BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

July 31, 2024

Black Basta Ransomware Gang Changes Tactics

SUMMARY

The Black Basta ransomware gang has changed tactics since the disruption of its partner QBot. The group is now employing new custom malware and leveraging various tools to evade detection and enhance their attack capabilities.

TECHNICAL DETAILS

Black Basta is a ransomware operator known for double-extortion campaigns, combining data theft with encryption to demand large ransom payments. After the QBot botnet disruption, the group formed new alliances with those affiliated with DarkGate malware and SilentNight. Mandiant tracks the Black Basta group as UNC4393 and highlights their use of new malware and tools in their operations, indicating their evolution and continued threat.

In late 2023, Black Basta turned to other initial access distribution methods, specifically those related to DarkGate malware. They later shifted to using SilentNight, a versatile backdoor malware delivered through malvertising. This change also marked the group's move away from phishing as their primary initial access method. Mandiant reports that Black Basta has transitioned from publicly available tools to internally developed custom malware.

Earlier this year, UNC4393 was observed deploying a custom memory-only dropper named DawnCry, initiating a multi-stage infection process that led to the deployment of DaveShell and PortYard tunneler. PortYard, a custom tool, establishes connections to Black Basta's command and control (C2) infrastructure and proxies traffic.

Tools used by Black Basta include:

- BASTA: A C++ ransomware that encrypts local files using ChaCha20/XChaCha20 and appends an encrypted key to each file.
- SYSTEMBC: A C tunneler that acts as a proxy between a C2 server and remote systems, retrieving additional payloads and hiding network traffic.
- KNOTWRAP: A memory-only dropper in C/C++ that decrypts and executes additional payloads in memory with advanced obfuscation techniques.
- KNOTROCK: A .NET utility that creates symbolic links on network shares and executes the BASTA ransomware with the link path.
- DAWNCRY: A memory-only dropper that decrypts an embedded resource into memory using a hard-coded key, containing shellcode and a DAVESHELL loader.
- PORTYARD: A tunneler that connects to a hard-coded C2 server, establishing TCP connections to relay servers and proxying traffic.
- COGSCAN: A .NET reconnaissance tool used to gather information on available network hosts.

Additionally, Black Basta continues to use "living off the land" binaries and readily available tools, including the Windows certutil command-line utility to download SilentNight and the Rclone tool to exfiltrate data.

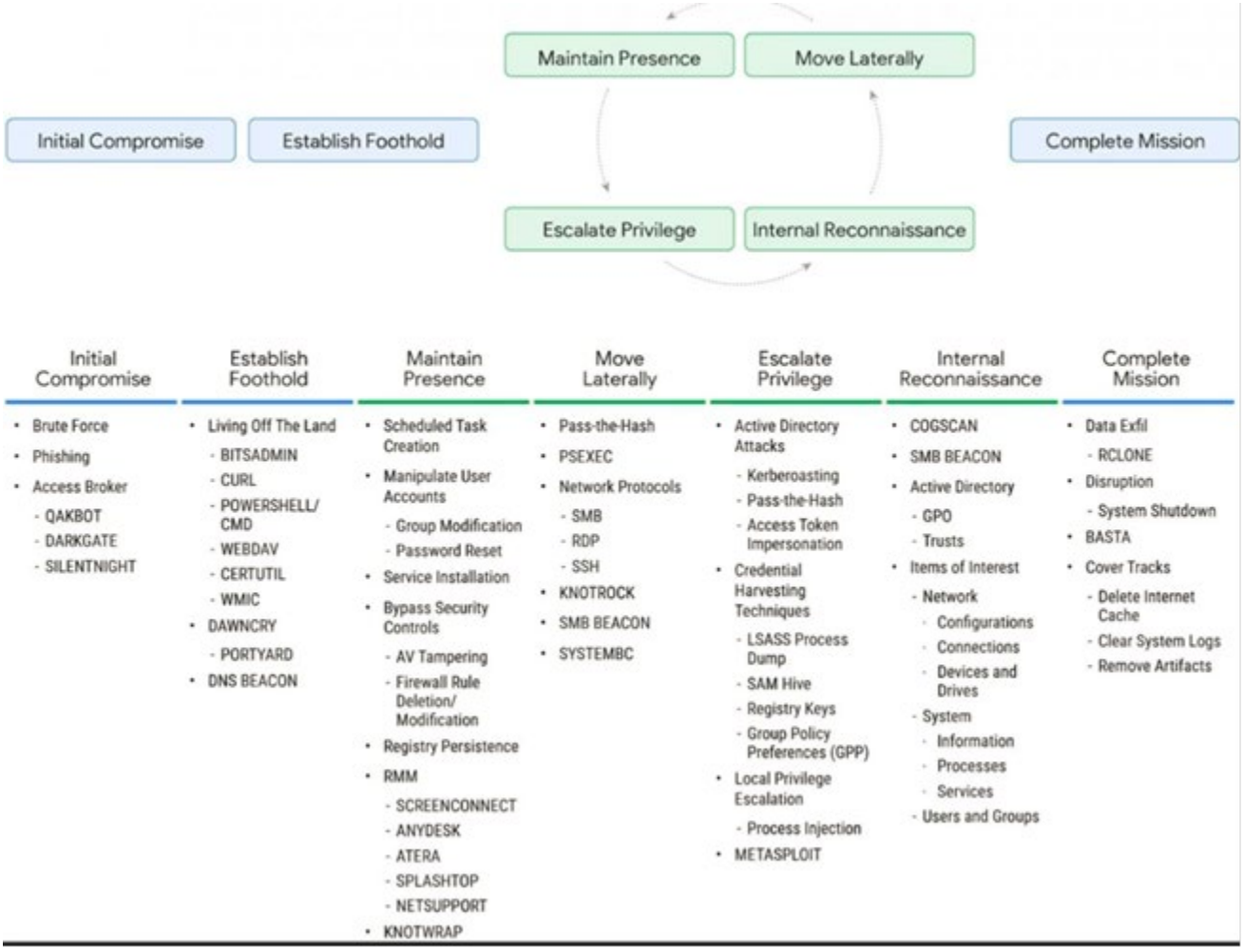

Figure 1. Black Basta's current attack lifecycle from Mandiant

INDICATORS OF COMPROMISE (IOCs)

Hashes

- a9447a25ab79eed2942997daced4eb3e
- d9c69ce1ba4c5411482ec014c8be40e3320e778e
- 021921800888bc174c40c2407c0ea010f20e6d32c596ed3286ebfe7bd641dd79
- af35580a4c293ba23dfe48c03ba1d949
- 77a9ec4ccd9ef76f376e04ce338170685cc26c95
- 1ede3018667af92918ad728f2bfd222d8e71826219c3d8374150cce772f0f7c2
- d4fd61c1bb582b77a87259bcd44178d4
- eead781343d33e0e0e9f998b963ecc8e8032ec31
- 23317330e82ce09b44c8142ed8efc2e068d595071053081bc438604eb0f28b41
- 387864bc379e0017c30fc5f608ac9868
- d3c4163a35204eee15bce9a08825c7e9bc0666ad
- 3c65da7f7bfdaf9acc6445abbedd9c4e927d37bb9e3629f34afc338058680407
- b2af1cd157221f240ce8f8fa88bf6d44
- 65a7fee21eb8842b34e729fc43b668e69905d1ac
- 50400d432452dca3de821d0c3323f62c90d6786abd6db5c1642b37a6b11312a7
- 25dd591a343e351fd72b6278ebf8197e

- 815e7090399df8b9a326c77bb03684f87252c437
- 6381559b7dcdac967085712b8dd016730ab142170a9526cc8daf601f36d826b4
- 3d339c1499363d7571073f9347c9fdb6
- 88437e51dd3872af3658b57e7f489758e8cbf31d
- 6f78256f20eb2b5594391095a341f8749395e7566fdd2ddd3a34a0db9bb9f871
- 286394d06972734946774c85742a094f
- 616415b3ec0c08511d232e56b51faf7a03c45183
- 8501e14ee6ee142122746333b936c9ab0fc541328f37b5612b6804e6cdc2c2c6
- c451ffca71ef1433e1208779c126ef20
- 506db9e2b0871253a9a44083d46831145da5dc13
- 8dd7757da361012d08ce5b33dfa485e256b66cfbc33c35409fd710af8565c284
- 7bd00958b9caabfc1e426205700b63fc
- 1eb93896854fe11e47942530ab109a74adb90c2b
- 93b038797a7f57f38b886395935377b9870c0b7e5db254fa10905149d63f731e

IP Addresses

- 104.207.146.23
- 116.202.235.163
- 131.226.2.165
- 134.122.36.228
- 136.244.110.56
- 139.162.141.128
- 140.82.26.90
- 144.202.30.15
- 162.33.179.6
- 163.116.145.66

Related Domains

- artstrailreviews.com
- cleaninghouseinc.com
- cloudwebstart.net
- conitreid.com
- coxfixed.com
- erihudeg.com
- globalusa.net
- investsystemus.net
- jenshol.com
- lindacolor.com

RECOMMENDATIONS

- Implement trusted ad-blocking software to reduce exposure to potentially malicious advertisements.
- Enforce browser security settings to block pop-ups and restrict JavaScript execution from unknown sources.
- Keep antivirus and antimalware software up to date to detect and block malicious ads.
- Implement web filtering solutions to block access to known malicious websites.
- Educate users about the dangers of malvertising and encourage them to avoid clicking on ads, especially from untrusted sources.
- Regularly update web browsers and plugins to protect against vulnerabilities that malvertising campaigns may exploit.
- Deploy EDR solutions to monitor, detect, and respond to suspicious activities on endpoints.
- Segment the network to limit the spread of malware and protect critical assets.

- Use tools that perform behavioral analysis to detect anomalies that may indicate the presence of custom malware.
- Implement application whitelisting to allow only approved software to run on the network.
- Stay updated with threat intelligence feeds to identify and defend against emerging malware threats.
- Perform regular backups and ensure they are stored securely to facilitate recovery in case of an attack.
- Implement MFA to add an extra layer of security, making it more difficult for attackers to gain unauthorized access.
- Use policies to restrict the execution of scripts (e.g., PowerShell, WScript, CScript) to only trusted administrators.
- Regularly audit and monitor the use of legitimate tools and binaries to detect unusual activities.
- Use application control solutions to restrict the use of legitimate tools and binaries that are often exploited by attackers.
- Apply the principle of least privilege, ensuring users and services have the minimum level of access necessary.
- Enforce security policies that limit the execution of potentially dangerous tools and binaries.

REFERENCES

- https://www.bleepingcomputer.com/news/security/black-basta-ransomware-switches-to-more-evasive-custom-malware/
- https://cloud.google.com/blog/topics/threat-intelligence/unc4393-goes-gently-into-silentnight/
- https://www.bleepingcomputer.com/news/security/how-the-fbi-nuked-qakbot-malware-from-infected-windows-pcs/