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?

nagomi SECURITY

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

nagomi SECURITY

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 "This Week in Cybersecurity News." In just the past few weeks, we've seen:

- Windows Quick Assist Anchors Black Basta Ransomware Gambit By Elizabeth Montalbano – DarkReading
- Ransomware gang targets Windows admins via PuTTy, WinSCP malvertising By Lawrence Abrams – BleepingComputer
- Black Basta ransomware group's techniques evolve, as FBI issues new warning 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?

JOINT CYBERSECURITY ADVISORY

TLP:CLEAR Product ID: AA24-131A

May 10, 2024

Co-Authored by:

MS-ISAC® Multi-State Information Sharing & Analysis Center®

#StopRansomware: Black Basta

SUMMARY

***Note**: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

Actions for critical infrastructure organizations to take today to mitigate cyber threats from ransomware:

- Install updates for operating systems, software, and firmware as soon as they are released.
- Require phishing-resistant MFA for as many services as possible.
- Train users to recognize and report phishing attempts.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Department of Health and Human Services (HHS), and Multi-State Information Sharing and Analysis Center (MS-ISAC) (hereafter referred to as the authoring organizations) are releasing this joint CSA to provide information on Black Basta, a ransomware variant whose actors have encrypted and stolen data from at least 12 out of 16 critical infrastructure sectors, including the Healthcare and Public Health (HPH) Sector.

From CISA's #StopRansomware: Black Basta

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.

nagomi SECURITY

Initial Access

Black Basta affiliates primarily use spearphishing [T1566] to obtain initial access. According to cybersecurity researchers, affiliates have also used Qakbot 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:

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

In his article for ars technica, 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

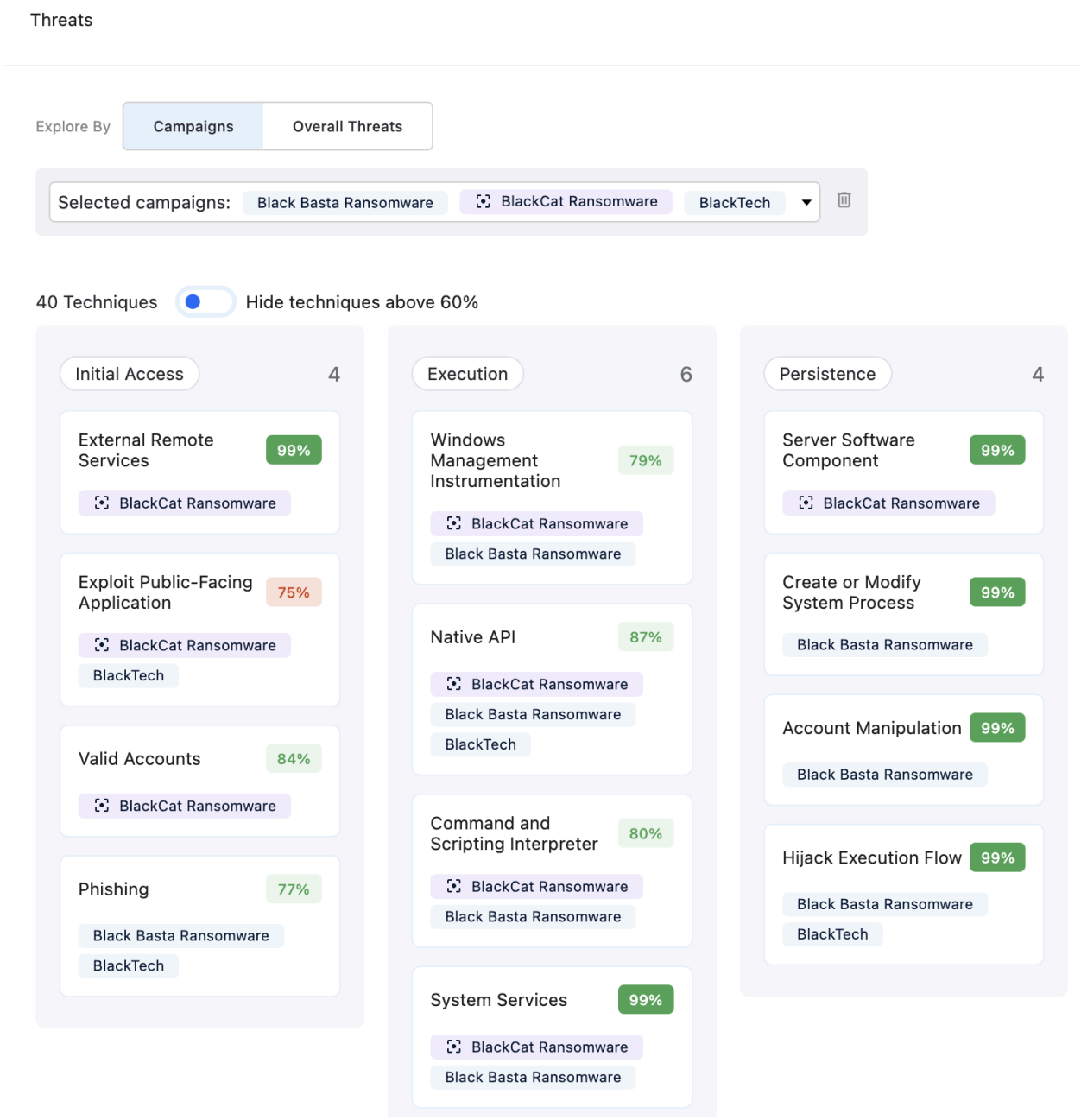


Figure 1 – Kill Chain and Technique Examples

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

nagomi SECURITY

BlackBasta has many variants. One of them uses a tool called Backstab, 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 (T1562)

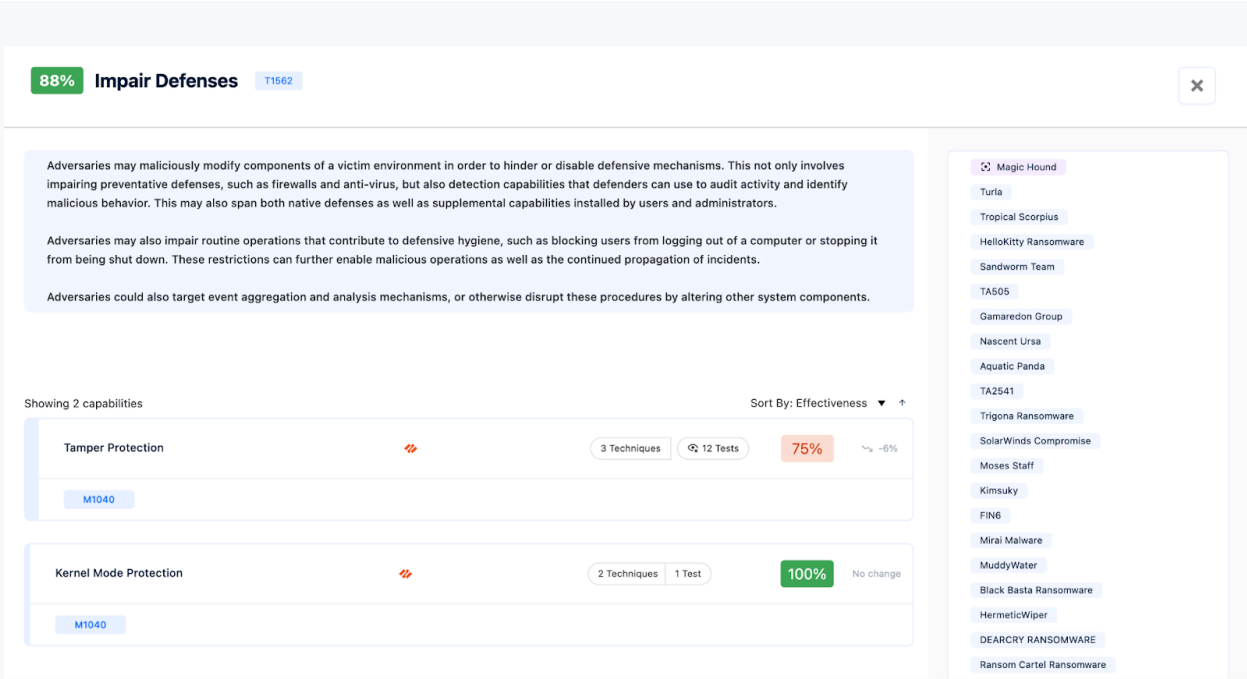
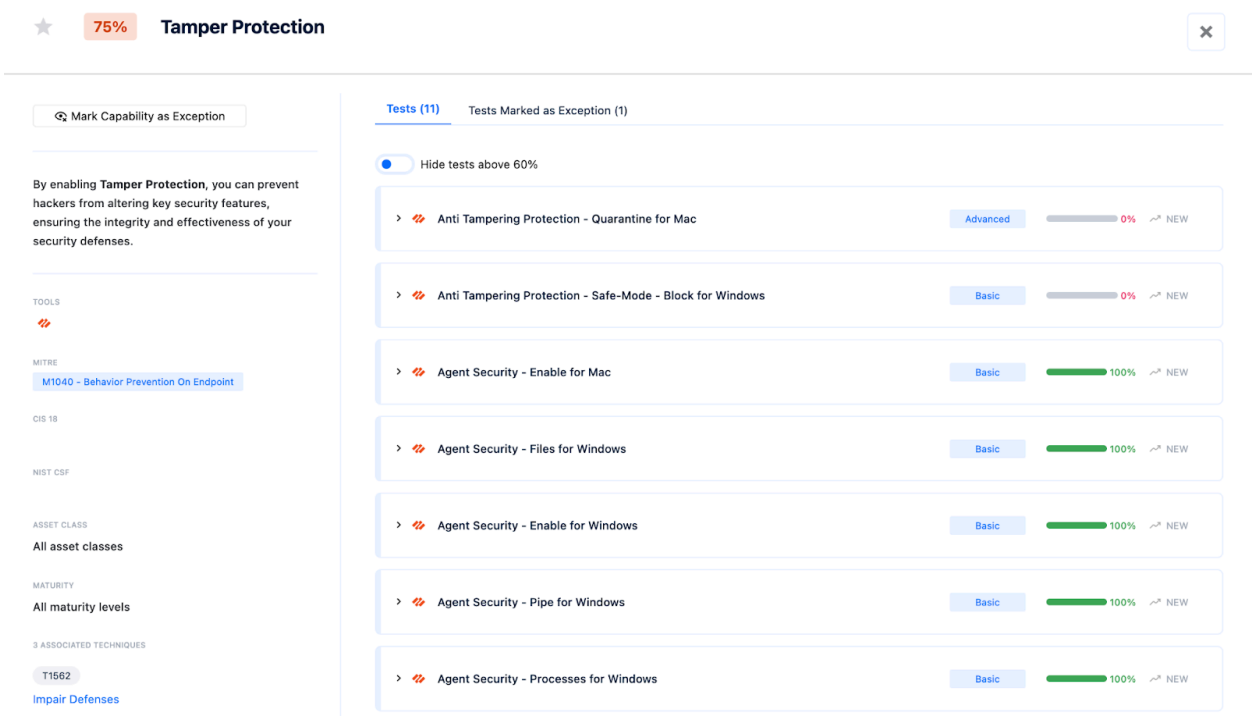


Figure 2 – Impair Defenses Technique on Nagomi Platform

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.



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

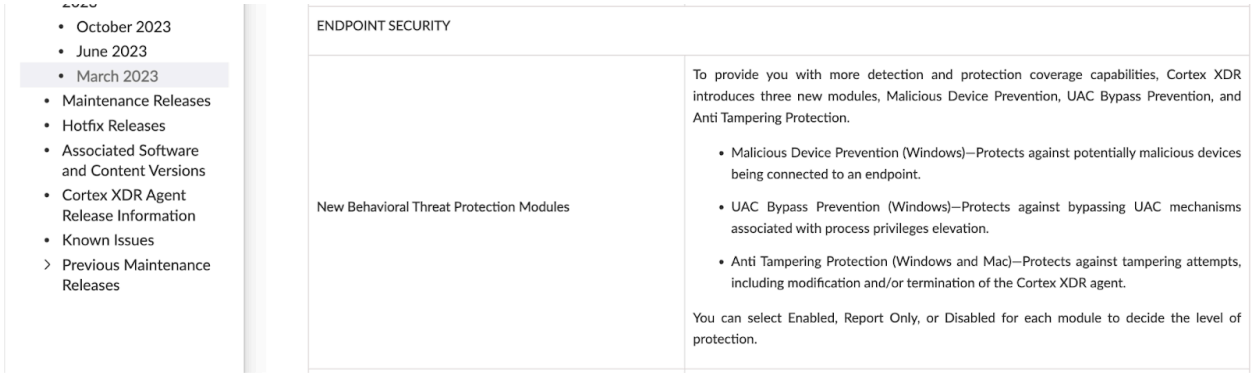


Figure 4 – Palo-Alto Cortex Releases notes

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.

nagomi SECURITY

“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.

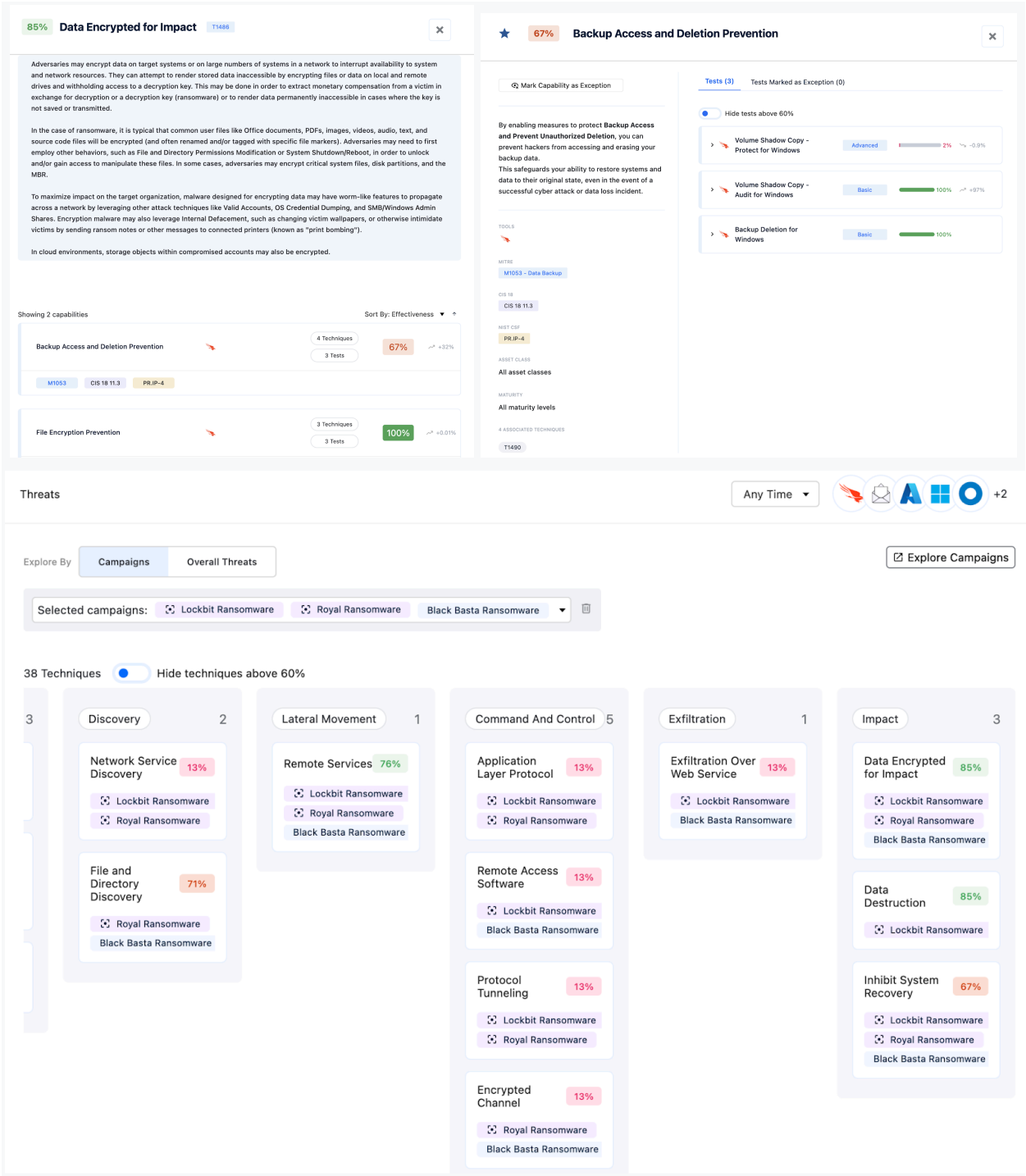


Figure 5 – Nagomi Technique Investigation Flow

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.

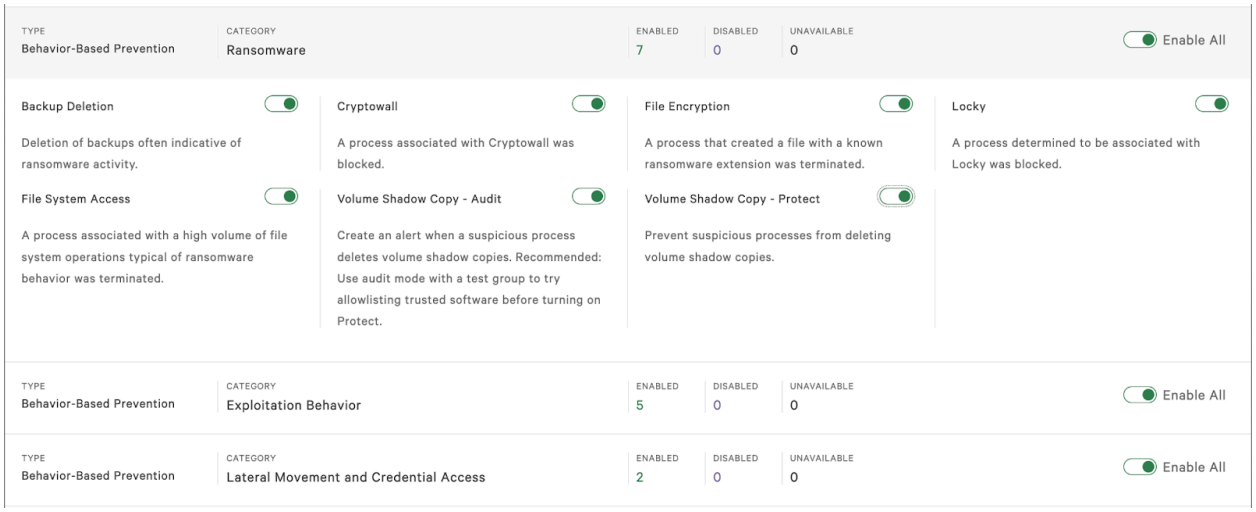


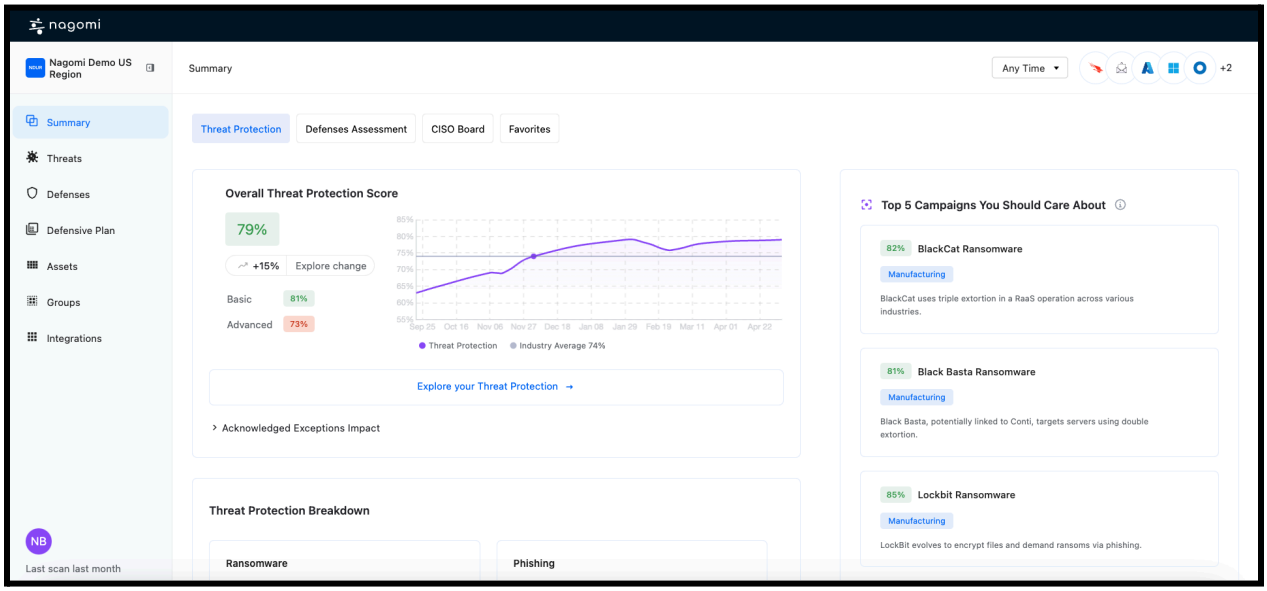
Figure 6 – CrowdStrike Ransomware Preventions

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 nagomi.security



nagomi SECURITY