Threat Actor Spotlight: BlackSuit Ransomware

Technical Analysis

Executive Summary

Since May 2023, Arete's Incident Response (IR) team has responded to multiple BlackSuit ransomware engagements against organizations in the healthcare, financial services, manufacturing, professional services, public service, entertainment, and retail sectors. This spotlight explores the ransomware behavior observed, statistics from IR engagements, and background information on the threat actor. Finally, we discuss security recommendations to better defend against this evolving cyber threat and mitigate the risk of financial and reputational losses arising from these incidents.

Incident Response Data on BlackSuit Ransomware

The information below is based on BlackSuit incidents investigated by Arete since May 2023. Our IR and Threat Intelligence teams work together to analyze key data points during every ransomware engagement and form real-time threat actor (TA) insights.

- Arete has investigated dozens of engagements involving BlackSuit.
- We have been extremely successful in negotiating discounted ransoms with this TA.
- The highest observed ransom demand is around $18 million.
- The average initial demand is around $2.5 million.
- The average ransom payment facilitated is around $500,000.
- Commonly observed methods of intrusions include remote desktop protocol (RDP), virtual private network (VPN), and firewall vulnerabilities.
- Tools observed during the investigations include CobaltStrike, WinRAR, PUTTY, Rclone, Advanced IP Scanner, Network Scanner, Mimikatz, and GMER.
- A commonly observed ransom note filename is **readme.blacksuit.txt**.
- In some instances, backups were encrypted or deleted, while in others, backups were used for restoration.

Background

The information about the BlackSuit threat actor group in this section was shared in Arete's 2024 Q1 Crimeware Report.

The most notable newcomer in Q1 was BlackSuit, the third most active group of Q1. Although Arete first observed BlackSuit ransomware operating in May 2023, it only accounted for less than a half percent of the total engagements in 2023. The group significantly increased its activity in Q1 2024, and there were more BlackSuit engagements in February 2024 alone than in all of 2023. BlackSuit operates as a private group without affiliates, targeting both Windows and Linux users and utilizing a double extortion method of stealing and encrypting sensitive data on a victim's network.

BlackSuit: A Continuation of Royal Ransomware?

The BlackSuit ransomware payload has significant code overlap with Royal ransomware, and the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI believe BlackSuit to likely be a rebranding or spinoff variant of Royal. While BlackSuit could be using the same developer or code with slight modifications, Arete also observed language used by BlackSuit in ransom negotiations identical to previous engagements with Royal, which lends to the assessment that the group might be a rebrand or offshoot. Regardless, BlackSuit's emergence demonstrates that although names may change, threat actors will find ways to adapt and evolve their operations.

Figure 1. Language from two separate BlackSuit TOR chats *(Source: Arete)*

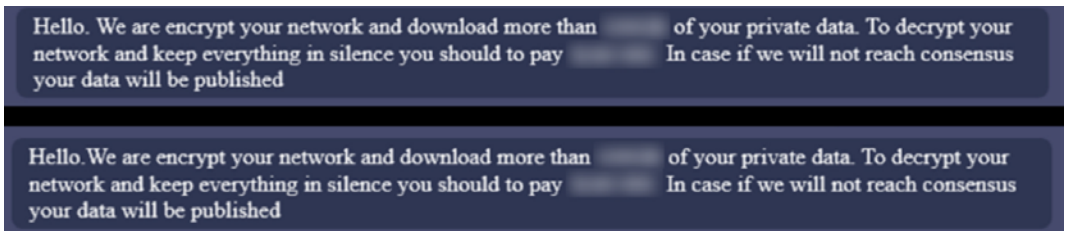

Figure 2. Identical language from two separate Royal TOR chats *(Source: Arete)*

Technical Analysis

Malware analysis revealed that BlackSuit ransomware:

- Supports multiple command-line arguments.
- Encrypts files on the system and mounted shares.
- Adds the following extension to encrypted files: .blacksuit (e.g., file.docx.blacksuit).
- Creates a ransom note with the following filename: readme.blacksuit.txt.
- Self-identifies the group as BlackSuit in the ransom note.
- References a data leak site in the ransom note that, when accessed, self-identifies the group as BlackSuit.
- Kills a list of processes and services.
- Maintains a list of whitelisted files and directories to make sure it will not render the system unusable, preventing recovery when running a decryptor.
- Attempts to prevent system recovery by deleting the system's volume shadow copies.
- Creates the following mutex during execution: WLm87eV1oNRx6P3E4Cy9.

Execution Pattern/Arguments

BlackSuit ransomware needs command line arguments to execute and encrypt files in the system. Command line arguments supported:

Command line argument	Description
-id [32-byte characters]	Ransomware ID
-size	Invoked with drag and drop
-ep	Number that represents the percentage of the file that will be encrypted
-path [target_directory_path]	Used to specify a target directory to encrypt
-localonly	Encrypt only the local system
-networkonly	Encrypt only shared volumes/directories
-aavm	Encrypt all files

The ransomware will not execute in the system without the "–id" argument followed by a 32-character value that is unique in each engagement and present in the ransom note TOR URL. Portion of the data in the ransom note that contains the ID:

> All your files will be decrypted, your data will be reset, your systems will stay in safe.
> Contact us through TOR browser using the link:
> *http://c7jpc6h2ccrdwmhofuij7kz6sr2fg2ndtbvvqy4fse23cf7m2e5hvqid[.]onion/?id=[32-characters]*

Execution of ransomware to encrypt files:

```
blacksuit.exe -id [32-characters]
```

The ransomware developer coded the logic to allow configuration of the 32-character value in the command line during execution. This same victim-specific 32-character string value is then added to the ransom note URL used for negotiations. Due to this implementation in the ransomware code, threat researchers can execute the ransomware without knowing the 32-character string value, as any value of this type can be used to execute the malicious code. In analyzing Royal ransomware samples, Arete found a similarity in that any 32-character value can be supplied to execute the ransomware, and the value is also added to the ransom note TOR chat URL.

Example of how the ransom note content looks with a randomly supplied string (e.g., blacksuit.exe -id 7777 77777777777777777777777777):

```
All your files will be decrypted, your data will be reset, your systems will stay in safe.
Contact us through TOR browser using the link:
http://c7jpc6h2ccrdwmhofuij7kz6sr2fg2ndtbvvqy4fse23cf7m2e5hvqid[.]
onion/?id=77777777777777777777777777777777
```

Obfuscated Files or Information: Software Packing

Most of the strings in the ransomware are encoded. The encoded strings are hardcoded and decoded at runtime. Every encoded string has its own decoding loop:

```
mov byte ptr ss:[esp+1F],C          C:'\f'
mov byte ptr ss:[esp+20],77         77:'w'
mov byte ptr ss:[esp+21],1D
mov byte ptr ss:[esp+22],77         77:'w'
mov byte ptr ss:[esp+23],51         51:'Q'
mov byte ptr ss:[esp+24],77         77:'w'
mov byte ptr ss:[esp+25],12
mov byte ptr ss:[esp+26],77         77:'w'
mov byte ptr ss:[esp+27],33         33:'3'
mov byte ptr ss:[esp+28],77         77:'w'
mov byte ptr ss:[esp+29],77         77:'w'
mov byte ptr ss:[esp+2A],77         77:'w'
mov al,byte ptr ss:[esp+1F]
```

Figure 3. Encoded strings hardcoded

```
00405D80  8A440C 1F     mov al,byte ptr ss:[esp+ecx+1F]
00405D84  0FB6D0        movzx edx,al
00405D87  83EA 77       sub edx,77
00405D8A  8BC2          mov eax,edx
00405D8C  C1E0 04       shl eax,4
00405D8F  03C2          add eax,edx
00405D91  03C0          add eax,eax
00405D93  99            cdq
00405D94  F7FB          idiv ebx
00405D96  8D42 7F       lea eax,dword ptr ds:[edx+7F]
00405D99  99            cdq
00405D9A  F7FB          idiv ebx
00405D9C  88540C 1F     mov byte ptr ss:[esp+ecx+1F],dl
00405DA0  41            inc ecx
00405DA1  83F9 0C       cmp ecx,C                          C:'\f'
00405DA4  72 DA         jb aaaa.405D80
```

Figure 4. String decoding loop

Some relevant strings decoded in memory:

Global\\WLm87eV1oNRx6P3E4Cy9	-ep
readme.blacksuit.txt	-path
\windows\	-localonly
svchost.exe	-networkonly
explorer.exe	-aavm
-size	Microsoft Enhanced RSA and AES Cryptographic Provider
cmd.exe /c vssadmin delete shadows /all /quiet	

Obfuscated Files or Information: Dynamic API Resolution

To avoid static or other defensive analysis, the ransomware uses dynamic API resolution to conceal malware characteristics and functionality. The ransomware initially decrypts DLL names, then loads the APIs. Hardcoded encoded DLL names are shown below:

Figure 5. Encoded DLL names

Figure 6. DLL name decoding loop

DLL names decoded at runtime:

shell32.dll	rstrtmgr.dll
user32.dll	ntdll.dll
advapi32.dll	Crypt32.dll
ws2_32.dll	Iphlpapi.dll
shlwapi.dll	

Stop Services and Processes

Before file encryption, the ransomware terminates a list of known running processes and services to encrypt as many files as possible. BlackSuit ransomware utilizes the Windows Restart Manager to terminate any process using files other than explorer.exe or a critical process.

Sequence of Windows Restart Manager APIs used by the ransomware:

RmStartSession	Starts the Restart Manager session
RmRegisterResources	Registers resources, in this case the targeted filename
RmGetList	Determine which processes or services are using the registered resource (file)
RmShutdown	Shuts down any identified process or service using the registered resource
RmEndSession	Closes the Restart Manager session

The ransomware also uses Windows native CreateToolhelp32Snapshot, Process32FirstW, and Process32NextW APIs to enumerate processes in the system.

File and Directory Exclusions

The ransomware excludes system-related files and folders, ransomware-related files, and whitelisted extensions during encryption.

Excluded file extensions:

.com .ani .scr .drv .hta .rom .bin .msc .ps1 .shs .adv .msu .prf .bat .idx .mpa .cmd .msi .mod .ocx .ics .386 .sys .rtp .wpx .msp .cab .ldf .lnk .cur .nls .hlp .key .ico .exe .icns .lock .theme .diagpkg .diagcab .nomedia .diagcfg .msstyles .themepack .blacksuit .deskthemepack

Excluded files and directories:

> “msocache”, “intel”, “$recycle.bin”, “windows”, “windows.old”, “mozilla firefox”, “$WinREAgent”, “boot”, “google”, “perflogs”, “system volume information”, “appdata”, “tor browser”, “$windows.~ws”, “application data”, “$windows.~bt”, “mozilla”, “readme.blacksuit.txt”

Inhibit System Recovery

Windows operating systems contain features that can help fix corrupted system files, including shadow copies, which are backups of files created by the Volume Shadow Copy Service (VSS). By deleting shadow copies, the ransomware can prevent victims from restoring files from backups, making it more difficult for them to recover their data without paying the ransom.

With the CreateProcessW function, the ransomware deletes volume shadow copies before file encryption by executing the following command:

```
cmd.exe /c vssadmin delete shadows /all /quiet
```

Code in the ransomware showing this operation (the EAX register contains the kernel32.CreateProcessW address):

```
lea ecx,dword ptr ss:[esp+70]
push ecx                                ecx:L"cmd.exe /c vssadmin delete shadows /all /quiet"
lea ecx,dword ptr ss:[esp+8C]
push ecx                                ecx:L"cmd.exe /c vssadmin delete shadows /all /quiet"
push 0
push 0
push 8000000
push 0
push 0
push 0
lea ecx,dword ptr ss:[esp+F0]
push ecx                                ecx:L"cmd.exe /c vssadmin delete shadows /all /quiet"
push 0
call eax
test eax,eax
```

Figure 7. Create process call to delete volume shadow copies

System Network Connections Discovery

BlackSuit ransomware can enumerate network-mounted shares by scanning the network interfaces.

Data Encrypted for Impact

The ransomware initially finds available drives and loads the files one by one using the Windows API FindFirstFileW and FindNextFileW. It then uses OpenSSL AES keys to encrypt the files and adds the extension .blacksuit to the encrypted file name.

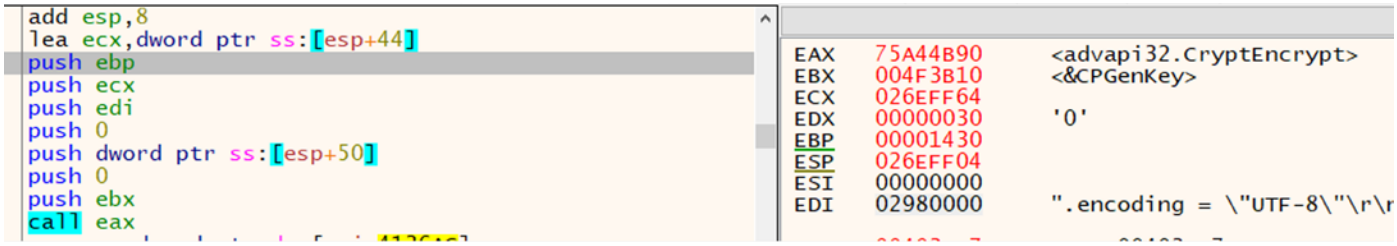

Figure 8. Windows native CryptEncrypt API call to encrypt the data

Public Key:

-----BEGIN RSA PUBLIC KEY-----MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA+O9F-Gkh466oxay/9u//rycLpGqFwcUSQIy0d27cnpRqq1W4De/boeoJC/HJqkr3WaEqr2JhgjSQcMimTxy8d-3NLJT7M3uTVaxXD3Bck83ns5S/WhiF5tQGHtAGetGv8gXYSq/bm6HAlWBMBAaOVw4of7ov7/cTAl1pwvgnaYzws4q6C9Q5zwmcU7DFcOohyVqBu/2svUlvtfMJGzYVeUJSUF6E2NMhCIxddDLr32wCuo-Z567uMBLQB2e5DUTkpIR1OdYeWyxhAXJSjQ5T9LpwUHNn89nuo25slwIUx2m5a2k6wn2husXhXj+NRN/c2F3zh2qkcgs318XY8es1r3UgIBdCYMMGKsZ0DxKJZ1fq4nU93c+aP0qFBawmYhglZq6MBYrG23LGbJPZvC8p-kyJYt51ygthCYVPtgThqlthdqzqnV+7gPaf/XRwHeLkqawPhe1omd9m7gSuFwlREu2MW1qZ7p3Nzfh8ZFX4/YN7PSN1m6Ve5HS1MgnR9cbj655Jt3IqgW6riIlrP+DbdrnjYo7yz2CsxSL3vKVtzcDzsbEFPkAFDyfSrYVxMY-CEUj8jHlctrNo+UiuZTT0O9dbwoGfCSrg8w+V0h8pYaiGnVwwGGkQbLgBAvz+iO0yElbZDLEPjxZ1+ipYzA-DufQSh8RHh/nXpWirlzQNH7oqrA0fUCAwEAAQ==

-----END RSA PUBLIC KEY-----

The ransomware encrypts files, adds the .blacksuit extension at the end of the encrypted files, and adds the following bytes at the end of the file ("??" represents variable bytes):

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ?? 00 00 00 ?? 00 00 00
```

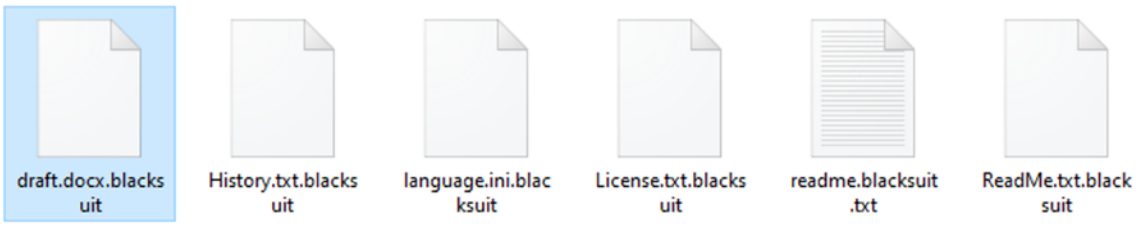

Figure 9. ".blacksuit" extension added to the encrypted files

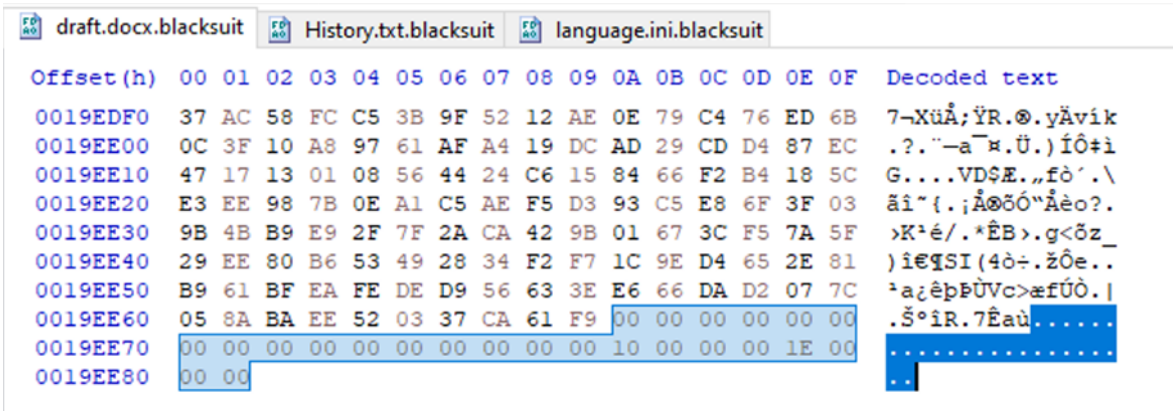

Figure 10. Padding bytes in encrypted files

Upon successful execution, the ransomware creates ransom notes with the file name readme.blacksuit.txt.

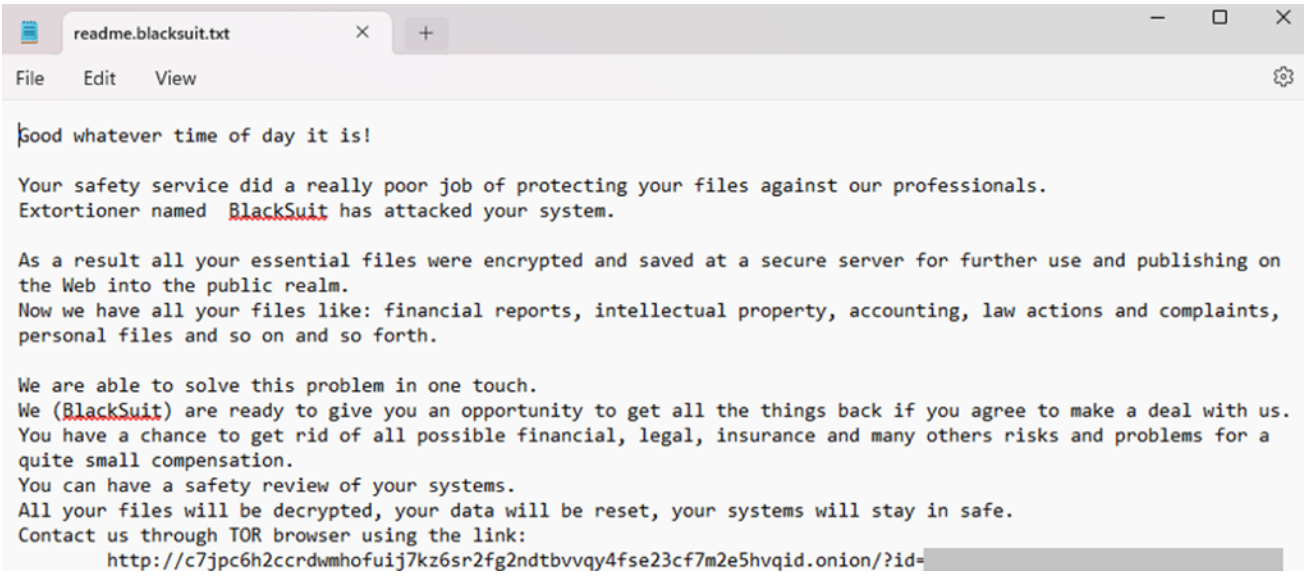

Figure 11. Screenshot of BlackSuit ransom note

Modify Registry

The ransomware did not perform any registry key modification.

Mutex

The mutex is the fundamental tool for managing shared resources between multiple threads or processes. Typically, ransomware uses a mutex to avoid reinfecting the victim system and causing multiple layers of encryption. The ransomware creates the following mutex value: “WLm87eV1oNRx6P3E4Cy9”.

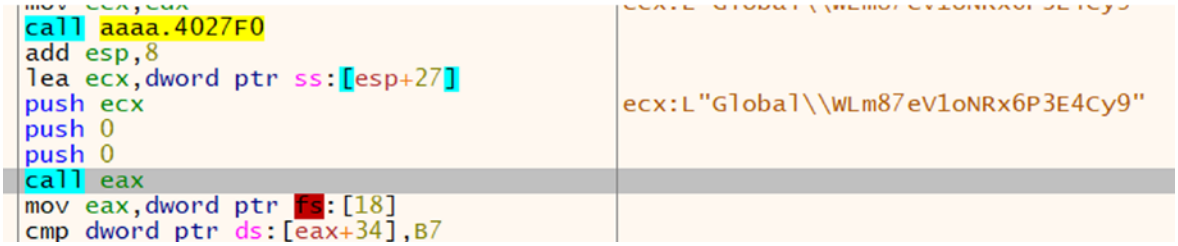

Figure 12. Screenshot of the mutex value created while debugging the ransomware

Network Activity

The ransomware did not try to communicate with a remote server other than encrypting data from mounted shares.

Indicators of Compromise

Indicator	Type	Context
f1684fb118d4d8fc56653fcc49e12a659b64c4459ba037fa94f-21783235cc6ba dede96fd44c0f78eb79ceb63b898874e8922efc59d8bfb-9f86505b1992bc00a3 79ab73a0e9dd8eac045c00fd1bd172a7f359588901f-93c83e6740157eb21e7df d96ff4b3e188f7ff96ed28c1381a6318dd76bb1fbd6ca02c6a-b0236e1c7f35aa	SHA256 hash	BlackSuit ransomware
C:\readme.blacksuit.txt	File path	BlackSuit ransomware
.blacksuit	Extension	Encrypted files extension
vssadmin delete shadows /all /quiet	Process	Volume Shadow Copy deletion
WLm87eV1oNRx6P3E4Cy9	Mutex	Mutex value object created by the BlackSuit ransomware

Any 32-character string	Password	Command line argument needed to properly execute the ransomware. The ransomware developer doesn't validate it
c7jpc6h2ccrdwmhofuij7kz6sr2fg2ndtbvvqy4fse23cf7m2e5h-vqid [.]onion weg7sdx54bevnvulapqu6bpzwztryeflq3s23tegbmnhkbpqz-637f2yd[.]onion	URL	TA data leak site (DLS)

Data Leak Site

The ransom note contains a data leak site (DLS) that displayed the following page, self-identifying the group as BlackSuit:

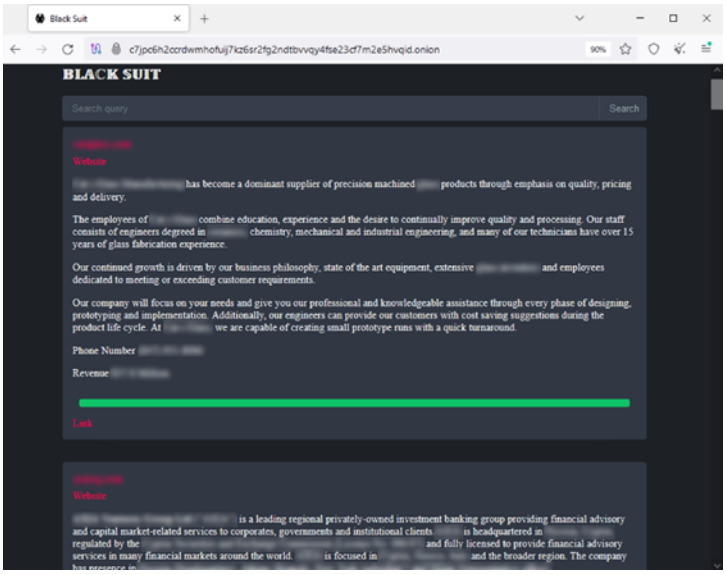

Figure 13. TOR DLS: c7jpc6h2ccrdwmhofuij7kz6sr2fg2ndtbvvqy4fse23cf7m2e5hvqid[.]onion

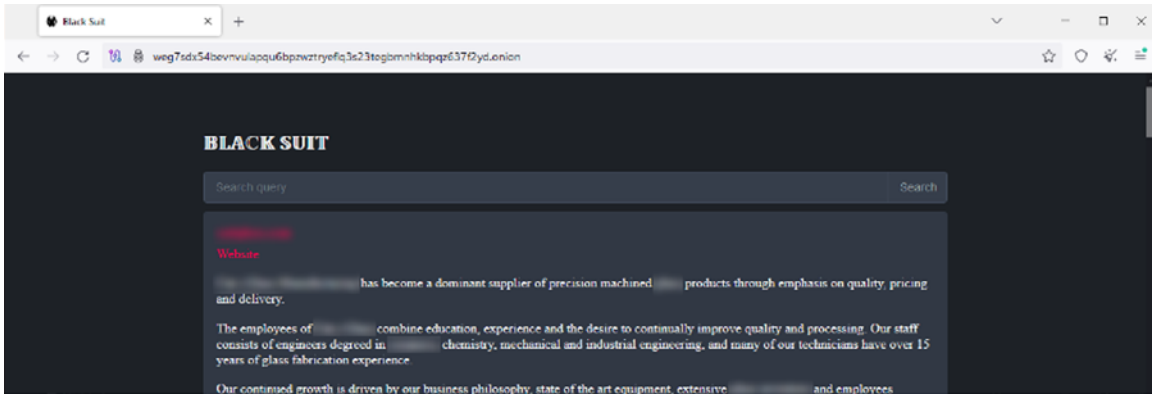

Figure 14. TOR DLS: weg7sdx54bevnvulapqu6bpzwztryeflq3s23tegbmnhkbpqz637f2yd[.]onion

Detection Mechanisms

Custom Detections and Blocking with Arete's Arsinal

SentinelOne S1QL 1.0 query syntax (STAR rule):

BlackSuit Ransomware Execution

EndpointOS = "Windows" **AND** ObjectType = "Process" **AND** TgtProcCmdLine RegExp "\.exe\s{1,5}\-id\s{1,5}[a-z0-9]{32}"

BlackSuit Ransom Note

EndpointOS = "Windows" **AND** ObjectType = "File" **AND** TgtFilePath Contains Anycase ":\readme.blacksuit.txt"

Volume Shadow Copy Deletion

(EndpointOS = "Windows" **AND** ObjectType = "Process") **AND** (TgtProcCmdLine Contains Anycase " vssadmin " **AND** TgtProcCmdLine Contains Anycase " delete " **AND** TgtProcCmdLine Contains Anycase " shadows" **AND** TgtProcCmdLine Contains Anycase " /all " **AND** TgtProcCmdLine Contains Anycase " /quiet")

Note: These threat hunting queries may need to be tuned for your specific network environment.

Yara

```
rule BlackSuit_ransomware

{
meta:
author = "areteir.com"
description = "Detects the BlackSuit ransomware executable"
target = "Windows systems"
file_type = "exe"
copyright = "Copyright © 2024 by Arete Advisors, LLC."
distribution = "No re-distribution without Arete Advisors, LLC consent."

   strings:
      $decoding_loop = { 99 F7 ?? 8D 42 ?? 99 F7 ?? 88 }
      $s2 = "-----END RSA PUBLIC KEY-----"
      $s1 = "-----BEGIN RSA PUBLIC KEY-----"

   condition:
      ( (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) ) and
      ( (all of them) and (#decoding_loop > 20) )
}
```

Recommended Mitigations

- Utilize an endpoint detection and response (EDR) solution with the capability to halt detected processes and isolate systems on the network based on identified conditions.
- Block any known attacker C2s in the firewall.
- Implement multi-factor authentication on RDP and VPN to restrict access to critical network resources.
- Eliminate unnecessary RDP ports exposed to the internet.
- Block a high number of SMB connection attempts from one system to others in the network over a short period of time.
- Perform periodic dark web monitoring to verify if data is available for sale on the black market.
- Perform penetration tests.
- Periodically patch systems and update tools.
- Monitor connections to the network from suspicious locations.
- Monitor downloads and uploads of files to file-sharing services outside standard work hours.
- Monitor file uploads from domain controllers to the internet.
- Monitor network scans from uncommon servers (e.g., RDP server).

Organizations can find the full list of US government recommended ransomware prevention and mitigation guidance here: https://www.cisa.gov/stopransomware/ransomware-guide.

References

https://areteir.com/press-releases/arete-releases-q1-2024-crimeware-report-detailing-ransomware-and-extortion-trends-and-shifts-in-the-cyber-threat-landscape/

https://areteir.com/solutions/managed-services/#arsinal-threat-management

https://therecord.media/car-dealerships-reports-sec-cdk-software-ransomware

https://www.bloomberg.com/news/articles/2024-06-21/cdk-hackers-want-millions-in-ransom-to-end-car-dealership-outage

https://www.bloomberg.com/news/articles/2024-06-24/blacksuit-cybercrime-gang-blamed-in-major-cdk-ransomware-attack