Stairwell threat report: Black Basta overview and detection rules

stairwell.com/resources/stairwell-threat-report-black-basta-overview-and-detection-rules/

Research

Written by **Threat Research**at Stairwell

May 15, 2024

Stairwell Threat Team analysis of Black Basta ransomware

The Stairwell Threat Research Team has been closely tracking the recent attacks from the Black Basta ransomware group against the US public health sector. First identified in April of 2022, Black Basta is a ransomware-as-a-service operation that emerged following the collapse of Conti. So far, this ransomware group has impacted hundreds of organizations, from construction to healthcare industries, since the group first emerged in 2022. Common tactics of Black Basta include spear-phishing, malicious PowerShell scripts (utilizing tools and other malware such as Cobalt Strike and Qakbot), and exfiltrating sensitive data.

Black Basta typically leverages double extortion tactics as part of their ransomware operations; this tactic involves attackers first exfiltrating data for potential future extortion, and then encrypting data locally on a target network. Typically, their ransom notes do not contain specifics of the demand – rather, victims are provided with a code and are directed to contact the group through a Tor browser. Victims are usually given between 10 and 12 days to pay the ransom before their data is released on the Black Basta TOR site, Basta News.

The Stairwell team has written the following YARA rules to help organizations detect their presence and take the necessary defensive and proactive measures to try to remediate Black Basta attacks. As Stairwell is based on providing evasion-resistant security capabilities, which is a fundamental principle for our development, we are releasing a number of YARA detection (see below) rules publicly to help organizations stay ahead of the threats posed by Black Basta. Stairwell customers and users can find copies of these rules under the Stairwell Research ruleset.

About Stairwell’s Threat Research Team

The Stairwell Threat Research Team consists of renowned threat researchers, incident responders, and cyber risk experts with the common goal of proactively improving organizations’ cyber defenses against the latest threats. The team continuously explores the threat landscape to uncover and gather the latest threat intelligence from around the globe. The findings from the Stairwell Threat Research Team are integrated into the Stairwell solution and often shared with the larger cybersecurity community.

YARA rules

```
rule BlackBasta_Ransomware_chat_site
{
  meta:
    author = "Stairwell Research Team"
    description = "Detection for the ransom chat site URL for BlackBasta ransomware"
    hash = "7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a"
    version = "0.1"
  strings:
    $ = "aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion"
  condition:
    all of them
}
```

```
rule BlackBasta_Ransomware_note
{
  meta:
    author = "Stairwell Research Team"
    description = "Detection for the ransom note in BlackBasta ransomware"
    hash = "7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a"
    version = "0.1"
  strings:
    $ = "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"
    $ = "(you should download and install TOR browser first https://torproject.org)"
    $ = "https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion:80/"
    $ = "Your company id for log in: "
  condition:
    5 of them
}

rule BlackBasta_Ransomware2
{
  meta:
    author= "Stairwell Research Team"
    description = "Detection for BlackBasta Ransomware"
    hash = "7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a"
    version = "0.1"
  strings:
    $ = "Done time: %.4f seconds, encrypted: %.4f gb"
    $ = "ERRRROR with file "
    $ = "C:\\Windows\\SysNative\\vssadmin.exe delete shadows /all /quiet"
    $ = "C:\\Windows\\System32\\vssadmin.exe delete shadows /all /quiet"
    $ = "Error 755: "
    $ = "%b %d %H : %M : %S %Y"
  condition:
    5 of them
}
```

```
rule BlackBasta_Ransomware {
  meta:
    author = "Stairwell Research Team"
    date = "2024-05-14"
    description = "Black Basta"
    hash_001 = "203d2807df6ef531efbec7bfd109986de3e23df64c01ea4e337cbe5ba675248b"
    hash_002 = "affcb453760dbc48b39f8d4defbcc4fc65d00df6fae395ee27f031c1833abada"
    hash_003 = "449d87ca461823bb85c18102605e23997012b522c4272465092e923802a745e9"
    hash_004 = "ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e"
    hash_005 = "50f45122fdd5f8ca05668a385a734a278aa126ded185c3377f6af388c41788cb"
    hash_006 = "7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a"
    hash_007 = "d1949c75e7cb8e57f52e714728817ce323f6980c8c09e161c9e54a1e72777c13"
    hash_008 = "a54fef5fe2af58f5bd75c3af44f1fba22b721f34406c5963b19c5376ab278cd1"
    hash_009 = "cce74c82a718be7484abf7c51011793f2717cfb2068c92aa35416a93cbd13cfa"
    hash_010 = "d943a4aabd76582218fd1a9a0a77b2f6a6715b198f9994f0feae6f249b40fdf9"
    hash_011 = "dc56a30c0082145ad5639de443732e55dd895a5f0254644d1b1ec1b9457f04ff"
  strings:
    $a_0 = "(you should download and install TOR browser first
https://torproject.org)"  ascii
    $a_1 = "The data will be published on TOR website if you do not pay the ransom"
ascii
    $a_2 = "You can contact us and decrypt one file for free on this TOR site"  ascii
    $a_3 = "C:\\Windows\\SysNative\\vssadmin.exe delete shadows /all /quiet"  ascii
    $a_4 = "C:\\Windows\\System32\\vssadmin.exe delete shadows /all /quiet"  ascii
    $a_5 = "mpz_powm: Negative exponent and non-invertible base."  ascii
    $a_6 = ".?AVfilesystem_error@filesystem@ghc@@"  ascii
    $a_7 = "Your data are stolen and encrypted"  ascii
    $a_8 = "serviceHub.testWindowstorehost.exe"  wide ascii
    $a_9 = "serviceHub.dataWarehouseHost.exe"  wide ascii
    $a_10 = "serviceHub.vsdetouredhost.exe"  wide ascii
    $a_11 = "mpz_import: Nails not supported."  ascii
    $a_12 = "mpz_div_qr: Divide by zero."  ascii
    $a_13 = "serviceHub.host.clr.x64.exe"  wide ascii
    $a_14 = "serviceHub.host.clr.exe"  wide ascii
    $a_15 = "brokerinfrastructure"  wide
    $a_16 = "mpz_powm: Zero modulo."  ascii
    $a_17 = "vsdebugconsole.exe"  wide ascii
    $a_18 = "dlaksjdoiwq.jpg"  wide
    $a_19 = "comsysapp"  wide
    $a_20 = "vctip.exe"  wide ascii
    $a_21 = "rOVdVGrd]d"  ascii
    $a_22 = "\"\"\"\"\"\"\"\"\"\"\"\"\"\"\":33333C3kf"  ascii
    $a_23 = "GIMP built-in sRG"  wide
    $a_24 = "6acspAPPL"  ascii
    $a_25 = "lkXKg'9Kf"  ascii
    $a_26 = " !AQaq0p@"  ascii
    $a_27 = " !0Ap@`\"P"  ascii
    $a_28 = "V&kg(zHT"  ascii
    $a_29 = ".basta" wide fullword
    $a_30 = "dlaksjdoiwq.jpg" wide fullword
    $a_31 = "fkdjsadasd.ico" wide fullword
    $a_32 = "readme.txt" wide fullword
    $a_33 = ".onion"

    $c_2 = "Done time: %.4f seconds, encrypted: %.4f gb"  wide ascii
    $c_3 = "ERRRRRRRROr"  ascii
    $c_4 = "Error 755: "  ascii

  condition:
    8 of them
}

rule Blackbasta_linux {
  meta:
    author = "Stairwell Research Team"
    date = "2024-05-15"
    description = "Linux Black Basta"
    hash_001 = "0d6c3de5aebbbe85939d7588150edf7b7bdc712fceb6a83d79e65b6f79bfc2ef"
    hash_002 = "96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be"
    hash_003 = "41b3d0d4419eac75017e76fe3bd76ec6a968cb68af4cf6335a27a196c47bac25"
    hash_004 = "1dff5e105493decfaa275720a822fadc57cca073f0d7eb3a11ad9efbb306985d"
    hash_005 = "d144b61c0626989039aa5eb56bd7d276a22959aeb19d1610cd35359a2ee85dc1"
    strings:
    $a_1 = "(you should download and install TOR browser first
https://torproject.org)"  ascii
    $a_2 = "The data will be published on TOR website if you do not pay the ransom"
ascii
    $a_3 = "https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion/"
ascii
    $a_4 = "You can contact us and decrypt one file for free on this TOR site"  ascii
    $a_5 = "mpz_rootrem: Negative argument, with even root."  ascii
    $a_6 = "Your data are stolen and encrypted"  ascii
    $a_7 = "C:/Users/dssd/Desktop/src"  ascii
    $a_8 = "CandiesPlus.cpp"  ascii
    $a_9 = "lockedWallpaper"  ascii
    $a_10 = "forcedPath"  ascii
    $a_11 = "/vmfs/volumes"  ascii

    $b_1 = "Done time: %.4f seconds, encrypted: %.4f gb"  ascii
    $b_2 = "Your company id for log in: "  ascii

  condition:
    uint32(0) == 1179403647 and 8 of them
}
```

```
rule Blackbasta_note
{
  meta:
    author="Stairwell Research Team"
    date="2024-05-14"
    description="Black Basta ransom note rule"
    hash="7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a"
    hash="8dacc4d09d9c9cfd16b98f215b9925f8e741b51dc49fe2af3d705760a73189fe"
    hash="15cd31ba6bd53f177ef700e93333e093d6ece9eece16848bee7b33eb267d4ee2"
    hash="ce180470d48a569c1f87fbfee0cf41b9842a1f69eb040f437bb90e06c7040b82"
  strings:
    $a1 = "You can contact us and decrypt one file for free on these TOR sites"
    $a2 = "Decryption ID: "
    $a3 = "The data will be published on TOR website "
    $a4 = "Your data are stolen and encrypted"
    $a5 = "Your company id for log in: "
    $a6 = "(you should download and install TOR browser first
https://torproject.org)"
    $a7 = "The data will be published on TOR website if you do not pay the ransom"
  condition:
    4 of them
}
```

Recommended reading