

# Threat Assessment: Black Basta Ransomware

[unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/](https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/)

Amer Elsad

August 25, 2022

By [Amer Elsad](#)

August 25, 2022 at 12:00 PM

Category: [Ransomware](#), [Threat Briefs and Assessments](#), [Unit 42](#)

Tags: [Black Basta ransomware](#), [threat assessment](#)



This post is also available in: [日本語 \(Japanese\)](#).

## Executive Summary

Black Basta is ransomware as a service (RaaS) that first emerged in April 2022. However, evidence suggests that it has been in development since February. The Black Basta operator(s) use the double extortion technique, meaning that in addition to encrypting files on the systems of targeted organizations and demanding ransom to make decryption possible, they also maintain a dark web leak site where they threaten to post sensitive information if an organization chooses not to pay ransom.

Black Basta affiliates have been very active deploying Black Basta and extorting organizations since the ransomware first emerged. Although the Black Basta affiliates have only been active for the past couple of months, based on the information posted on their leak site, they have compromised over 75 organizations at the time of this publication. Unit 42 has also worked on several Black Basta incident response cases.

The ransomware is written in C++ and impacts both Windows and Linux operating systems. It encrypts users' data using a combination of ChaCha20 and RSA-4096, and to speed up the encryption process, the ransomware encrypts in chunks of 64 bytes, with 128 bytes of data remaining unencrypted between the encrypted regions. The faster the ransomware encrypts, the more systems can potentially be compromised before defenses are triggered. It is a key factor affiliates look for when joining a Ransomware-as-a-Service group.

Palo Alto Networks customers receive help with detection and prevention of Black Basta ransomware through the following products and services: [Cortex XDR](#) and [Next-Generation Firewalls](#) (including [cloud-delivered security services](#) such as [WildFire](#)).

If you think you may have been impacted by a cyber incident, the [Unit 42 Incident Response team](#) is available 24/7/365. You can also take preventative steps by requesting any of our [cyber risk management services](#).

Related Unit 42 Topics [Ransomware](#), [Threat Assessments](#)

## Table of Contents

---

- [Black Basta Overview](#)
- [Technical Details](#)
- [Tactics, Techniques and Procedures](#)
- [Victimology](#)
- [Courses of Action](#)
- [Conclusion](#)
- [Additional Resources](#)

## Black Basta Overview

---

Black Basta is ransomware as a service (RaaS) that leverages [double extortion](#) as part of its attacks. The attackers not only execute ransomware but also exfiltrate sensitive data and threaten to release it publicly if the ransom demands are not met. The threat actors behind the ransomware deploy a name-and-shame approach to their victim, where they use a Tor site, Basta News, to list all of the victims who have not paid the ransom.

Although the Black Basta RaaS has only been active for a couple of months, according to its leak site, it had compromised over 75 organizations at the time of this publication. At least 20 victims were posted to its leak site in the first two weeks of the ransomware's operation, which indicates the group likely is experienced in the ransomware business and has a steady source of initial access.

It is also possible that this is not a new operation but rather a rebrand of a previous ransomware group that brought along their affiliates. Based on multiple similarities in tactics, techniques and procedures (TTPs) - victim-shaming blogs, recovery portals, negotiation tactics, and how quickly Black Basta amassed its victims - that the Black Basta group could include current or former members of the Conti group.

Unit 42 has observed the Black Basta ransomware group using QBot as an initial point of entry and to move laterally in compromised networks. QBot, also known as Qakbot, is a Windows malware strain that started as a banking trojan and evolved into a malware dropper. It has been used by other ransomware groups, including MegaCortex, ProLock, DoppelPaymer and Egregor. While these ransomware groups used QBot for initial access, the Black Basta group was observed using it for both initial access and to spread laterally throughout the network.

Figure 1 below shows the standard attack lifecycle observed with Black Basta ransomware.

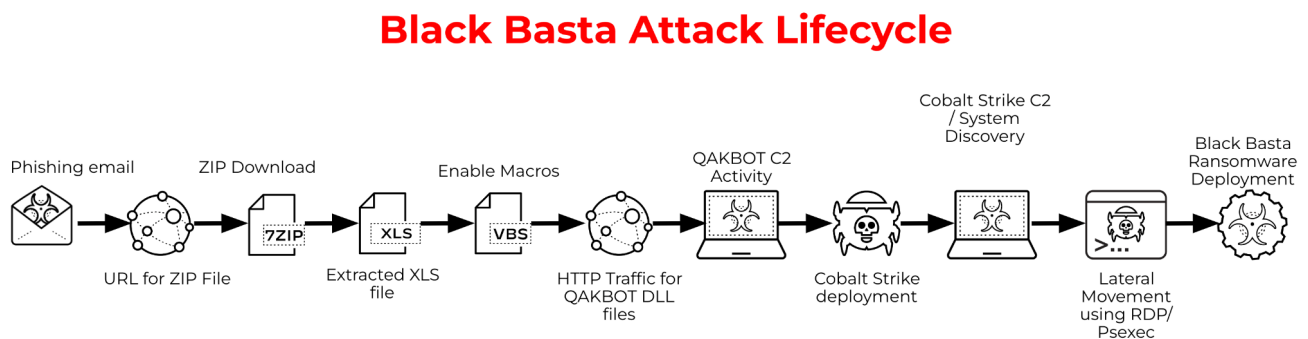


Figure 1. Black Basta attack lifecycle based on Unit 42 incident response cases.

## Technical Details

Black Basta is written in C++ and is cross-platform ransomware that impacts both Windows and Linux systems. In June 2022, a VMware ESXi variant of Black Basta was observed targeting virtual machines running on enterprise Linux servers.

The ransomware includes anti-analysis techniques that attempt to detect code emulation or sandboxing to avoid virtual/analysis machine environments. It also supports the command line argument `-forcepath` that is used to encrypt files in a specified directory. Otherwise, the entire system, except for certain critical directories, is encrypted.

The ransomware spawns a mutex with a string of dsajdhas.0 to ensure a single instance of the malware is running at a time. Then it will iterate through the entire file system, encrypting files with a file extension of .basta.

Black Basta ransomware encrypts users' data through a combination of ChaCha20 and RSA-4096. To speed up the encryption process, the ransomware encrypts in chunks of 64 bytes, with 128 bytes of data remaining unencrypted between the encrypted regions. The ransomware also attempts to delete shadow copies and other backups of files using [vssadmin.exe](#), a command-line tool that manages Volume Shadow Copy Service (VSS), which captures and copies stable images for backups on running systems.

It writes the Random-letters.ico and Random-letters.jpg files to the %TEMP% directory. The .jpg file is leveraged to overwrite the desktop background and appears as follows:

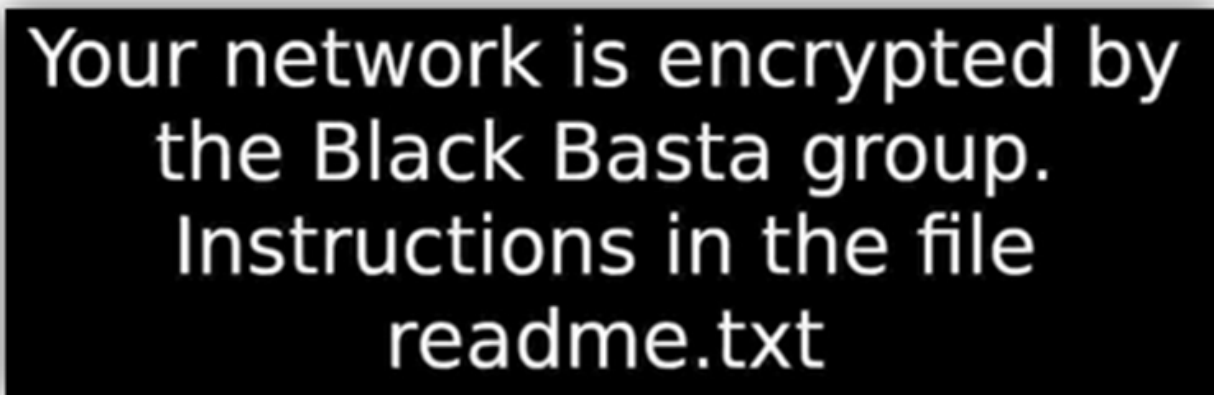


Figure 2. Black Basta desktop wallpaper.

It adds a custom icon to the registry, corresponding to the .basta icon, which is shown in Figure 3.



Figure 3. Black Basta icon.

It will then boot the system in safe mode and proceed to encrypt files. Following successful encryption, the file's extension is changed to .basta and the ransomware will write numerous instances of readme.txt, which contains the following ransom note:

```

*readme.txt - Notepad
File Edit Format View Help
Your data are stolen and encrypted
The data will be published on TOR website if you do not pay the ransom
You can contact us and decrypt one file for free on this TOR site
https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcyvtvolt33s77xyipi7nypxyd.onion/

```

Figure 4. Black Basta ransom note.

## Tactics, Techniques and Procedures

We have observed Black Basta affiliates leveraging the following TTPs:

Tactic / Technique	Notes
<b>TA0001 Initial Access</b>	
T1566.001. Phishing: Spear phishing Attachment	Victims receive spear phishing emails with attached malicious zip files - typically password protected. That contains malicious doc including .doc, .pdf, .xls
<b>TA0002 Execution</b>	
T1569.002. System Services: Service Execution	Black Basta has installed and used PsExec to execute payloads on remote hosts.
T1047. Windows Management Instrumentation	Utilizes Invoke-TotalExec to push out the ransomware binary.
T1059.001. Command and Scripting Interpreter: PowerShell	Black Basta has encoded PowerShell scripts to download additional scripts.
<b>TA0003 Persistence</b>	
T1136. Create Account	Black Basta threat actors created accounts with names such as temp, r, or admin.
T1098. Account Manipulation	Added newly created accounts to the administrators' group to maintain elevated access.
T1543.003. Create or Modify System Process: Windows Service	Creates benign-looking services for the ransomware binary.

---

T1574.001. Hijack Execution Flow: DLL Search Order Hijacking	Black Basta used Qakbot, which has the ability to exploit Windows 7 Calculator to execute malicious payloads.
--	---

---

#### **TA0004 Privilege Escalation**

---

T1484.001. Domain Policy Modification: Group Policy Modification	Black Basta can modify group policy for privilege escalation and defense evasion.
--	---

---

T1574.001. Hijack Execution Flow: DLL Search Order Hijacking	Black Basta used Qakbot, which has the ability to exploit Windows 7 Calculator to execute malicious payloads.
--	---

---

T1543.003. Create or Modify System Process: Windows Service	Creates benign-looking services for the ransomware binary.
---	--

---

#### **TA0005 Defense Evasion**

---

T1484.001. Domain Policy Modification: Group Policy Modification	Black Basta can modify group policy for privilege escalation and defense evasion.
--	---

---

T1218.010. System Binary Proxy Execution: Regsvr32	Black Basta has used regsvr32.exe to execute a malicious DLL.
--	---

---

T1070.004. Indicator Removal on Host: File Deletion	Attempts to delete malicious batch files.
---	---

---

T1112. Modify Registry	Black Basta makes modifications to the Registry.
------------------------	--

---

T1140. Deobfuscate/Decode Files or Information	Initial malicious .zip file bypasses some antivirus detection due to password protection.
--	---

---

T1562.001. Impair Defenses: Disable or Modify Tools	Disables Windows Defender with batch scripts, such as d.bat or defof.bat.
---	---

---

T1562.004. Impair Defenses: Disable or Modify System Firewall	Uses batch scripts, such as rdp.bat or SERVI.bat, to modify the firewall to allow remote administration and RDP.
T1562.009. Impair Defenses: Safe Boot Mode	Uses bcdedit to boot the device in safe mode.
T1574.001. Hijack Execution Flow: DLL Search Order Hijacking	Black Basta used Qakbot, which has the ability to exploit Windows 7 Calculator to execute malicious payloads.
T1622. Debugger Evasion	Uses IsDebuggerPresent to check if processes are being debugged.
<b>TA0006 Credential Access</b>	
T1555. Credentials from Password Stores	Black Basta uses Mimikatz to dump passwords.
<b>TA0007 Discovery</b>	
T1087.002. Account Discovery: Domain Account	Used commands such as net user /domain and net group /domain.
T1016. System Network Configuration Discovery	Lists internal IP addresses to target in C:\Windows\pc_list.txt – typically found on the Domain Controller.
T1082. System Information Discovery	Uses GetComputerName to query the computer name.
T1622. Debugger Evasion	Uses IsDebuggerPresent to check if processes are being debugged.
<b>TA0008 Lateral Movement</b>	
T1021.001. Remote Services: Remote Desktop Protocol	Black Basta has used RDP for lateral movement.
<b>TA0009 Collection</b>	

T1560.001. Archive Collected Data: Archive via Utility	
<b>TA0010 Exfiltration</b>	
T1567. Exfiltration over Web Service	
<b>TA0011 Command and Control</b>	
T1219. Remote Access Software	Black Basta has installed and used legitimate tools such as TeamViewer and AnyConnect on targeted systems.
T1573. Encrypted Channel	Uses Qakbot primarily and Cobalt Strike.
<b>TA0040 Impact</b>	
T1486. Data Encrypted for Impact	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. It encrypts files excluding those with a .exe, .cmd, .bat and .com extension. Uses ChaCha20 or RSA-4096 to encrypt victims.
T1489. Service Stop	Uses sc stop and taskkill to stop services.
T1490. Inhibit System Recovery	Black Basta deletes Volume Shadow Copies using vssadmin.

*Table 1. Tactics, techniques and procedures for Black Basta activity.*

## Victimology

The ransomware group and its affiliate program reportedly compromised multiple large organizations, in sectors including consumer and industrial products; energy, resources and agriculture; manufacturing; utilities; transportation; government agencies; professional services and consulting; and real estate.

Black Basta operators also posted on dark web forums expressing interest in attacking organizations based in Australia, Canada, New Zealand, the U.K. and the U.S. Threat actors using the ransomware impacted organizations based in the U.S., Germany, Switzerland, Italy, France and the Netherlands (listed in descending order by numbers of allegedly breached organizations).



## BlackBasta

Скупаем и берем под реализацию доступы в корп сети таких стран: USA, CA, UK, AU, NZ.

TOX: [REDACTED]

## BlackBasta

We buy and monetize for a share of profits corporate network access credentials from the following countries: the USA, Canada, the UK, Australia, and New Zealand.

TOX: [REDACTED]

Figure 5. Black Basta post on dark web forums.

The threat actor(s) responsible for Black Basta operate a cybercrime marketplace and victim name-and-shame blog. This site is hosted as a Tor hidden service, where the Black Basta ransomware group lists their victims' names, descriptions, percentage of stolen data which has been published, number of visits and any data exfiltrated. There were 75 victims listed on the leak site at the time of writing.

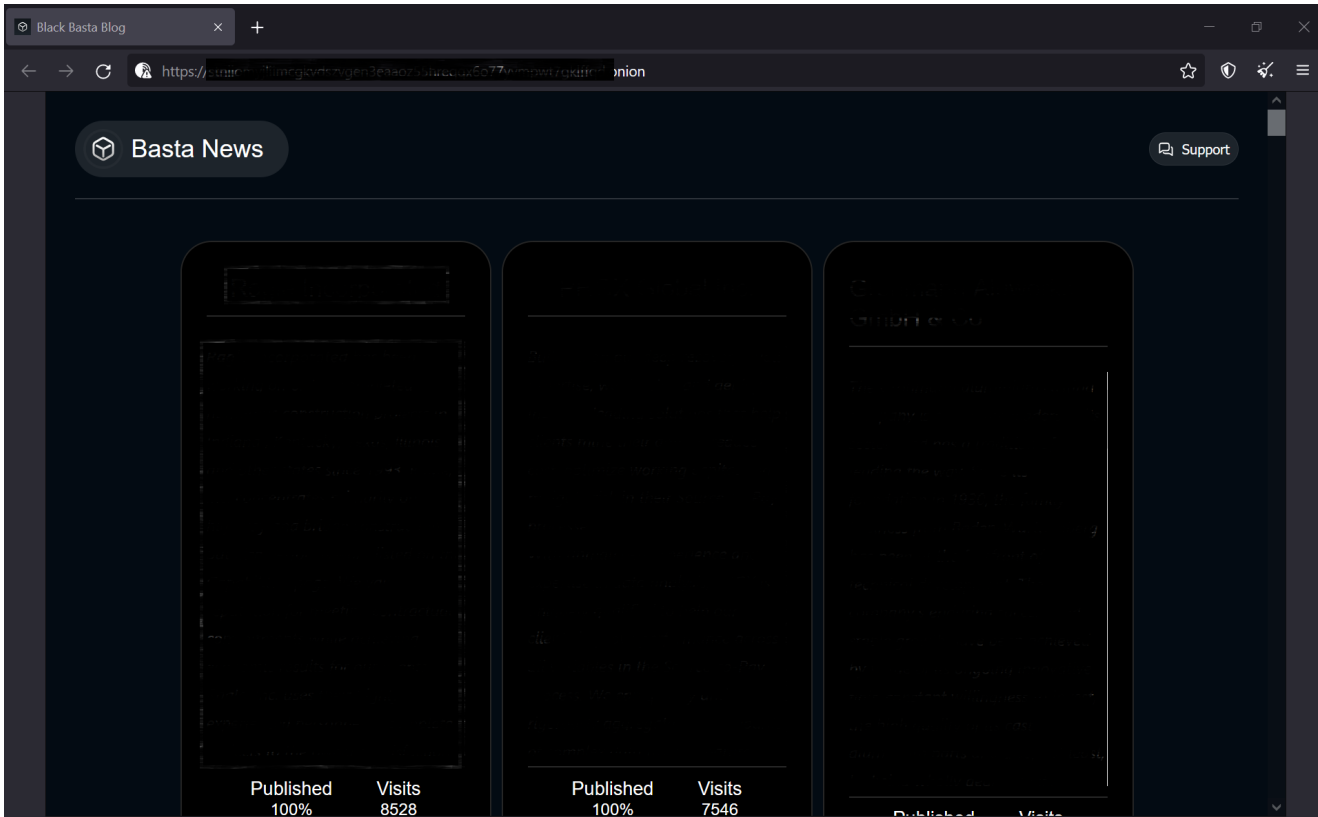


Figure 6. Black Basta News site where the threat actors post allegedly breached organizations (details redacted) and number of visits.

## Courses of Action

Several adversarial techniques were observed in activity associated with Black Basta, and the following measures are suggested within Palo Alto Networks products and services to mitigate threats related to Black Basta ransomware, as well as other malware using similar techniques:

**Product / Service**

**Course of Action**

**Initial Access**

---

The below courses of action mitigate the following techniques:  
Spear Phishing Attachment [[T1566.001](#)]

---

THREAT PREVENTION

Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'

---

Ensure a secure antivirus profile is applied to all relevant security policies

---

NEXT-GENERATION FIREWALLS

Set up File Blocking

---

CORTEX XDR PREVENT

Configure Malware Security Profile

---

CORTEX XSOAR

Deploy XSOAR Playbook – Endpoint Malware Investigation

---

Deploy XSOAR Playbook – Phishing Investigation – Generic V2

---

**Execution**

---

The below courses of action mitigate the following techniques:  
Service Execution [[T1569.002](#)], Windows Management Instrumentation [[T1047](#)], PowerShell [[T1059.001](#)]

---

NEXT-GENERATION FIREWALLS

Ensure remote access capabilities for the User-ID service account are forbidden.

---

Ensure that User-ID is only enabled for internal trusted interfaces

---

Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist

---

Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones

---

---

Ensure that the User-ID service account does not have interactive logon rights

---

Ensure that 'Include/Exclude Networks' is used if User-ID is enabled

---

Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources exists

---

Ensure that the User-ID Agent has minimal permissions if User-ID is enabled

---

Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone

---

CORTEX XDR PREVENT

Configure  
Restrictions  
Security Profile

---

### **Persistence, Privilege Escalation, Defense Evasion**

---

The below courses of action mitigate the following techniques: Create Account [T1136], Account Manipulation [T1098], Regsvr32 [T1218.010], File Deletion [T1070.004], Disable or Modify Tools [T1562.001], Modify Registry [T1112], Deobfuscate/Decode Files or Information [T1140], Disable or Modify System Firewall [T1562.004], Windows Service [T1543.003], DLL Search Order Hijacking [T1574.001], Group Policy Modification [T1484.001]

---

NEXT-GENERATION FIREWALLS

Ensure that the User-ID Agent has minimal permissions if User-ID is enabled

---

Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones

---

Ensure that the User-ID service account does not have interactive logon rights

---

Ensure that 'Include/Exclude Networks' is used if User-ID is enabled

---

Ensure remote access capabilities for the User-ID service account are forbidden.

---

Ensure that User-ID is only enabled for internal trusted interfaces

---

CORTEX XSOAR	Deploy XSOAR Playbook – Access Investigation Playbook
Deploy XSOAR Playbook – Block Account Generic	
Deploy XSOAR Playbook – Impossible Traveler	
CORTEX XDR PREVENT	Configure Host Firewall Profile
Enable Anti-Exploit Protection	
Configure Restrictions Security Profile	
Configure Behavioral Threat Protection under the Malware Security Profile	
Enable Anti-Malware Protection	
<b>Credential Access</b>	
The below courses of action mitigate the following techniques: Credentials from Password Stores <a href="#">[T1555]</a>	
CORTEX XDR	Cortex XDR monitors for behavioral events and files associated with credential access and exfiltration
<b>Discovery</b>	
The below courses of action mitigate the following techniques: System Network Configuration Discovery <a href="#">[T1016]</a> , System Information Discovery <a href="#">[T1082]</a> , Domain Account <a href="#">[T1087.002]</a>	
CORTEX XDR	Cortex XDR monitors for behavioral events along a causality chain to identify discovery behaviors
<b>Lateral Movement</b>	

---

The below courses of action mitigate the following techniques:  
Remote Desktop Protocol [T1021.001]

---

NEXT-GENERATION FIREWALLS

Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist

---

Ensure remote access capabilities for the User-ID service account are forbidden

---

Ensure that the User-ID Agent has minimal permissions if User-ID is enabled

---

Ensure that User-ID is only enabled for internal trusted interfaces

---

Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone

---

Ensure that the User-ID service account does not have interactive logon rights

---

Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned and set to appropriate actions

---

Ensure that 'Include/Exclude Networks' is used if User-ID is enabled

---

Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones

---

Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources exists

---

CORTEX XDR PREVENT

Configure Host Firewall Profile

---

CORTEX XSOAR

Deploy XSOAR Playbook – Access Investigation Playbook

---

Deploy XSOAR Playbook – Block Account Generic

---

**Collection**

---

The below courses of action mitigate the following techniques:  
Archive via Utility [T1560.001]

---

---

CORTEX XDR	Monitors for behavioral events via BIOC's including the creation of zip archives
------------	--

---

### Command and Control

---

The below courses of action mitigate the following techniques:  
Remote Access Software [T1219], Encrypted Channel [T1573]

---

CORTEX XSOAR	Deploy XSOAR Playbook – PAN-OS Query Logs for Indicators
--------------	--

---

Deploy XSOAR Playbook – Block URL

---

Deploy XSOAR Playbook – Block IP

---

NEXT-GENERATION FIREWALLS	Ensure that the Certificate used for Decryption is Trusted
---------------------------	--

---

Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone

---

Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists

---

Ensure 'SSL Forward Proxy Policy' for traffic destined to the Internet is configured

---

Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS

---

Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist

---

THREAT PREVENTION	Ensure DNS sinkholing is configured on all anti-spyware profiles in use
-------------------	---

---

Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use

---

---

Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet

---

Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'

---

Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats

---

Ensure a secure antivirus profile is applied to all relevant security policies

---

## URL FILTERING

Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet

---

Ensure all HTTP Header Logging options are enabled

---

Ensure that PAN-DB URL Filtering is used

---

Ensure that URL Filtering uses the action of 'block' or 'override' on the URL categories

---

Ensure that access to every URL is logged

---

## Impact

The below courses of action mitigate the following techniques: Data Encrypted for Impact [T1486], Service Stop [T1489], Inhibit System Recovery [T1490]

---

## CORTEX XSOAR

Deploy XSOAR Playbook – Ransomware Manual for incident response.

---

Deploy XSOAR Playbook – Palo Alto Networks Endpoint Malware Investigation

---

## Conclusion

Black Basta ransomware operators have been active since at least April 2022. Although their RaaS has only been active for the past couple of months it had compromised at least 75 organizations at the time of this publication. Due to the high-profile nature and steady stream

of Black Basta attacks identified globally in 2022, the operators and/or affiliates behind the service likely will continue to attack and extort organizations.

Palo Alto Networks helps detect and prevent Black Basta ransomware in the following ways:

- WildFire: All known samples are identified as malware.
- Cortex XDR:
  - Identifies indicators associated with Black Basta.
  - Anti-Ransomware Module blocks Black Basta encryption behaviors on Windows.
  - Local Analysis detection for Black Basta binaries on Windows and Linux.
  - Behavioral Threat Prevention prevents Black Basta behaviors.
- Next-Generation Firewalls: DNS Signatures detect the known C2 domains, which are also categorized as malware in Advanced URL Filtering.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call North America Toll-Free: 866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, APAC: +65.6983.8730, or Japan: +81.50.1790.0200.

Indicators of compromise and Black Basta-associated TTPs can be found in the Black Basta ATOM.

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

## Additional Resources

---

**Get updates from  
Palo Alto  
Networks!**

---

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.