Emerging Threats 2024: Black Basta Ransomware

What We've Seen, What's New, and How to Optimize Your Existing Security Tools to Protect Against Black Basta Ransomware



Credential Stuffing. Black Basta. Lockbit 2.0. Dragon Force.

Every week we see news stories about emerging threat actors, campaigns, and techniques targeting by industry, sector, and organization type. But what do these threats actually mean and how can security teams ensure that their security tools are configured optimally to protect against these threats?



Introduction	3
Black Basta Ransomware	4
What is Black Basta Ransomware?	4
What are Black Basta Ransomware's Techniques?	4
Initial Access	5
Discovery and Execution	5
Lateral Movement	5
Privilege Escalation and Lateral Movement	5
Exfiltration and Encryption	6
Black Basta in the News	6
The CISO's Perspective on Black Basta Ransomware	7
Nagomi Notes on Black Basta Ransomware: Main Characteristics and Attack Methods	8
How to Configure CrowdStrike Falcon to Protect Against Black Basta Ransomware	13
Enable Volume Shadow Copy in CrowdStrike Falcon	13
Summary	14



Introduction

There isn't a week that goes by without news of another breach, a new attack method, or an evolving threat. We can say that with confidence since we post a weekly blog post series on the Nagomi blog entitled "<u>This Week in Cybersecurity News</u>." In just the past few weeks, we've seen:

- Windows Quick Assist Anchors Black Basta Ransomware Gambit By Elizabeth Montalbano – DarkReading
- <u>Ransomware gang targets Windows admins via PuTTy, WinSCP malvertising</u> By <u>Lawrence Abrams</u> – BleepingComputer
- <u>Black Basta ransomware group's techniques evolve, as FBI issues new warning</u> in wake of hospital attack By Graham Cluley – Exponentiale Blog

The frequency of attacks aided by the rapid evolution of attack methods make it incredibly difficult for security professionals to stay up-to-date on the threats they face in the wild. Add to that the number of security tools in their environments and their own pace of change (in a good way), and it becomes overwhelming to keep up.

The purpose of this document and its companion webinar and video series is to:

- 1. Highlight emerging threats seen in 2024
- 2. Explain what's new and different about these threats from what we've seen in the past
- 3. Give high level advice about how to protect against these threats
- 4. Suggest granular, tool-specific configuration settings to optimize defenses

We will continue to update this series throughout 2024 as new threats emerge.



Black Basta Ransomware

What is Black Basta Ransomware?

Black Basta (AKA BlackBasta) is a ransomware operator and Ransomware-as-a-Service (RaaS) criminal enterprise that first emerged in early 2022 and immediately became one of the most active RaaS threat actors in the world, racking up 19 prominent enterprise victims and more than 100 confirmed victims in its first few months of operation. Black Basta targets organizations in the US, Japan, Canada, the United Kingdom, Australia, and New Zealand in highly targeted attacks rather than employing a spray-and-pray approach. The group's ransom tactics use a double extortion tactic, encrypting their victim's critical data and vital servers while threatening to publish sensitive data on the group's public leak site.

What are Black Basta Ransomware's Techniques?



From CISA's <u>#StopRansomware: Black Basta</u>

CISA's #StopRansomware: Black Basta advisory shows the high-level techniques used by Black Basta and actions critical infrastructure organizations should take today to mitigate threats from Black Basta.



Initial Access

Black Basta affiliates primarily use spearphishing [<u>T1566</u>] to obtain initial access. According to cybersecurity researchers, affiliates have also used <u>Qakbot</u> during initial access.

Starting in February 2024, Black Basta affiliates began exploiting ConnectWise vulnerability CVE2024-1709 [CWE-288] [T1190]. In some instances, affiliates have been observed abusing valid credentials [T1078].

Discovery and Execution

Black Basta affiliates use tools such as SoftPerfect network scanner (netscan.exe) to conduct network scanning. Cybersecurity researchers have observed affiliates conducting reconnaissance using utilities with innocuous file names such as Intel or Dell, left in the root drive C:\ [T1036].

Lateral Movement

Black Basta affiliates use tools such as BITSAdmin and PsExec, along with Remote Desktop Protocol (RDP), for lateral movement. Some affiliates also use tools like Splashtop, Screen Connect, and Cobalt Strike beacons to assist with remote access and lateral movement.

Privilege Escalation and Lateral Movement

Black Basta affiliates use credential scraping tools like Mimikatz for privilege escalation. According to cybersecurity researchers, Black Basta affiliates have also exploited ZeroLogon (CVE-2020-1472, [CWE-330]), NoPac (CVE-2021-42278 [CWE-20] and CVE-2021-42287 [CWE-269]), and PrintNightmare (CVE-2021-34527, [CWE-269]) vulnerabilities for local and Windows Active Domain privilege escalation [T1068].



Exfiltration and Encryption

Black Basta affiliates use RClone to facilitate data exfiltration prior to encryption. Prior to exfiltration, cybersecurity researchers have observed Black Basta affiliates using PowerShell [T1059.001] to disable antivirus products, and in some instances, deploying a tool called Backstab, designed to disable endpoint detection and response (EDR) tooling [T1562.001]. Once antivirus programs are terminated, a ChaCha20 algorithm with an RSA-4096 public key fully encrypts files [T1486]. A .basta or otherwise random file extension is added to file names and a ransom note titled readme.txt is left on the compromised system. To further inhibit system recovery, affiliates use the vssadmin.exe program to delete volume shadow copies [T1490].

Black Basta in the News

Recent examples include:

- <u>AHA, H-ISAC warn hospitals about Black Basta following Ascension cyberattack</u> (Healthcare IT News)
- CISA and Partners Release Advisory on Black Basta Ransomware (CISA Alert)
- Black Basta Ransomware Hit Over 500 Organizations (SecurityWeek)
- <u>Black Basta ransomware group is imperiling critical infrastructure, groups warn</u> (Ars Technica)

In his <u>article for ars technica</u>, Dan Goodin reported on a new development with Black Basta, crediting research from Rapid7:

Recently, researchers from security firm Rapid7 observed Black Basta using a technique they had never seen before. The end goal was to trick employees from targeted organizations to install malicious software on their systems. On Monday, Rapid7 analysts Tyler McGraw, Thomas Elkins, and Evan McCann reported:

Since late April 2024, Rapid7 identified multiple cases of a novel social engineering campaign. The attacks begin with a group of users in the target environment receiving a large volume of spam emails. In all observed cases, the spam was significant enough to overwhelm the email protection solutions in place and arrived in the user's inbox. Rapid7 determined many of the emails themselves were not malicious, but rather consisted of newsletter sign-up confirmation emails from numerous legitimate organizations across the world.



With the emails sent, and the impacted users struggling to handle the volume of the spam, the threat actor then began to cycle through calling impacted users posing as a member of their organization's IT team reaching out to offer support for their email issues. For each user they called, the threat actor attempted to socially engineer the user into providing remote access to their computer through the use of legitimate remote monitoring and management solutions. In all observed cases, Rapid7 determined initial access was facilitated by either the download and execution of the commonly abused RMM solution AnyDesk, or the built-in Windows remote support utility Quick Assist.

In the event the threat actor's social engineering attempts were unsuccessful in getting a user to provide remote access, Rapid7 observed they immediately moved on to another user who had been targeted with their mass spam emails.

The CISO's Perspective on Black Basta Ransomware

While most ransomware-as-a-service campaigns are similar and use commodity attacks, the merging of malware and social engineering tactics is a powerful combination. By creating a targeted, multi-pronged, bespoke attack that uses research, phone calls, and trust, Black Basta is able to dramatically increase the chance of installing malware on the target's system. Then, by being patient, they are able to operate undetected.

Though security awareness training is necessary and can be effective, this new way of overwhelming an employee's inbox plays on confusion and ultimately makes the end user think "did I do something wrong?" upon seeing droves of newsletter signup emails hitting the inbox simultaneously. And Black Basta is able to leverage the panic with perfect timing, acting as an IT helpdesk employee ready to calm the victim and help them get back to their normal working day.

One of the best ways to take away this new technique's advantage is through clear and simple communication. By letting your employees know that a sudden increase in newsletter signups is the entrance vector for a new attack, they will know to contact the security team and not answer any calls claiming to be there to help.



Nagomi Notes on Black Basta Ransomware: Main Characteristics and Attack Methods

Threats **Overall Threats** Explore By Campaigns BlackCat Ransomware Ū Selected campaigns: Black Basta Ransomware BlackTech ▼ 40 Techniques Hide techniques above 60% 4 **Initial Access** Execution 6 Persistence 4 **External Remote** Windows Server Software 99% 99% 79% Services Management Component Instrumentation 🔄 BlackCat Ransomware BlackCat Ransomware 🖸 BlackCat Ransomware Black Basta Ransomware **Exploit Public-Facing** Create or Modify 75% Application System Process Native API 87% ElackCat Ransomware Black Basta Ransomware BlackTech BlackCat Ransomware Black Basta Ransomware Account Manipulation 99% BlackTech Valid Accounts 84% Black Basta Ransomware 🕒 BlackCat Ransomware Command and 80% Scripting Interpreter Hijack Execution Flow 99% Phishing 77% BlackCat Ransomware Black Basta Ransomware Black Basta Ransomware BlackTech Black Basta Ransomware BlackTech System Services BlackCat Ransomware Black Basta Ransomware

Figure 1 – Kill Chain and Technique Examples

In addition to CISA's advisory notes, Nagomi has published the following on Black Basta and its methods.



BlackBasta has many variants. One of them uses a tool called <u>Backstab</u>, which tries to disable the endpoint detection and response (EDR) software on the endpoint to allow itself to operate more comfortably.

Nagomi associates the relevant defensive capabilities against anti-tampering and malicious driver load attempts with Impair Defenses Mitre Technique (<u>T1562</u>)

88% Impair Defenses	562		×
Adversaries may maliciously modify compo impairing preventative defenses, such as fi malicious behavior. This may also span bot Adversaries may also impair routine operat from being shut down. These restrictions of Adversaries could also target event aggreg	nents of a victim environment in order to rewalls and anti-virus, but also detection i h native defenses as well as supplemental ions that contribute to defensive hygiene, an further enable malicious operations as ation and analysis mechanisms, or otherw	hinder or disable defensive mechanisms. This not only involves capabilities that defenders can use to audit activity and identify capabilities installed by users and administrators. such as blocking users from logging out of a computer or stopping it well as the continued propagation of incidents. ise disrupt these procedures by altering other system components.	 ☑ Magic Hound Turla Tropical Scorplus Helickitty Ransomware Sandworm Team TA505 Gamaredon Group Nascent Ursa Aquatic Panda
owing 2 capabilities		Sort By: Effectiveness 🔻	↑ TA2541
Tamper Protection	14	3 Techniques 3 Techniques 75%	% SolarWinds Compromise Moses Staff
M1040			Kimsuky FIN6
Kernel Mode Protection	-	2 Techniques 1 Test 100% No chan	Mirai Maiware MuddyWater Black Basta Ransomware
M1040			HermeticWiper
			DEARCRY RANSOMWARE

By inspecting the techniques on the Nagomi Platform, customers are able to understand how secure they are against each specific technique and what defensive capabilities are available for them to adjust their posture. They can also browse those capabilities and understand more deeply what actions and features you need to cultivate to become more secure.



Tests (11) Tests Marked as Exception (1)		
Hide tests above 60%		
> 🎸 Anti Tampering Protection - Quarantine for Mac	Advanced	0% ~"NEW
> 🍄 Anti Tampering Protection - Safe-Mode - Block for Windows	Basic	0% ~" NEW
> 🌮 Agent Security - Enable for Mac	Basic 10	0% ~"NEW
> 🤣 Agent Security - Files for Windows	Basic 10	0% ~ [#] NEW
> 🥙 Agent Security - Enable for Windows	Basic 10	0% ~"NEW
> 🌮 Agent Security - Pipe for Windows	Basic 10	D% ~™NEW
> 🍫 Agent Security - Processes for Windows	Basic 10	0% ~ ³ NEW
	Tests (11) Tests Marked as Exception (1) Image: Hide tests above 60% Image: Hide tests above 60% Image: Marked as Exception - Quarantine for Mac Image: Marked as Exception - Quarantine for Mac Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image: Marked as Exception - Safe-Mode - Block for Windows Image	Tests (11) Tests Marked as Exception (1) Image: Hide tests above 60% Image: Anti Tampering Protection - Quarantine for Mac Image: Anti Tampering Protection - Quarantine for Mac Image: Anti Tampering Protection - Safe-Mode - Block for Windows Image: Agent Security - Enable for Mac Image: Ima

Appendix 3 – Tamper Protection

Since cyber threats such as ransomware are always evolving, security vendors are continuously making efforts to keep pace. As such, each company works hard to add new features and new security capabilities. Since new features are usually disabled by default, they are often unused despite offering protection against new threats. As an example, we can take a look at the new Anti-Tamper Protection in Palo-Alto Cortex XDR that was added on March 2023

2020		
October 2023 lune 2023	ENDPOINT SECURITY	
March 2023 Maintenance Releases Hotfix Releases Associated Software and Content Versions Cortex XDR Agent Release Information Known Issues Previous Maintenance Releases	New Behavioral Threat Protection Modules	 To provide you with more detection and protection coverage capabilities, Cortex XDR introduces three new modules, Malicious Device Prevention, UAC Bypass Prevention, and Anti Tampering Protection. Malicious Device Prevention (Windows)—Protects against potentially malicious devices being connected to an endpoint. UAC Bypass Prevention (Windows)—Protects against bypassing UAC mechanisms associated with process privileges elevation. Anti Tampering Protection (Windows and Mac)—Protects against tampering attempts, including modification and/or termination of the Cortex XDR agent. You can select Enabled, Report Only, or Disabled for each module to decide the level of protection.

Figure 4 – Palo-Alto Cortex Releases notes

Nagomi is helping its customers monitor and be aware of all new security features that will help them mitigate the most modern and up-to-date security threats.



"Black Basta affiliates use common initial access techniques—such as phishing and exploiting known vulnerabilities," as CISA mentioned. Again, you can inspect your relevant defenses for "Phishing" and "Exploit Public-Facing Applications" as shown in Figure 1.

The final phase is the impact. Each threat will act differently according to its main purpose. Sometimes, it will exfiltrate data, destroy a critical service, or encrypt files, as is most common for ransomware. Black Basta was designed to encrypt files on the endpoints, but it does so just after deleting volume shadow copies via the 'vssadmin.exe' program. Deleting shadow copies is a common technique ransomware uses to inhibit system recovery.



85% Data Encrypted for Impact TM68	× 67% Backup Access an	d Deletion Prevention
Adversaries my encrypt data on target systems or on large number of systems in a network is interrupt availability and network resources is a decryption level. This yeah attempt to reade strend data inaccessible by encrypting files of data on local and drives and withholding access is a decryption level. This may be done in other to extract movemary compensation from exchange for decryption or a decryption key (ransomwest) or to network data permanently inaccessible in cases when not saved or the anomatic and order on a decryption key (ransomwest) or to network data permanently inaccessible in cases when not saved or the anomatic and order on a decryption key (ransomwest) or to network data permanently inaccessible in cases when not saved or the anomatic and order on some order of data permanently inaccessible in cases when not saved or the adversaries may network by the stand order of the measures, adversaries may encrypt critical system files, disk partition (ransom data) or hydres multiplayers, or otherwise of the measures, adversaries may encrypt critical system files, disk partition data and the target organization, makines decigned for encrypting data may have worm-like features it been files. In some cases, adversaries may encrypt critical system files, disk partition data and and the integrated organization, makines decigned for encrypting data may have worm-like features it been diversary thermal Datacounts, 05 Credential Damping, and SMB/Windo Shaves. Encryption makers are also lowerage internal Datacounts, 05 Credential Damping, and SMB/Windo Shaves. Encryption makers are also lowerage internal Datacounts, 05 Credential Damping, and SMB/Windo Shaves. Encryption makers are also lowerage internal Datacounts, and a changing vicin makers. So the stress (Shave Access and Deletion Prevention and and and adversary the stress (Shave Access and Deletion Prevention and and adversary the stress (Shave Access and Deletion Prevention and adversary to complete attack techniques is a decryptine stress (Shave Access	system note the here is and to first note data s, and the s, and the source states from accessing and erasing your backup data. The safeguards your ability to restore systems and data to their original state, even of a successful cyber attack or data loss incident. The successful cyber attack or data loss incident. The succe	Tests (3) Tests Marked as Exception (0) Hids tests above 60% Volume Shadow Coty - Protect for Windows Volume Shadow Coty - Audit for Windows Back 100% < 40%
Threats		Any Time • 💊 🗟 🛔 🔘 +2
Selected campaigns: 🕃 Lockbit Ransomware 🕃 Royal Ransomware	Black Basta Ransomware 🔹	
3 Discovery 2 Lateral Movement Network Service 13% Discovery 2 Remote Services 76% ⓒ Lockbit Ransomware ⓒ Royal Ransomware Black Basta Ransomware	1 Command And Control 5 Application Layer Protocol 13% C Lockbit Ransomware Royal Ransomware	Exfiltration 1 Impact 3 Exfiltration Over 13% Data Encrypted 85% Stackbit Ransomware Stockbit Ransomware 85% Black Basta Ransomware Black Basta Ransomware
File and Directory 71% Discovery C Royal Ransomware Black Basta Ransomware	Remote Access 13% Software 13%	Data 85% Destruction 85%
	Protocol Tunneling 13% S Lockbit Ransomware Royal Ransomware	Inhibit System Recovery C Lockbit Ransomware Royal Ransomware Black Basta Ransomware
	Encrypted Channel 13% Coval Ransomware Black Basta Ransomware	

Figure 5 – Nagomi Technique Investigation Flow

In the Nagomi Platform, you can see the relevant attacking groups and the threat that is relevant for each technique (left figure) by pressing on it you can see the relevant



defensive capabilities, in this case, are "Backup Access and Deletion Prevention" and "File Encryption Prevention".

Now we'll look at one specific tool and how to ensure the best protection against Black Basta given these defensive capabilities.

How to Configure CrowdStrike Falcon to Protect Against Black Basta Ransomware

Enable Volume Shadow Copy in CrowdStrike Falcon

The Nagomi Proactive Defense Platform gives customers detailed instructions to remediate misconfigurations and measurements to show impact. For the Volume Shadow Copy example in CrowdStrike, Nagomi suggests navigating to your CrowdStrike options, and there on the left pane menu go to:

"Endpoint security" -> "Configure" -> "Prevention policies" -> "Windows policies" and there you should choose your relevant policies.

Inside the policies configuration, navigate to the "Behavior-Based Prevention" Section and make sure to toggle "Volume Shadow Copy—Audit" and "Volume Shadow Copy—Protect".

These configuration settings will aid in preventing malicious actions against your backups.

More than that, it is well recommended to enable other ransomware preventions such as "Backup Deletion", "File Encryption" and "File System Access" to make sure that theCrowdstrike Agent takes action for more malicious ransom attempts.



TYPE Behavior-Based Prevention	category Ransomware		enabled 7	DISABLED O	UNAVAILABLE O		Enable All
Backup Deletion		Cryptowall	File Encr	yption		Locky	
Deletion of backups often indical ransomware activity. File System Access	tive of	A process associated with Cryptowall was blocked.	A proces ransomw	s that created are extension	a file with a known was terminated.	A process determined to be Locky was blocked.	associated with
A process associated with a high system operations typical of rans behavior was terminated.	a volume of file somware	Create an alert when a suspicious process deletes volume shadow copies. Recommended: Use audit mode with a test group to try allowlisting trusted software before turning on Protect.	Prevent : volume s	suspicious pro hadow copies.	ocesses from deleting		
TYPE Behavior-Based Prevention	CATEGORY Exploitation Be	ahavior	enabled 5	DISABLED O	UNAVAILABLE O		Enable All
TYPE Behavior-Based Prevention	CATEGORY Lateral Movem	ent and Credential Access	enabled 2	DISABLED O	UNAVAILABLE O		Enable All
Figure 6 – CrowdStrike Ransomware Preventions							

Summary

While Black Basta isn't new, the group – like other ransomware groups – is evolving its techniques. To meet the challenge, security tools are constantly adding new features and options to protect against these new threats. At Nagomi, we will continue to highlight examples of how security teams can ensure that their existing tools are optimized to combat threats like Black Basta.



About Nagomi Security

Nagomi is changing the way security teams balance risk and defense, empowering customers to focus on what matters now. By mapping customers' existing security tools to the threats that matter and providing prescriptive remediation plans, the Nagomi Proactive Defense Platform finally makes it possible to optimize, measure, and maximize the ROI of security investments. To see a product tour, book a demo, and see why security teams trust Nagomi Security visit <u>nagomi.security</u>

📬 nagomi		
Nagomi Demo US Region	Summary	Any Time • 💫 🖄 🛔 🚺 +2
Summary	Threat Protection Defenses Assessment CISO Board Favorites	
Defenses	Overall Threat Protection Score	ⓒ Top 5 Campaigns You Should Care About ①
Assets	7.970 80% (****15% Explore change 70% 70% Davie 80%	82% BlackCat Ransomware Manufacturing
 Integrations 	Dask. OVA 60% Advanced 73% 50% 50% Image: Sep 25 Oct 16 Nov 06 Nev 27 Det 18 Jan 06 Jan 29 Feb 19 Mar 11 Apr 01 Apr 22 Fibrar Protection Image 74%	Detectes uses upon short on it is need uponetical actual remain
	Explore your Threat Protection → Acknowledged Exceptions Impact	Bit/k Black Basta Ransomware Manufacturing Black Basta, potentially linked to Conti, targets servers using double extention
		85% Lockbit Ransomware
NB	Threat Protection Breakdown	Manufacturing LockBit evolves to encrypt files and demand ransoms via phishing.
Last scan last month	kansomware Phishing	

