OPERATIONAL REPORT: BLACKBASTA RANSOMWARE GROUP

DATE: yyyy-mm-dd RECIPIENT: SOC leader ANALYST: Name

EXECUTIVE SUMMARY

- The group started its operation in early 2022 against companies from multiple spheres of activity (including the financial sector)
- Current level of activity: low since the start of 2023
- The group uses a double extortion technique exfiltration and encryption - and targets a network's key assets - servers and hypervisors
- No known victims based in the UAE; the victims are mainly located in the United States of America, Germany and Italy.
- Main initial vectors of infection include vulnerable Internet facing application exploitation, phishing emails and vulnerable remote access exploitation
- The QakBot malware was often used in past attacks

<u>CONTEXT</u>: BlackBasta is a ransomware group that started its operations in April 2022. BlackBasta operators are mainly russian-native speakers as post on Darkweb forums are written in russian. Multipe reports state that the ransomware group is a Ransomware-as-a-Service (RaaS) that recruits affiliates that conduct malicious operations with the BlackBasta encryption payload against a percentage of the paid ransom. The group uses a double extortion technique as it exfiltrates data from the target's network before encrypting the most important assets of a network (servers, virtual environments, storage devices).

OBJECTIVE: financial gain

<u>VICTIMOLOGY:</u> companies from the healthcare, government, financial services, energy, transportation, education and media. Most of the victims are based in the United States of America and Europe.

PUBLICATION SITE:

http://stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gk lffqd.onion/

GROUP PECULIARITIES:

- The final encryption payload is specific to the group as it adds the .basta extension to encrypted files.
- The group has not published any data from victims based in the Commonwelath of Independent States (CIS).
- BlackBasta operators have used the QakBot malware in most of their past operations to deliver the final encryption payload on the target's network.

Analyst assessment: the analyst assesses with a medium level of confidence that BlackBasta ransomware started its operations in April 2022 as the compilation date of the encryption payload is from 2022 and the first victim published on the group's website is from April 2022.

The analyst assesses with low confidence that the groups uses the RaaS model as no recruitment campaigns from the ransomware group has been identified on the Darkweb.

The analyst assesses with a medium level of confidence that the group does not target CIS countries since some operators are russian-native speakers and no data on victims based in CIS countries have been leaked by the group after one year of operation.



II/ MODUS OPERANDI

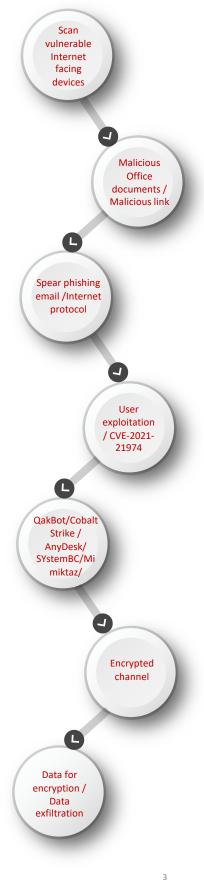
<u>CYBER KILL CHAIN:</u> in past operations, the initial vector of infection was mainly spear phishing emails with a malicious link or an attached document. The attached document usually was an Office document within a password protected archive to evade defenses. After the user execution of the malicious document, the QakBot malware is dropped on the compromised machine. QakBot has information gathering capabilities, persistence capabilities, and additional tool download and execution capabilities.

Once the malicious operator has an initial foothold on the targeted network, he proceeds to do a network discovery with several open source tools including SoftPerfect network scanner, Ntscan, and Cobalt Strike. The next step is usually laterall movement with legitimate remote access tools including AnyDesk and AteraAgent or the Remote Desktop Protocol (RDP) service. While getting access to additional assets, the operator attempts to gain in privileges by dumping password stores using the Mimikatz tool.

After the privilege escalation phase completed, the malicious operator usually creates additional persistence means including creating new accounts on the targeted domain's Active Directory. With domain level privileges, the threat actor is able to access data from contained in key assets including servers and storage devices. The exfiltration phase is usually conducted with legitimate tools including Rclone to exfiltrate data over cloud services and file sharing platforms.

Once the exfiltration phase is completed, the malicious operator proceeds to the encryption phase by executing the final encryption payload responsible for the deletion of the shadow copies and the encryption of files of interest by adding the .basta extension to the encrypted files. Finally, a ransom note is dropped on compromised machines' desktops asking for a ransom.

Analyst assessment: as for other ransomware groups, the initial vector of infection usually is the of a vulnerable exploitation Internet-facing application, a spear-phishing email or the use of compromised valid credentials available for sale in Darkweb. the Patch management, Internet exposure monitoring and credential leak monitoring should be a priority to defend against the BlackBasta ransomware group.



TLP:CLEAR

III/ TOOLS & EXPLOITS

On-the-shelf:

- QakBot: malware mainly delivered through phishing and spear phishing e-mails. The malware is used to steal sensitive information (login credentials and financial information), download additional tools, execute binaries, data exfiltration and C2 communications. Recent campaigns include the delivery of QakBot with malicious OneNote documents.
- Cobalt Strike: attacker-simulating framework used by pentesters and malicious actors
- Mimikatz: tool that allows attackers to dump passwords stored in memory, as well as hashes, PINs and Kereberos tickets.
- **SystemBC**: Remote Access Trojan (RAT) that provides a persistent remote eonnection to attackers after the initial compromise of a machine. The malware can also download and execute additional tools on a compromised machine.

Custom:

 BlackBasta encryption payload: Windows and Linux versions available. One of the first payloads was compiled in February 2022; a VMWare ESXi variant was observed in mid-2022. The payload has several anti analysis techniques including sandboxing environment detections. Once executed, the payload deletes shadow copies, adds the .basta extension to encrypted files and drops a ransom note on the compromised machines. The payload has both full and partial encryption methods to fasten the overall encryption process.

Known exploited vulnerabilities:

- ZeroLogOn (CVE-2020-1472): vulnerability that affects Windows servers and that allows an attacker to bypass authentication and gain administrator-level privileges on a vulnerable machine.
- NoPac (CVE-2021-42287): after having access to a Windows domain Active Directory, this vulnerability allows an attacker to impersonate a domain admin with a reguler user account. Several proof of concepts are available for free on GitHub.
- PrintNightMare (CVE-2021-34527): critical vulnerability disclosed in June 2021 affecting the Zindows Print Spooler service. This vulnerability allows an attacker to execute malicious code with system privileges. An attacker could then install additional tools, view, change or delete data, or create new accounts.
- VMWare ESXi vulnerability (CVE-2021-21974): vulnerability impacting VMWare ESXi products that allow an attacker with an access to the same network segment as an ESXi to conduct remote code execution on the vulnerable machine.



IV/ RECOMMENDATIONS

CYBER KILL CHAIN	RECOMMENDATIONS
Reconnaissance	 Set MFA for remote connexions (VPN) to prevent used of compromised valid credentials Limit Internet exposure to prevent unwanted adversary's scan
Weaponization	• N/A
Delivery	 Set up / Acquire email filtering solutions to limit exposure to phishing attacks
Exploit	 User warning VS phishing attacks Patch management especially for Internet facing applications
Install	• Principle of least privileges ot limit the installation of legitimate remote management tools
C2	 QakBot operatons monitoring Block known C2 infrastructure Data Loss Prevention policy to limit or stop sensible data exfiltration
Actions on Objective	 Backup policy 3:2:1 Segment networks to limit scope of attack Apply Windows Tier Model to manage admin access Patch management to prevent exploitation of CVEs on critical assets like servers hypervisors.



			Supply Chain Compositive Trusted Reautoweahp Valid Accounts	Rennes Services Hardware Additins Presiding Reptaation Through Removable Media	Initial Access Dw+5y Componie Equil MadeAwing AddeAwing AddeAwing AddeAwing AddeAwing
		Wickson Management Interpretation	Schware Depolyment Tools Seystem Seystem Seystem Seystem Seasonal of the set	Comrunidation Native API Bornedued Teac/ceb Shared Modulee	Execution Comment and Screening Hangshead Hangshead Equation for Client Evenation Inter-Process
	Pa-C8 Boot Shaveshel Save Schwa Componet Draftic Signing Signing Kecourts	Bound Receit Service Hack Execution Five Mode Autovolcation Process Office Application Sanap	Create Account Oreate or Modify System Proces Event Triggared Execution	Ausoidat Eukonon Beat ar Logan Ivitiaitzation Seripsa Browaer Edensions Compromise Ciloant Schware Bloary	Persistence Account Mangunation Mangunation Bill States
		Hyaci Bucuton Flow Process Ispection Schoolood Tawala Tawala Vinki	Ekcape to Hoat Event Triggend Execution Deplotation for Ph/Alage Excatation	Autoritat suscition Boot er Soripte Soripte Soripte System Process Domain Policy Modification	Privilege Escalation Acute Evolution Correl Methanism Correl Methanism Acutes Tokan Manipulation
Separa Integra Hanada Sacolar Diseased 2 Manana Integra 2 Manana Person Person Person Casto Anna Casto Anna Repara Dana Repara	Honolar Beneral Levendon Evendon Manguerading Monthy Antones Honolar Monthy Mon	Pla aud Cevectory Vermissions Modification Higo: Generation Flow Tengan Defenses	Doman Puky Modriation Evention Guardialia Exploitation for Deprint Evasion	Debugar Evasion Declara sala Decode Files or Mormation Direct Volume Access	Defense Evasion Avera Evanion Control Machanian Control Machanian Access Tolen Manipulation B173 John
	Server Troby Steve Trees Steve Web Search Cooké Unexand Crockimáte	Multi-Factor Aufertication Network Soffing OS Credential Darges Forgo Auforetication Carrification	hoput Capture Modify Authentication Process Multi-Factor Authentication Herengetion	Pratavoda asoroa Expetitation for Credential Access Forced Authentication Forge Web Credentials	Credential Access Acces
Survey Su	Discovery Overy Registry Renau System Discovery Discovery Overen Mismittion	Soffing Pasaword Paky Discovery Development Development Development Operation Group Discovery	Circup Policy Discovery Network Save Discovery Discovery	Discovery Evaluation Domain Trust Discovery File and Directory Discovery	Discovery Account Dacovery Application Window Discovery Borovers Boolmark
			Schware Deployment Tools Taked Consist Ocraint Shared Auto-Reinnale Auto-Reinnale Maternal	Too Transer Remote Service Secsion Hijadring Aemote Services Replication Through Removable Media	Lateral Movement Espolation of Remote Senicor Internal Spourphishing Lateral
	Irent Cupture Screen Capture Video Capture	Shara form Network Sharad Doke Data form Removable Media Deta Staged Email Collection	Deta Repository Deta from Hichemation Repositories Deta Irom Deta Irom Local System	Automated Collection Browser Seption Hiscking Oligboard Data	Collection Adversaryin-the-Middle Active Collected Data
	Hence vocas Schwar Traffic Sepanicy Web Service	Layer Protocol Nor-Standard Ped Pretocol Turneing Prony	Fatback Crannels Tos/Teaster Tos/Teaster Math:Stago Channels	Data Obluscation Dynamic Resolution Encrypted Channel	Command and Control Application Laye Protocol Communication Proceeding
			Ceritration Over Web Service Schuduled Transfer	Adardative Protocol Over C2 Channel Exitination Over Other Network Medium Editization Over Physical Medium	Exfiltration Automated Editration Dual Transfer Site Lumb Editration Over
		of Service Clockal of Service Resource Frighting Service Stop System Shutdown/Reboot	of Surves of Surves Franket Craption Infort System Recovery	for Inqued Data Manipulation Defacement Disk Wipe	Account Account Account Account Data Data Data Data Data Data Data Da

Annexe 1 – MITRE ATT&CK NAVIGATOR

Analyst assessment	Yara rules		Samples	Last seen	First seen	Kill chain phase	OS and architecture	Capabilities	Malware type	Names		Threat actor name
BlackBasta operatos also use legitimate tools during their attacks including remote management solutions (AnyDesk, AteraAgent, etc.); application blacklisting & whitelisting policies should give defenders a protection against unwanted installation of these legitimate tools by BlackBasta operators.	Available	3ea11f515eb42ed351b3e53855097b35dcf00 744f9b584d81503408b34d3c22 b699bca70cfca8591da0d4 20D03F8272648FA3FD31E22288 b4c542a8fe01aec4d5 a9faf9fd868299b71fb4e34847e 27895d8d3400 e893699d8c2f47abd99f E2220F ba01d539a0fc		Today	2007	Exploit / Install / C2	Windows	Information theft / additional tool download / tool execution / data exfiltration / defense evasion	Trojan	Qbot, PinkSlipbot	QakBot	BlackBasta ransomware
s during their attacks including r defenders a protection against	Available	744f9b584d81503408b34d3c22 27895d8d3400	fdd15df9dc42717a91f94ae508	Today	2012	All	Windows	Information gathering / Persistence / additional tool download and execution / laterlaization / C2	Attack emulation framework	Cobalt Strike	Cobalt Strike	omware
emote management solutio unwanted installation of th	Available	b699bca70cfca8591da0d4 e893699d8c2f47abd99f	5e19e7fc39a959eae012ef	Today	2019	Exploit / Install / C2	Windows	C2 communications / File download & execution / Script execution	RAT	Coroxy	SystemBC	
a operatos also use legitimate tools during their attacks including remote management solutions (AnyDesk, AteraAgent, etc.); application b & whitelisting policies should give defenders a protection against unwanted installation of these legitimate tools by BlackBasta operators.	Available	20D03F8272648FA3FD31E222B8 E2220F		Today	Early 2022	Actions on objective	Windows / Limux / Vmware	Data encryption / anti analysis features	Encryption payload	BlackBasta	BlackBasta encryption payload	
pplication blacklisting operators.	Available	b4c542a8fe01aec4d5 ba01d539a0fc	31eb1de7e840a342f d468e558e5ab627bc	Today	2007	Actions on objective	Windows	Credential data gathering	Password dumper	Mimikatz	Mimikatz	

Annexe 2 – MALWARE CAPABILITIES

Sources

https://www.cybereason.com/blog/cybereason-vs.-black-basta-ransomware

https://www.reliaquest.com/blog/qbot-black-basta-ransomware/

https://github.com/fastfire/deepdarkCTI/blob/main/ransomware_gan g.md

https://www.sentinelone.com/anthology/black-basta/

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

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

https://securityscorecard.com/research/a-deep-dive-into-black-basta-ransomware/

https://www.trellix.com/enus/about/newsroom/stories/research/qakbot-evolves-to-onenotemalware-distribution.html

https://www.fortinet.com/blog/threat-research/cve-2021-42278-cve-2021-42287-from-user-to-domain-admin-60-seconds

https://informer.io/resources/understanding-zerologon-cve-2020-1472

https://www.vmware.com/security/advisories/VMSA-2021-0002.html