Adversary Profile

Operations Flow

Make separate notes or use labels (e.g. victim-a, client-1, server-2) in the tables below to document the operations flow for later use in a diagram and/or the emulation plan.

Adversary Tools

Please feel free to duplicate lines as needed. Not all tools need to be present in the adversary profile.

Tool	ATT&CK Software ID	CTI Reference and Comments
netcat		[1] NW scanner and generic TCP/UDP relay
mimikatz	S0002: Mimikatz	[1]
BITSAdmin	S0190: BITSAdmin	[1]
PsExec	S0029: PsExec	[1]
Coroxy		[1]
Qakbot	S0650: QakBot	[1][2]
Cobeacon (aka Cobalt Strike beacon)	S0154: Cobalt Strike	[1]

Rclone	S1040: Rclone	[1]
Black Basta ransomware	S1070: Black Basta	[1]
netscan.exe		[2] NW scanner
Splashtop		[2] RDP?
Screen Connect		[2] [3] CVE-2024-1708 and CVE-2024-1709
Cobalt Strike	S0154: Cobalt Strike	[2]
certutil	S0160: certutil	[7]

TTPs

Please feel free to duplicate lines as needed. Not all tactics need to be present in the adversary profile.

Tactic	Technique ID	Procedure	CTI Reference and Comments
Reconnaissance	-	-	Not emulated
Resource Development	-	-	Not emulated
Initial Access	T1021.001: Remote Desktop Protocol	RDP or PS into first server using known credentials	[1] Black Basta turned to underground markets to acquire network access credentials

	T1078: Valid Accounts T1566.002: Spearphishing Link		
Execution	T1059.001: PowerShell T1569.002: Service Execution T1047: Windows Management Instrumentation T1543.003: Windows Service	RDP or PS into first server Powershell	[1] Uses various scripting interpreters like PowerShell and Windows command shell. [1] Stops and deletes the service named "Fax", which it then impersonates for its encryption routine. [1] Has been observed to use Windows Management Instrumentation (WMI) to spread and execute files over the Network. [1] One build restarts the victim's system in safe mode, most likely for evasion purposes, before performing encryption. This build also modifies the "Fax" service to enable it to run in safe mode and with service-level access.

Persistence	T1078.003: Valid Accounts: Local Accounts	Change PW of domain admin	
Privilege Escalation	T1543.003: Windows Service T1078.003: Valid Accounts: Local Accounts ~~T1211: Exploitation for Defense Evasion~~	TBD	[1] Exploits the PrintNightmare vulnerability (CVE-2021-34527) to perform privileged operations For practical reasons we decided to go with a technique that does not require a CVE to be present on the victim [1] One build restarts the victim's system in safe mode, most likely for evasion purposes, before performing encryption. This build also modifies the "Fax" service to enable it to run in safe mode and with service-level access.
Defense Evasion	T1562.001: Disable or Modify Tools T1562.009: Safe Mode Boot T1222.001: File and Directory Permissions	Kill AV Abuse unprotected scheduled job ~~Boot to safe mode before encryption~~	~~[1] uses a batch script containing PowerShell commands to disable antimalware applications … uses Group Policy Objects (GPOs) to disable Windows Defender and Security Center … reboots the victim's computer in safe mode to circumvent any antimalware~~ [5] Batch scripts are often deployed to inhibit detection by anti-virus or other

	Modification; Windows File and Directory Permissions Modification

T1078.003: Valid Accounts: Local Accounts | | security software. The script names vary; however, the content appears to be similar and generally operates in a similar way by removing Windows Defender in stages. Other scripts to remove specific anti-virus have also been identified including a script to establish a scheduled task to prevent anti-virus being reenabled.

[4] Uses bcdedit to boot the device in safe mode.

[6] After running the ransomware as administrator, it removes shadow copies, disables Windows recovery and repair, and boots the PC in safe mode. |
| Credential Access | T1003: OS Credential Dumping | Mimikatz to dump creds and pass the hash | [1] uses Mimikatz to dump credentials |
| Discovery | T1046: Network Service Discovery | Collect information about domain users, including identification of domain | [1] uses Qakbot's and Cobeacon's information-gathering… uses … Netcat to scan the system and the network |

	T1087.002 Account Discovery: Domain Account T1087.001 Account Discovery: Local Account T1033: System Owner/User Discovery T1082: System Information Discovery T1069.001: Permission Groups Discovery: Local Groups T1057: Process Discovery	admin accounts using BloodHound / SharpHound. Enumerate local accounts	[2] Usage of SharpHound to enumerate AD information [4] tsp todo
Lateral Movement	T1197: BITS Jobs	~~We transfer mimikatz and sharphound via BITS~~	[1] Black Basta uses different tools and pieces of malware to spread its

	T1570: Lateral Tool Transfer	Because of stability issues with bits, switch to certutil	ransomware to other remote systems in the network: BITSAdmin PsExec Windows Management Instrumentation (WMI) RDP Qakbot Cobeacon
Collection	xxx	xxx	Not emulated
Command and Control	T1105: Ingress Tool Transfer	Download tooling with certutil	[7] … Black Basta continues using "living off the land" binaries and readily available tools in its latest attacks, including the Windows certutil command-line utility to download SilentNight and the Rclone tool to exfiltrate data.
Exfiltration	T1567: Exfiltration Over Web Service	Exfil via rclone to Kali	[1] Black Basta uses Cobeacon to exfiltrate the stolen data on an established command-and-control (C&C) server. It uses Rclone to exfiltrate data from compromised systems.
Impact	T1486: Data Encrypted for Impact	~~Encrypt files and add .basta ending~~	[1] Black Basta uses the ChaCha20 algorithm to encrypt files. The ChaCha20 encryption key is then encrypted with a

	T1490: Inhibit System Recovery T1491.001: Internal Defacement	~~Change desktop background~~ ~~Place .txt ransom note~~ ~~Add icon for .basta files~~ Delete shadow copies with vssadmin	public RSA-4096 key that is included in the executable.Black Basta uses the ChaCha20 algorithm to encrypt files. The ChaCha20 encryption key is then encrypted with a public RSA-4096 key that is included in the executable. [4] It encrypts files excluding those with a .exe, .cmd, .bat and .com extension. Uses ChaCha20 or RSA-4096 to encrypt victims. [1] Black Basta avoids encrypting files in these folders: • $Recycle.Bin • Windows • Local Settings • Application Data • boot It avoids encrypting files with these strings in their file names: • OUT.txt • NTUSER.DAT • readme.txt (the ransom note) • dlaksjdoiwq.jpg (a desktop wallpaper found in the %TEMP% folder)

			● fkdjsadasd.ico (an icon used for encrypted files, found in the %TEMP% folder) [4] Black Basta modifies the Desktop background by adding a .jpg in C:\Temp and creating a registry key HKCU\Control Panel\Desktop. Additionally modifies the registry to change the icon of encrypted files. [5] After data exfiltration, the next stage is to encrypt endpoints with the Black Basta ransomware binary. The executable name varies between incidents; however, it often provides the same capabilities. The binary launches a command line to delete VSS shadow copies with vssadmin, as shown in Figure 11, before encrypting files and creating the readme.txt file.

References

1: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

2: https://www.cisa.gov/sites/default/files/2024-05/aa24-131a-joint-csa-stopransomware-black-basta_1.pdf`

3: https://www.trendmicro.com/en_us/research/24/b/threat-actor-groups-including-black-basta-are-exploiting-recent-.html

4: https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/

5: https://www.kroll.com/en/insights/publications/cyber/black-basta-technical-analysis

6: https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html

7: https://www.bleepingcomputer.com/news/security/black-basta-ransomware-switches-to-more-evasive-custom-malware/