Quorum Cyber

Threat Intelligence Black Basta Ransomware

TLP Status: White

Prepared by: Jack Alexander

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version		Date	Summary of Changes
0.1		01/02/2023	Initial Report
1.0		13/04/2023	Final PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
-	-	-

Black Basta Ransomware

Overview

Target Industry: During the first half of 2022, Black Basta targeted a diverse range of private sectors, including: construction, professional services, fashion, materials, manufacturing, transportation, finance, retail and media. The diversity of targets suggest that all sectors are likely to be targets in the future.

Severity Level: High - Compromise by Black Basta ransomware will almost certainly result in the encryption and theft of sensitive data and the attempt to leverage to extort the victim for financial gain.

First seen used in the wild back in April 2022, Black Basta is a ransomware gang that operates a ransomware strain of the same name and generates financial income via their own exploitations, and by selling their product as a Ransomware as a Service (RaaS) model. RaaS allows malicious users, with no indigenous tooling or infrastructure, to exploit their chosen targets by renting a Black Basta licence to use in attacks. Little is known about the exact pricing of Black Basta, but most RaaS gangs price licences based on the perceived value of the intended target. Other RaaS licences have previously been distributed for as little as US$100.

Black Basta is growing in popularity and can often be found on intelligence vendors' trending pages. The gang mostly targets victims in English speaking countries, such as the UK, the US, Australia, Canada and New Zealand. However, other West European countries also appear to be high on the targeting profile.

The ransomware is written in C++ and affects both Windows and Linux operating systems and encrypts data within target systems as fast as possible, in segments of 64 and 128 bytes. The aim of fast encryption is to attempt to compromise as much data as possible before defences are triggered that will alert the user.

The main method of initial compromise for Black Basta ransomware is through spear phishing campaigns.

Impact

Successful system exploitation via Black Basta will almost certainly result in the compromise of confidentiality, availability and integrity of sensitive data and the subsequent exposure of the victim to extortion attempts and negative reputational impact. In a recent ransomware attack against Pendragon, a ransom of $60M (£53M) was demanded, a sum that could soon be an average quantity, depending on the perceived net worth of the target victim.

Should the ransom threat be declined by the victim, then the threat actor will likely publish the encrypted data on dark web forums for other parties to view. This will result in a loss of company reputation and potential legal damages.

Vulnerability Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide additional protection against ransomware threats such as Black Basta. EDRs can alert system users of potential breaches and prevent further progress prior to the malware causing significant damage.

If an EDR solution is not being used, the first instance of detection is likely to be the ransom note. The note will be labelled as:

- Readme.txt

Affected Products

- Windows OS
- Linux OS and Linux based VMware

Containment, Mitigations & Remediations

It is recommended that employees receive training on how to detect markers of spear phishing emails. The main method of initial compromise implemented by the Black Basta ransomware gang is spear phishing. Therefore, in-house training will prove to reduce the effectiveness of potential future campaigns.

As stated above, one main method of reducing the threat of Black Basta ransomware is to detect it in the early stages using an effective and monitored EDR solution. An effective EDR tool will increase detection of malicious attempts of ransomware compromise and halt them if detected.

Organisations can also perform routine back-ups of sensitive data that is required to operate business affairs. It is also advised that an offline copy is retained, in the event that back-ups are impacted by the attack. Therefore, if a breach occurs and the business can no longer function, a back-up is ready to use, and the business can continue to operate with minimal disruption. However, this does not nullify the fact that customer and employee data may have also been lost, and potentially released at will by the threat actor if ransom demands are not met.

Indicators of Compromise

Black Basta Associated File Hashes (SHA-256):

- 17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90
- 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa
- 7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a
- ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e
- 96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be
- a54fef5fe2af58f5bd75c3af44f1fba22b721f34406c5963b19c5376ab278cd1
- 1d040540c3c2ed8f73e04c578e7fb96d0b47d858bbb67e9b39ec2f4674b04250
- f088e6944b2632bb7c93fa3c7ba1707914c05c00f9491e033f78a709d65d7cff
- 2967e1d97d32605fc5ace49a10828800fbbefcc1e010f6004a9c88ef3ecdad88
- ac49c114ef137cc198786ad8daefa9cfcc01f0c0a827b0e2b927a7edd0fca8b0

Black Basta Associated File Hashes (MD-5):

- 8917af3878fa49fe4ec930230b881ff0ae8d19c9
- a996ccd0d58125bf299e89f4c03ff37afdab33fc
- 5f99214d68883e91f586e85d8db96deda5ca54af
- eb43350337138f2a77593c79cee1439217d02957
- 920fe42b1bd69804080f904f0426ed784a8ebbc2
- 14177730443c70aefeeda3162b324fdedf9cf9e0

Associated Black Basta IP Address:

- 23[.]106[.]160[.]188

Files Created:

- %Temp%\fkdjsadasd.ico
- %Temp%\dlaksjdoiwq.jpg

Processes Spawned:

- cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet
- cmd.exe /c C:\Windows\System32\vssadmin.exe delete shadows /all /quiet

Registry Key Created:

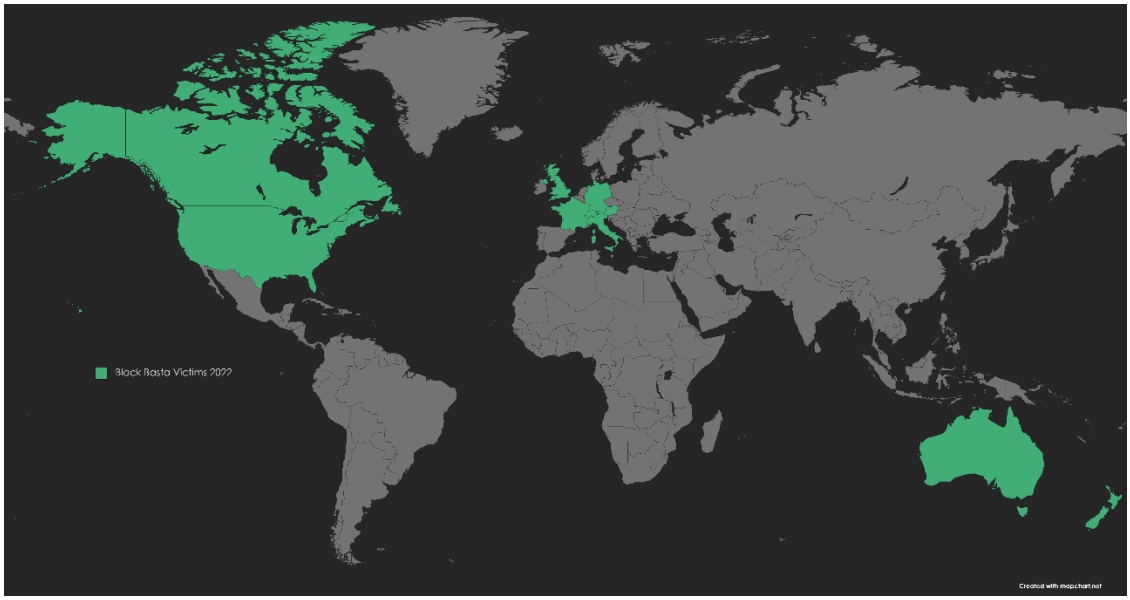
- HKEY_CLASSES_ROOT.basta

Threat Landscape

Ransomware continues to be one of the prominent threats facing the private sector. The recent attack against automotive retailer Pendragon, and the record-breaking demand of £53 million, suggests that the threat is growing as criminal groups are becoming comfortable demanding ever-increasing ransom quantities.

Open-source reporting suggests that the Black Basta ransomware strain was the third most used ransomware variant in October 2022. There is a realistic possibility that this growth will continue, and the ransomware will be seen in a greater number of attack efforts.

Previous attacks have predominantly been focused against western companies. However, there is insufficient evidence to suggest the specific motivations of western targeting.



Threat Group

The Black Basta ransomware gang operates via a double extortion technique. This means that not only does the group encrypt the confidential data of the victim and demand a ransom for the keys, but they also threaten victims with the publishing of the data on their own dark web site. This is likely designed to increase pressure on the victim and increase the possibility of payment.

Despite the group's relatively recent formation, it is highly likely that it is composed of experienced cyber criminals who have experience with ransomware extortion tactics. This would be due to the fact that the double extortion technique is implemented, as well as the observed significant rise to notoriety.

Mitre Methodologies

Initial Access
T1078 - Valid Accounts[1]
T1566.001 - Phishing: Spear-phishing Attachment[2]

Execution
T1059 - Command and Scripting Interpreter[3]
T1047 - Windows Management Instrumentation[4]

Persistence
T1078 - Valid Accounts[5]

Privilege Escalation
T1078 - Valid Accounts[6]

Defence Evasion
T1078 - Valid Accounts[7]
T1112 - Modify Registry[8]
T1027 - Obfuscate Files or Information[9]
T1562.001 - Impair Defences: Disable or Modify Tools[10]

Credential Access
T1003 - OS Credential Dumping[11]

Discovery
T1082 - System Information Discovery[12]

[1] https://attack.mitre.org/techniques/T1078/
[2] https://attack.mitre.org/techniques/T1566/001/
[3] https://attack.mitre.org/techniques/T1059/
[4] https://attack.mitre.org/techniques/T1047/
[5] https://attack.mitre.org/techniques/T1078/
[6] https://attack.mitre.org/techniques/T1078/
[7] https://attack.mitre.org/techniques/T1078/
[8] https://attack.mitre.org/techniques/T1112/
[9] https://attack.mitre.org/techniques/T1027/
[10] https://attack.mitre.org/techniques/T1562/001/
[11] https://attack.mitre.org/techniques/T1003/
[12] https://attack.mitre.org/techniques/T1082/

T1083 - File and Directory Discovery[13]

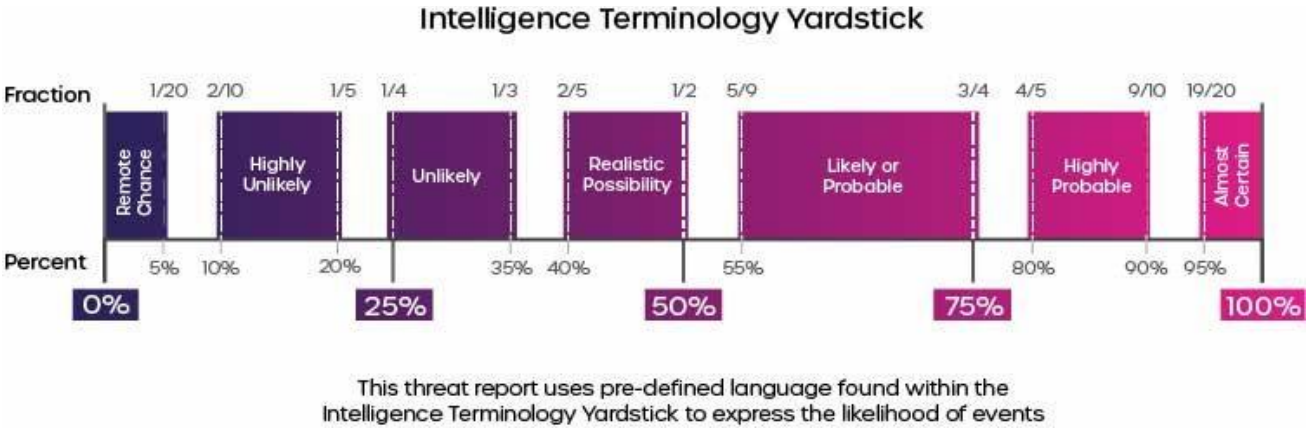
Exfiltration
T1567 - Exfiltration Over Web Service[14]
T1041 - Exfiltration Over C&C Channel[15]

Impact
T1490 - Inhibit System Recovery[16]
T1489 - Service Stop[17]
T1486 - Data Encrypted for Impact[18]

Further Information

- Security Scorecard: Black Basta Deep Dive
- Avertium: Black Basta Deep Dive

Intelligence Cut-off Date (ICoD): 15/02/2023 10:00 GMT



[13] https://attack.mitre.org/techniques/T1083/

[14] https://attack.mitre.org/techniques/T1567/
[15] https://attack.mitre.org/techniques/T1041/
[16] https://attack.mitre.org/techniques/T1490/
[17] https://attack.mitre.org/techniques/T1489/
[18] https://attack.mitre.org/techniques/T1486/