Quorum Cyber

Threat Intelligence
8Base
Threat Actor Profile

TLP Status: CLEAR

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

Microsoft Solutions Partner

Document Control

Revision History

Version	Date	Summary of Changes
0.1	29/06/2023	Initial Report
1.0	13/10/2023	PDF Formatting

Related Documents

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

Document Name	Date	Version
-	-	-

Threat Actor Profile – 8Base

Overview

8Base is a ransomware group that is reported to have originated from RansomHouse. It is focused on encryption of data and public shaming of organisations by conducting double-extortion ransomware campaigns and threatening to leak stolen data to coerce organisations into paying the ransom. The similarities that exist with RansomHouse mean that there is a realistic possibility that there could be a subsidiary connection.

The group has targeted a wide range of industries, including hospitality, law, healthcare, manufacturing, finance and information technology, with victims located in various countries such as Spain, Italy, the United States, Brazil, Canada, India, France, and the United Kingdom. Although the group has targeted a wide range of industries, the most targeted as of the time of writing has been business services with 17 attacks.

The 8Base ransomware group utilises the 8Base ransomware, SmokeLoader and Phobos. Further, the group operates within the context of the Ransomware-as-a-Service (RaaS) model.

Targeted Sectors

The 8Base ransomware group has targeted a wide range of industry sectors, including hospitality, law, healthcare, manufacturing, finance, and information technology.

Threat Actor Motivations

The 8Base ransomware group has stated on their site that they are "simple pen testers" and focus on targeting organisations that are deemed to be lacking in security maturity as they have "considered their financial gain to be above the interest of their partners / individuals".

Activity Timeline

The following table contains details regarding recent examples of significant 8Base ransomware operations:

Date of Attack	Victim	Assessed Motivation
July 2023	Kansas Medical Center[1]	Highly Likely **Financial**
August 2023	Alberta Dental Service Corp[2]	Highly Likely **Financial**
August 2023	Oregon Sports Medicine[3]	Highly Likely **Financial**

[1] 8Base claims to have stolen patient data and employee info from Kansas Medical Center (databreaches.net)
[2] Canadian dental service pays ransom in 8Base ransomware attack - SiliconANGLE
[3] Oregon Sports Medicine allegedly hit by 8Base threat actors (databreaches.net)

Associated Malware

- **8Base Ransomware:** It is likely that 8Base may be related to the Phobos ransomware group as they share code similarities and use similar file extensions. The malware has been active since at least May 2023. The ransomware strain is loaded via SmokeLoader and uses the '.8base' file extension for encrypted documents.
- **SmokeLoader:** A notorious and highly configurable loader malware that has been active since 2011.Its main objective is to download or load stealthier and more effective malware onto infected systems. It is often distributed through phishing campaigns, malicious documents, and fake pirated software or crack sites. SmokeLoader has been observed delivering various malware families, including ransomware, such as Phobos and 8Base.
- **Phobos Ransomware:** This ransomware variant is able to encrypt a system without access to the internet as the encryption key is hard-coded and uses persistence methods to continue encrypting files in AES-256 with RSA-1024 after the ransom note is created. The ransomware also disables OS processes, recovery mode and firewall.

Indicators of Compromise

8Base Ransomware Group Associated File Hashes (SHA-256):

- e142f4e8eb3fb4323fb377138f53db66e3e6ec9e82930f4b23dd91a5f7bd45d0
- 518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c
- afddec37cdc1d196a1136e2252e925c0dcfe587963069d78775e0f174ae9cfe3
- c6bd5b8e14551eb899bbe4decb6942581d28b2a42b159146bbc28316e6e14a64
- 5ba74a5693f4810a8eb9b9eeb1d69d943cf5bbc46f319a32802c23c7654194b0

8Base Ransomware Group Associated File Hashes (SHA-1):

- 5d0f447f4ccc89d7d79c0565372195240cdfa25f
- 3d2b088a397e9c7e9ad130e178f885feebd9688b

8Base Ransomware Group Associated File Hashes (MD-5):

- 9769c181ecef69544bbb2f974b8c0e10
- 20110ff550a2290c5992a5bb6bb44056

8Base Ransomware Group Associated Domains:

- wlaexfpxrs[.]org
- admhexlogs25[.]xyz
- admlogs25[.]xyz
- admlog2[.]xyz

- dnm777[.]xyz
- serverlogs37[.]xyz
- dexblog[.]xyz
- blogstat355[.]xyz
- blogstatserv25[.]xyz

Mitre Methodologies

Execution
T1204[4] - User Execution

Persistence
T1547.001[5] - Registry Run Keys / Startup Folder
T1098 - Account Manipulation[6]

Defence evasion
T1562.004 [7]- Disable or Modify System Firewall

Collection
T1005 - Data from Local System[8]

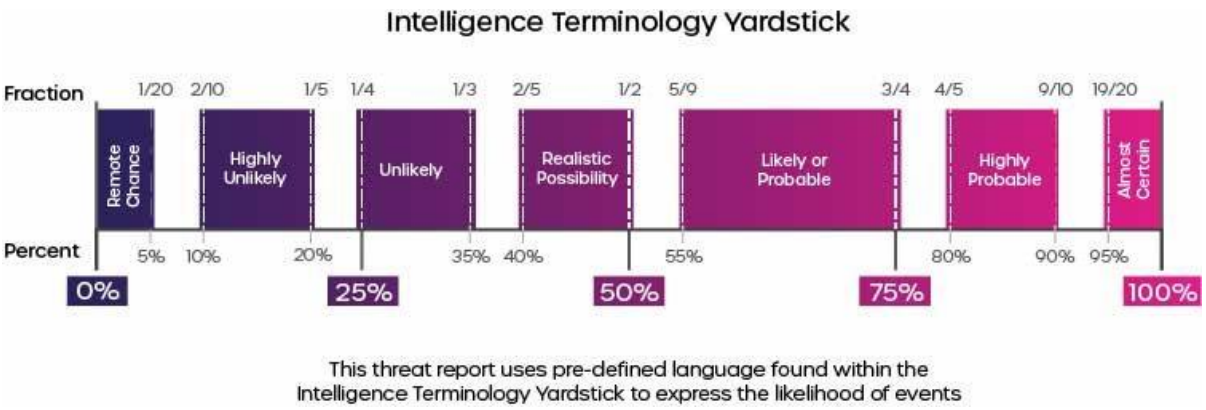
Impact
T1486[9] - Data Encrypted for Impact

Additional Information

- 8Base Ransomware - VMware Security Blog

Intelligence Cut-off Date (ICoD): 12/10/2023, 13:00 UTC

[4] User Execution, Technique T1204 - Enterprise | MITRE ATT&CK®
[5] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[6] Account Manipulation, Technique T1098 - Enterprise | MITRE ATT&CK®
[7] Impair Defenses: Disable or Modify System Firewall, Sub-technique T1562.004 - Enterprise | MITRE ATT&CK®
[8] Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®
[9] Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events