255cf018)
- bc_gost.sys (5d9365e15af76cf73337aa36a575cc2a64f58879e181d10abfe817c25654505e)
- bc_gost.sys (65cc253282fda93b574ecd195009e597e97e783141eee249530f12eda446007e)
- bc_gost.sys (c7a7b6cee59649ea74a95634c152c8c48b93b2ff6cc1f6625c17a3453446b927)
- bc_gost.sys (f6a661cabeb32815aefde843c7d073b5cd27ea5759dcacb952a8f4d33c50fd0b)
- bc_gost.sys (f7b2729fa4c17645d7d44a93ab69a20ede2c65bf281d40633b51cbfc3465515e)
- bc_gost.sys (f91dcb5cb7bcc877f8a3f2a8ac8d8c02fcea9b3f90d4eecb720e616ec02fe494)
- bc_idea.sys (2c83d173f99134452a57560ae9f50d6678fe770be0b787982f8ad3a5e5b9692e)
- bc_idea.sys (35304edd129fa1217aa2ac359b71cce72f1d7061284760cece56a44dd3aff076)
- bc_idea.sys (4eba7573b17715366dc131f6abc6e0439d87decba9ce891a1d8952366dc3deb2)
- bc_idea.sys (69dcbb57466f246f67a502b66b3f479cbf74aa2c5eeaa994ba2572fd732978a9)
- bc_idea.sys (91cfcd7c19b2882f648c36d4afe0e3d757ccb7fdbc2bbb9af615ef556afab6b4)
- bc_idea.sys (fa0640b866e6481b2136a18ec8fcd4755496eb8390dc23211b6fc99cc88bfb5d)
- bc_rc6.sys (0685e68d68d2d9b21b1756f5a69e3f36dbeb07ada5ce6a48f8f604168791f941)
- bc_rc6.sys (17f45315a3dfed231faa0c5e4633b7c02e3fcc6911edf24751ffe3ea7c25a870)
- bc_rc6.sys (31e291b4cee55cc5cb034d99f6c477d8c0668ceed0d9e9546c08c7d441a7c8f7)
- bc_rc6.sys (6a9cf36e20bdb6906aef9f878cec7ee4530db2cedd66c9c10c827b8142fa6993)
- bc_rc6.sys (acf4fefcf4c4103eef80749bac322563102d853505f22ab0ced6e08caec53d4b)
- bc_rc6.sys (b6e94264aeac3ca303f6c2449f7744930da472a8452c7a26a69da14e960aa847)
- bc_rijn.sys (0ea0de965613cc7c8ec541a8dd0d8ff56b915318655e995979ef1edaa5447d6c)
- bc_rijn.sys (136a1583aadc7fccb138b228700699f2a61a6a700969f2fefdda09eda70c8545)
- bc_rijn.sys (13dbc844d813c5957d11f246d275ae4cacddb0bb13753467c3439feb8c991a36)
- bc_rijn.sys (b0f0741c0958d745322fd1b3641cd067e89bb64aca77a35547d070bc2541cef7)
- bc_rijn.sys (d0726cb7124a0eca88bdea11b2d2189aaf113c2c6657085ef512ce6b1316d2f9)
- bc_rijn.sys (e03984ab633880b24429463475bd9cf5e422c3ce42d841ce5fc7558f38484188)
- bc_serp.sys (15fc43233c1e4718bd7b830f81e189990169c025949166b16f259d3123c85287)
- bc_serp.sys (18af08c5a2be4b6689e3aa0e3bd1277eb63f79b65026f62c6ec5e6af7bd9e4c4)
- bc_serp.sys (4704439237cb1805463a78a5a0f227e86cc5a4f90134ef310ac32f1c4702879f)
- bc_serp.sys (6c6171fe30c71b101064546e357b8a1dd79dfd3713a10e80955718741358525b)
- bc_serp.sys (963682d41149c6ee0743ff73f13e082a579353fe2e663a9d1a3b24ba22ccac2a)
- bc_serp.sys (dc5c6ea3691ffb95de0cd6ce38e7ff2d3c6f606c33798a1a7ea1a4aa2d9476e4)
- bc_tfish.sys (01b8111654951b08b226b8d96bbe2bd95d6c3c0c5e58d4f5d176772b74501ce7)

- bc_tfish.sys (16a249c470ce899559c5e686ee07c5fd4a456952b5cd1f4d72882469c3fe4c51)
- bc_tfish.sys (760adc2b1682d5942f38bec3cde66f4334bc9742290092838ab7083e830c5178)
- bc_tfish.sys (8911f8a8f5d906d57dd966aa2de807a04019c327b518c2fa734b5ec8e7ada119)
- bc_tfish.sys (f5dca1c3096c3f3c4805eb1d31442a998d1223bdd062093da264d3e1b3333efd)
- bc_tfish.sys (f92c1bb1a5f8f0980505c8e21daa918cb43f8d3c5e6c75d4800e733af98ba1df)
- BCAlarm.dll (c6b2ae4b5dd388357f6a50407240add3511f5f02601328e736ec55bcc3f5aba2)
- BCArchive.exe (3af98084f71255e03cbf600167132988e52f612ae1ec49798408bf3a11e0c157)
- BCArchive.exe (9106988ea7c8f5ea4c8044751021b5e148df7b3ae512de0adb5225298e6a54ca)
- BCArchUP.exe (05c1668994163eb1592ed333a6010e9640b6cc3e13e33bb10ba9f74f389c1a47)
- BCArchUP.exe (a11e8dbc6e2933a1854c8fcff4c1d7e5fb6105ced648c2cd2ae8a56904007283)
- bcbus.inf (b910f14be7186ac697470e17e1fa301e491ff898a3c42b46bdef795033f1d585)
- bcbus.sys (013685503cd1a1a78cac0c6289dd1b192ca773e67f84d13d330c00d5d7adccf1)
- bcbus.sys (47cbdbcec974fdfd320801e5a0f10b40c323ffe890fd4b2dd33131898d0dfdf9)
- bcbus.sys (65d8126dcc9d4867d61946722b725807aaf528f56396c898952175aa6b89977f)
- bcbus.sys (6c84c06080713fa232c831de8dd23bf112ed8886ddf6e77a29d1d4ce7fbcde60)
- bcbus.sys (b107bc7305b380750be01bd8baf09e6fb1e044480f4ea33113b7b56aed5a8cf1)
- bcbus.sys (be6d5ec3e92787ec85d00e8563af1bbca24c84d5e973bc41f3afa5cea82d6f82)
- bcclient (b86b6ccccc2b442ace1f8ddd5f706c5e1795932fc75f5a6bd9f6bc4834baa0d9)
- bcdpp.exe (a4788e8b374c8b52280ad4e112c95e88a010c9be8ebc0be4e1d470af3f1d6d2a)
- BcdpTray.exe (fc88fcb607e79086dbc03938449da7856db334648a442a5cfa48f79e7dfdc40c)
- bcfmgr.exe (7edc898dd81e21b8048634f092ca361b0de17f44bd98cd94552dddc4ae56b035)
- bcfmgr.exe (e904aaedabd6ab729470dd178c798b45503e8624d3b825e98fb6587deeec6e90)
- bcfnt.inf (50466b6f1d9cef13ad47f557de0033bedf98e9254e8c353b0c0660d6855ce6cb)
- bcfnt.inf (9de0ad3c4e0305e62f8ceadd8c1cd601b778defbb2f2a0e53bd405af18a0f962)
- bcfnt.sys (0d4d4462b8ab1c31539d293a22532cc0fb3a06d070779f60775db8e42b82248f)
- bcfnt.sys (20cd5ebecd08c586eca73b6c7d756916326b749144cd381d278b82107a8b0d66)
- bcfnt.sys (89c11faddbeb572b86148ed8e5d59a42bf27ecaee54035a566ea70a7b31c8ccb)
- bcfnt.sys (f1b18eea0658966012b2611ba24a5cdfe3a4c27603b3887c328ca11920b3303a)
- BCGPUpdt.dll (2264d4717aa138b08ed27edc09b5bcadea1e811c7892c0d7e6d45fb46cb4cf02)
- BCKeyMan.dll (ba658784ef733abc451fb7cd8aa11987059d9c422c67c4feb6663e9e1e2afd2b)
- BCKeyMan.dll (f4e3306294a6b6298239894ef274cea120528b6f49873cf594f13eed4121e8dd)
- BCResident.exe (570d097c5606e5765c7a5a811f99fe08b402a096f2119e762a192da91a6c8b84)
- BCShExt.DLL (146f10f8fe52e8659487efeb6a7117533ec218008aa70cd5af59499442c025c3)
- BCShExt.DLL (654ad61bc4de2b9ad07add2dc7a6de22d24436f699bdb7923c7f510ee67b7e0a)
- BCShExt.DLL (e9a096c886ce42c2dec0fae1492c2943a2e321fcff2a5697d1689ff146f4b4b6)
- BCSrvMan.exe (3ce2743a72fbb993e1cbbf3ea259862cd9803882d16b65f92b7c6c16b61aa822)
- bcswap.sys (2cfc58dd2b8c08e3c4407f4aff32f7983e9ae578001849d9e421825e2b9abcda)
- bcswap.sys (31263d97442970555f6fc7ec2bfcad169ad1641032c015d2477a4898c46b5f89)
- bcswap.sys (32b63da470ccbd894ae2c11ca29be4ffc6f3cb83412cdd9ace62c42276771c47)
- bcswap.sys (a95e8739840d161796ff836286d9715cf87450e811f37a60fd39e29245a91d89)
- bcswap.sys (ba8f0d5bbd4fbf3c5ee383963649089204876e03dcb3ca38188c02c963d46c90)
- bcswap.sys (da0520af5334d2c4be5742d4b29a69d4b114bfde0bb3c164a4f3fd8ea590c4bb)
- BCTextEncoder.dll (202d3211f3b03e27d97dfe844caa92914e485386398a9ba7c3f3d78d7f7955b2)
- BcveCredentialProvider.dll (451876b5aa6cc29e14b1d9da5b987d60745b8ed39c6b1287a2f1fbf4eeb702ff)
- BcveCredentialProvider.dll (4998e368b9b2a9c454bfbd86801a69805c4f60c61f6d7f1b0b403f18e69d5ec6)
- bcveicon.exe (58f4e044351afa49e7462937f17d9a79916ea06d8310ba9a8f2e8c6ef47c9707)
- bcveserv.exe (deb543266ff4f1a8b8f8f15f68b9922d7d2623e79b26a84c8236db7b6510cb7f)
- BcveServiceMessages.dll (05c1f378387942f03a18484cb6767d22f25d8d5818e136c73862259edb313563)
- BcveShellExt.dll (3a6b8dc45ce2dff7559e62c77fd11b3f3aa513443c0fc97e36a03f51502efcbf)
- BcveShellExt.dll (4f989ded91837ec5be147692f5f781696569d11858116311ba7333b76d6fecba)

- bcvetray.exe (818adc2b797146bdcfbb690bb5cbe44130567da63b5b01366caae1e5a1019cec)
- BCView.EXE (1a186d51bb4e4fd18acad387b2872d164e3a772e935b26c9fc673fdf53ccb533)
- BCWipe.dll (b4dbb117b45e7149221f83d079b2afef8841ce78ded641a9ee34b31b1c40de90)
- BCWipe.exe (8327eb8465d62959a40ea487c0fd0da178a8857e4b49a1594c5a2df3631ca179)
- BCWipeGUI.exe (49862483089de3b18d2c987bd9c8d63c79e055f7f091b5cc0e9a13e0490ff05e)
- BCWipeLib2.dll (1d117250e71bcb4a4f8b759bd0e48c280c9b4a94b903d5067441cf5d6a73e06e)
- BCWipeSample.bat (156eec2df1e26bfbcfb08a80d41fc86acc4ed8b200b9cd760868596acd43144c)
- BCWipeSvc (952476a3ead7a97ff9c4906a2801ad993e4850a3e10c4350bbd44ab2eeabbb02)
- BCWipeTM.exe (3037956db905355f66cbd02ad9778f86551b0c34f386ee0adb7c2feb941a0e30)
- BestCrypt.exe (dda5b7aa7a56f5fc85e21a8c16c9acf408b81896fa07a208297e4b204f8a8668)
- fsh.sys (3bf93f08148db1fd799d52833992ad8903b20381a08d2958c8baf9ccd2ad4d50)
- fsh.sys (7d2afe145e66217f2a2430b1dc9c71814277c1f5f1916a1ea314feb86d7f91e7)
- fsh.sys (9668bec9cc2c525edf897939efd7a26056fe6d6f7268361a9448b74068ce9926)
- fsh.sys (a5fe2a3bfacbf02e5f2be092e6af2ccac2bc70f43b56f786d2f0a6858c4678fc)
- fsh.sys (de1a49eef7b01c19fa2a46931a6a54e7ccc61068a52963d2056c9d732c176bdc)
- fsh.sys (f8a468fbaa678ec74cf8739f0213c6b2a9df18694992f05380d9225481c11b3c)
- Jetico.UI.BCWipe.Shared.dll (b4bae8c229c3ff820f15d54e58a88377d3b79d643320d5bba94a0087f4b43b43)
- Jetico.UI.MVVM.dll (e7e7e64b221789fa45794130e77f67c47e68844b030d9187498d944e6502107a)
- Jetico.UI.Resources.dll (31b6f1384275554549e3eb574ed01febafeff62365d48750d219e893e467b181)
- Jetico.UI.Shared.dll (f8eb44bd60f85b5402b2aecfc1c352bc21d550eb25c51d5dbc6809bdcf699477)
- Jetico.UI.UserControls.dll (3c26d89a807271ff5e997809ef1be68a81beb87998fd8ca6ff5d623a7204da2b)
- Jetico.UI.Utils.dll (e11b5e56cbd36d6face6f255c07e4e2bfa9cc0a79a2c65d8507f99b221410af9)
- Jetico.UI.Windows.dll (31755794f33469c9187446c6fc5ea3f947c1ab04617f729e21762e664fb581d4)
- KGGhost.dll (a26c4c8f2c65a873dccc2c848c0ecf14abee44f947b44feeec5364cea011ba70)
- kgsha.dll (50c1b9fd90e4b18070efb9ce6c9d362227cb2da4a02be3f464f9b211ed086c33)
- kgsha256.dll (e1afd9b1c97f5e09c68f3265cc52af8ea02d8d505a6506cb44dfd0814608d5fe)
- logview.exe (b1db8bf866330712a677db84f5b23f48d9b84a6b9e4f1f9d043e67ac93543cdf)
- logview.exe (cd7c9f1bd77e304a913758e95597d96399f823d887d7787fd8e9d8ec7a921d38)
- MftWipeFilter.sys (047f3c13898f5b7984d2d95676bc55d0a1cde00ac8fb4cb74481802adc309b8c)
- MftWipeFilter.sys (1b4e3a984959e8c1c0ce2e1e55c0b599ef73227f9a39c8a6039a85b9da5dc409)
- MftWipeFilter.sys (4c3298977e859627d54468193cf7adf252d32a20d313c0c34c7192fca5252fe1)
- MftWipeFilter.sys (a16d60977beb3e4acbda2e6b769530b7bcdeb7bb12a73644d3b7781dd34d730e)
- MftWipeFilter.sys (bc2a4f9f20a9c6adbb65c4cae42a954100ad6717031eb1e590911bfaef192a25)
- mhk.sys (15ce39694a19430805a6920524220f856404700a23e574776425df5850de6633)
- mhk.sys (620b19aa443e2d0814fea9b6b4732cb7854a2cf33840b42e099726b937d06ac9)
- mhk.sys (6faa455c80d548d2450588e85c73ac1667ba642b214f5b04c6072e179e1c48b8)
- mhk.sys (761b8fb4873225e011fbba3ef140757388e306033eed997e3e63dae5bd3957e9)
- mhk.sys (ae2357aa6ebcf4849be81983d3d84fe5e9ff724d5be058ef84438942ef6b7334)
- mhk.sys (e7316cffc40a2942deeefbae8d030d8cbc8c5a9369ac7a027f44701200afe332)
- moh.sys (1306865023ba27276b1f252b0c169b5328f78fc4be9a801d9a7e6e6ca3f2b005)
- moh.sys (64f7448ced830520904b8859d1d27a5cd8bd4b8fe897bf633e3bf3e06df9e56b)
- moh.sys (9dcbcb09a9194722d969ebac4fe3c709fa2988932071b5568be172ce488a4728)
- moh.sys (e726f8ab10879cf65e26dd03a5cf29a4edee1abfeba5f84c90be335a033695ae)
- moh.sys (f2ef863e0279c04ea51fc6c7f01c9859ba8cea01cdd39d2f02c2bf22204d9df3)
- moh.sys (fe055f9806e10baec9fa227eb0bf5bfd2506eb2f628dcc8a5e386e5e05e18ba5)
- TextEncoder.exe (df19dd36c641f6f9581093db33aff7912582e8deaf2f44733facf84a1af7aa4d)

Jason Hill

Jason is a Security Researcher within the Varonis Research Team and has a penchant for all-things threat intelligence. Equally happy analyzing nefarious files or investigating badness, Jason is driven by the desire to make the cyber world a safer place.