Black Basta

[Black Basta](https://attack.mitre.org/software/S1070) is ransomware written in C++ that has been offered within the ransomware-as-a-service (RaaS) model since at least April 2022; there are variants that target Windows and VMWare ESXi servers. [Black Basta](https://attack.mitre.org/software/S1070) operations have included the double extortion technique where in addition to demanding ransom for decrypting the files of targeted organizations the cyber actors also threaten to post sensitive information to a leak site if the ransom is not paid. [Black Basta](https://attack.mitre.org/software/S1070) affiliates have targeted multiple high-value organizations, with the largest number of victims based in the U.S. Based on similarities in TTPs, leak sites, payment sites, and negotiation tactics, security researchers assess the [Black Basta](https://attack.mitre.org/software/S1070) RaaS operators could include current or former members of the [Conti](https://attack.mitre.org/software/S0575) group.(Citation: Palo Alto Networks Black Basta August 2022)(Citation: Deep Instinct Black Basta August 2022)(Citation: Minerva Labs Black Basta May 2022)(Citation: Avertium Black Basta June 2022)(Citation: NCC Group Black Basta June 2022)(Citation: Cyble Black Basta May 2022)

Detail	Value
Category	enterprise-attack
Label	malware
Type	malware
Modified At	2023-05-01T17:05:56.388Z
Created At	2023-03-08T19:14:27.348Z

Attack Tactics(s)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
			Windows Management Instrumentation (T1047)	Launch Daemon (T1543.004)	Launch Daemon (T1543.004)	Time Based Evasion (T1497.003)		System Service Discovery (T1007)					Inhibit System Recovery (T1490)
			Network Device CLI (T1059.008)					Remote System Discovery (T1018)					
			Native API (T1106)					System Information Discovery (T1082)					
								Time Based Evasion (T1497.003)					

Technique(s)

Technique - T1543 - Description

Sub Technique(s)

Detail	Value
ID	T1543
Tactic	undefined
Platforms	Linux, Windows, macOS
Contributors	undefined
Version	1.1
Modified At	undefined
Created At	10 January 2020

ID	SubTechnique
T1543.001	Launch Agent
T1543.002	Systemd Service
T1543.003	Windows Service
T1543.004	Launch Daemon

${detectionDiv}

Mitigations(s)

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system.[5] On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed drivers.[6]
M1028	Operating System Configuration	Ensure that Driver Signature Enforcement is enabled to restrict unsigned drivers from being installed.
M1047	Audit	Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them.
M1022	Restrict File and Directory Permissions	Consider adjusting read and write permissions for NTFS EA, though this should be tested to ensure routine OS operations are not impeded. [24]
M1018	User Account Management	In cloud environments, ensure that users are not granted permissions to create or modify traffic mirrors unless this is explicitly required.
M1045	Code Signing	Require signed binaries.
M1033	Limit Software Installation	Restrict software installation to trusted repositories only and be cautious of orphaned software packages.

Technique - T1543 - Description

Detail	Value
ID	T1543
Tactic	undefined
Platforms	Linux, Windows, macOS

Detail	Value
Contributors	undefined
Version	1.1
Modified At	undefined
Created At	10 January 2020

Sub Technique(s)

ID	SubTechnique
T1543.001	Launch Agent
T1543.002	Systemd Service
T1543.003	Windows Service
T1543.004	Launch Daemon

Detection(s)

ID	Detects	Data Components
DS0012	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.	Script Execution

Mitigations(s)

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system.[5] On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed drivers.[6]
M1028	Operating System Configuration	Ensure that Driver Signature Enforcement is enabled to restrict unsigned drivers from being installed.
M1047	Audit	Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them.
M1022	Restrict File and Directory Permissions	Consider adjusting read and write permissions for NTFS EA, though this should be tested to ensure routine OS operations are not impeded. [24]
M1018	User Account Management	In cloud environments, ensure that users are not granted permissions to create or modify traffic mirrors unless this is explicitly required.
M1045	Code Signing	Require signed binaries.
M1033	Limit Software Installation	Restrict software installation to trusted repositories only and be cautious of orphaned software packages.

Technique - T1490 - Description

Detail	Value
ID	T1490
Tactic	undefined
Platforms	IaaS, Linux, Network, Windows, macOS
Contributors	Austin Clark, @c2defense; Pallavi Sivakumaran, WithSecure; Yonatan Gotlib, Deep Instinct
Version	1.2
Modified At	undefined
Created At	02 April 2019

${detectionDiv}

Mitigations(s)

ID	Mitigation	Description
M1028	Operating System Configuration	Ensure that Driver Signature Enforcement is enabled to restrict unsigned drivers from being installed.
M1018	User Account Management	In cloud environments, ensure that users are not granted permissions to create or modify traffic mirrors unless this is explicitly required.
M1053	Data Backup	Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.[66] Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent

ID	Mitigation	Description
		recovery. In cloud environments, enable versioning on storage objects where possible, and copy backups to other accounts or regions to isolate them from the original copies.[67]

Technique - T1490 - Description

Detail	Value
ID	T1490
Tactic	undefined
Platforms	IaaS, Linux, Network, Windows, macOS
Contributors	Austin Clark, @c2defense; Pallavi Sivakumaran, WithSecure; Yonatan Gotlib, Deep Instinct
Version	1.2
Modified At	undefined
Created At	02 April 2019

Detection(s)

ID	Detects	Data Components
DS0012	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to	Script Execution

ID	Detects	Data Components
	determine their actions and intent.	

Mitigations(s)

ID	Mitigation	Description
M1028	Operating System Configuration	Ensure that Driver Signature Enforcement is enabled to restrict unsigned drivers from being installed.
M1018	User Account Management	In cloud environments, ensure that users are not granted permissions to create or modify traffic mirrors unless this is explicitly required.
M1053	Data Backup	Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.[66] Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery. In cloud environments, enable versioning on storage objects where possible, and copy backups to other accounts or regions to isolate them from the original copies.[67]

Technique - T1018 - Description

Detail	Value
ID	T1018
Tactic	undefined
Platforms	Linux, Network, Windows, macOS
Contributors	Austin Clark, @c2defense; Daniel Stepanic, Elastic; RedHuntLabs, @redhuntlabs
Version	3.4
Modified At	undefined
Created At	31 May 2017

${detectionDiv}

Technique - T1018 - Description

Detail	Value
ID	T1018
Tactic	undefined
Platforms	Linux, Network, Windows, macOS

Detail	Value
Contributors	Austin Clark, @c2defense; Daniel Stepanic, Elastic; RedHuntLabs, @redhuntlabs
Version	3.4
Modified At	undefined
Created At	31 May 2017

Detection(s)

ID	Detects	Data Components
DS0012	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.	Script Execution

Technique - T1007 - Description

Detail	Value
ID	T1007
Tactic	undefined
Platforms	Linux, Windows, macOS
Contributors	Harshal Tupsamudre, Qualys
Version	1.5
Modified At	undefined
Created At	31 May 2017

${detectionDiv}

Technique - T1007 - Description

Detail	Value
ID	T1007
Tactic	undefined
Platforms	Linux, Windows, macOS

Detail	Value
Contributors	Harshal Tupsamudre, Qualys
Version	1.5
Modified At	undefined
Created At	31 May 2017

Detection(s)

ID	Detects	Data Components
DS0012	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.	Script Execution

Technique - T1059 - Description

Detail	Value
ID	T1059
Tactic	undefined
Platforms	Azure AD, Google Workspace, IaaS, Linux, Network, Office 365, Windows, macOS

Detail	Value
Contributors	undefined
Version	2.4
Modified At	undefined
Created At	31 May 2017

Sub Technique(s)

ID	SubTechnique
T1059.001	PowerShell
T1059.002	AppleScript
T1059.003	Windows Command Shell
T1059.004	Unix Shell
T1059.005	Visual Basic
T1059.006	Python
T1059.007	JavaScript
T1059.008	Network Device CLI

ID	SubTechnique
T1059.009	Cloud API

${detectionDiv}

Mitigations(s)

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system.[5] On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed drivers.[6]
M1038	Execution Prevention	Use application control where appropriate.
M1026	Privileged Account Management	Modify Registry settings (directly or using Dcomcnfg.exe) in HKEY_LOCAL_MACHINE\\SOFTWARE\\Classes\\AppID\\{AppID_GUID} associated with the process-wide security of individual COM applications.[21]Modify Registry settings (directly or using Dcomcnfg.exe) in HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Ole associated with system-wide security defaults for all COM applications that do no set their own process-wide security.[22] [23]
M1045	Code Signing	Require signed binaries.
M1021	Restrict Web-Based Content	Web proxies can be used to enforce external network communication policy that prevents use of unauthorized external services.
M1049	Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.
M1042	Disable or Remove Feature or Program	Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.

Technique - T1059 - Description

Detail	Value
ID	T1059
Tactic	undefined
Platforms	Azure AD, Google Workspace, IaaS, Linux, Network, Office 365, Windows, macOS
Contributors	undefined
Version	2.4
Modified At	undefined
Created At	31 May 2017

Sub Technique(s)

ID	SubTechnique
T1059.001	PowerShell
T1059.002	AppleScript
T1059.003	Windows Command Shell
T1059.004	Unix Shell

ID	SubTechnique
T1059.005	Visual Basic
T1059.006	Python
T1059.007	JavaScript
T1059.008	Network Device CLI
T1059.009	Cloud API

Detection(s)

ID	Detects	Data Components
DS0012	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.	Script Execution

Mitigations(s)

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system.[5] On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed drivers.[6]
M1038	Execution Prevention	Use application control where appropriate.

ID	Mitigation	Description
M1026	Privileged Account Management	Modify Registry settings (directly or using Dcomcnfg.exe) in HKEY_LOCAL_MACHINE\\SOFTWARE\\Classes\\AppID\\{AppID_GUID} associated with the process-wide security of individual COM applications.[21]Modify Registry settings (directly or using Dcomcnfg.exe) in HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Ole associated with system-wide security defaults for all COM applications that do no set their own process-wide security.[22] [23]
M1045	Code Signing	Require signed binaries.
M1021	Restrict Web-Based Content	Web proxies can be used to enforce external network communication policy that prevents use of unauthorized external services.
M1049	Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.
M1042	Disable or Remove Feature or Program	Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.

Technique - T1082 - Description

Detail	Value
ID	T1082
Tactic	undefined
Platforms	IaaS, Linux, Network, Windows, macOS
Contributors	Austin Clark, @c2defense; Maril Vernon @shewhohacks; Praetorian
Version	2.5
Modified At	undefined
Created At	31 May 2017

${detectionDiv}

Technique - T1082 - Description

Detail	Value
ID	T1082
Tactic	undefined
Platforms	IaaS, Linux, Network, Windows, macOS

Detail	Value
Contributors	Austin Clark, @c2defense; Maril Vernon @shewhohacks; Praetorian
Version	2.5
Modified At	undefined
Created At	31 May 2017

Detection(s)

ID	Detects	Data Components
DS0012	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.	Script Execution

Technique - T1106 - Description

Detail	Value
ID	T1106
Tactic	undefined
Platforms	Linux, Windows, macOS
Contributors	Gordon Long, Box, Inc., @ethicalhax; Stefan Kanthak
Version	2.1
Modified At	undefined
Created At	31 May 2017

${detectionDiv}

Mitigations(s)

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system.[5] On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed drivers.[6]
M1038	Execution Prevention	Use application control where appropriate.

Technique - T1106 - Description

Detail	Value
ID	T1106
Tactic	undefined
Platforms	Linux, Windows, macOS
Contributors	Gordon Long, Box, Inc., @ethicalhax; Stefan Kanthak
Version	2.1
Modified At	undefined
Created At	31 May 2017

Detection(s)

ID	Detects	Data Components
DS0012	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.	Script Execution

Mitigations(s)

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system.[5] On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed drivers.[6]

ID	Mitigation	Description
M1038	Execution Prevention	Use application control where appropriate.

Technique - T1047 - Description

Detail	Value
ID	T1047
Tactic	undefined
Platforms	Windows
Contributors	@ionstorm
Version	1.3
Modified At	undefined
Created At	31 May 2017

${detectionDiv}

Mitigations(s)

ID	Mitigation	Description
M1040	Behavior Prevention on	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system.[5] On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed drivers.[6]

ID	Mitigation	Description
	Endpoint	
M1038	Execution Prevention	Use application control where appropriate.
M1026	Privileged Account Management	Modify Registry settings (directly or using Dcomcnfg.exe) in HKEY_LOCAL_MACHINE\\SOFTWARE\\Classes\\AppID\\{AppID_GUID} associated with the process-wide security of individual COM applications.[21]Modify Registry settings (directly or using Dcomcnfg.exe) in HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Ole associated with system-wide security defaults for all COM applications that do no set their own process-wide security.[22] [23]
M1018	User Account Management	In cloud environments, ensure that users are not granted permissions to create or modify traffic mirrors unless this is explicitly required.

Technique - T1047 - Description

Detail	Value
ID	T1047
Tactic	undefined
Platforms	Windows
Contributors	@ionstorm
Version	1.3

Detail	Value
Modified At	undefined
Created At	31 May 2017

Detection(s)

ID	Detects	Data Components
DS0012	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.	Script Execution

Mitigations(s)

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system.[5] On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed drivers.[6]
M1038	Execution Prevention	Use application control where appropriate.
M1026	Privileged Account Management	Modify Registry settings (directly or using Dcomcnfg.exe) in HKEY_LOCAL_MACHINE\\SOFTWARE\\Classes\\AppID\\{AppID_GUID} associated with the process-wide security of individual COM applications.[21]Modify Registry settings (directly or using Dcomcnfg.exe) in HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Ole associated with system-wide security defaults for all COM applications that do no set their own process-wide security.[22] [23]

ID	Mitigation	Description
M1018	User Account Management	In cloud environments, ensure that users are not granted permissions to create or modify traffic mirrors unless this is explicitly required.

Technique - T1497 - Description

Detail	Value
ID	T1497
Tactic	undefined
Platforms	Linux, Windows, macOS
Contributors	Deloitte Threat Library Team; Sunny Neo
Version	1.3
Modified At	undefined
Created At	17 April 2019

Sub Technique(s)

ID	SubTechnique
T1497.001	System Checks

ID	SubTechnique
T1497.002	User Activity Based Checks
T1497.003	Time Based Evasion

${detectionDiv}

Technique - T1497 - Description

Detail	Value
ID	T1497
Tactic	undefined
Platforms	Linux, Windows, macOS
Contributors	Deloitte Threat Library Team; Sunny Neo
Version	1.3
Modified At	undefined
Created At	17 April 2019

Sub Technique(s)

ID	SubTechnique
T1497.001	System Checks
T1497.002	User Activity Based Checks
T1497.003	Time Based Evasion

Detection(s)

ID	Detects	Data Components
DS0012	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.	Script Execution

IoC

IoC	IoC Type	Threat Type	Malware	Malware Alias	Malware Printable	First Seen	Last Seen	Confidence level	Reference	Tags	Anonymous	Reporter
sha256_hash	payload	win.blackbasta	no_name_software	Black Basta	Black Basta	2022-05-01 20:23:05	-	50	Link	-	0	Virus_Deck
md5_hash	payload	win.blackbasta	no_name_software	Black Basta	Black Basta	2022-10-07	-	50	Link	-	0	Virus_Deck

IoC	IoC Type	Threat Type	Malware	Malware Alias	Malware Printable	First Seen	Last Seen	Confidence level	Reference	Tags	Anonymous	Reporter
						05:04:40						
sha256_hash	payload	win.blackbasta	no_name_software	Black Basta	Black Basta	2022-10-12 17:17:43	-	100	Link	BlackBasta,Ransomware	0	abuse_ch
sha256_hash	payload	win.blackbasta	no_name_software	Black Basta	Black Basta	2022-10-12 17:17:43	-	100	Link	BlackBasta,Ransomware	0	abuse_ch
sha256_hash	payload	win.blackbasta	no_name_software	Black Basta	Black Basta	2022-10-12 17:17:43	-	100	Link	BlackBasta,Ransomware	0	abuse_ch
md5_hash	payload	elf.blackbasta	null	Black Basta	Black Basta	2022-12-01 00:02:34	-	50	Link	-	0	Virus_Deck