Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

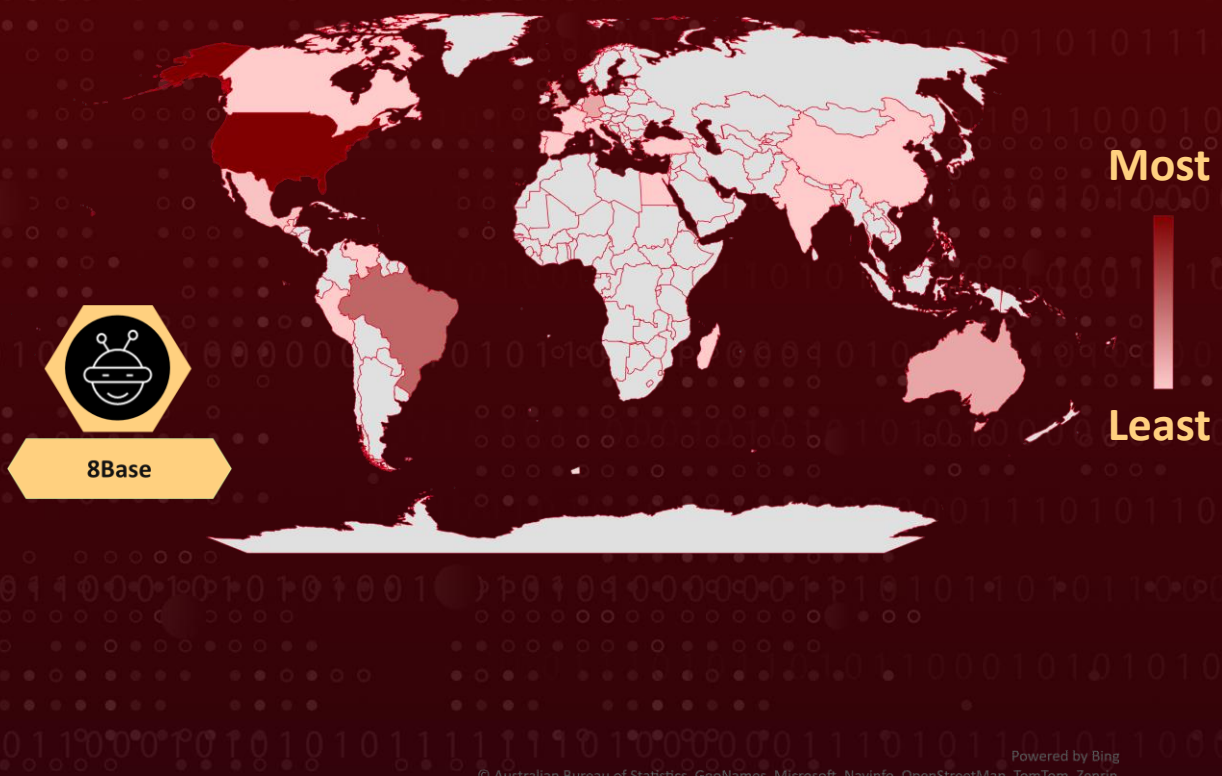
Surge in 8Base Ransomware Group Activity

Date of Publication	Admiralty code	TA Number
July 07, 2023	A1	TA2023289

Summary

First Appearance: March 2022
Actor Name: 8Base
Target Countries: United States, Brazil, Australia, Germany, United Kingdom, Mexico, Portugal, Belgium, Egypt, China, Spain, Madagascar, France, Peru, Canada, Turkey, Guatemala, Venezuela, India, Italy
Target Sectors: Business Services, Finance, Manufacturing, Technology, Healthcare, Real Estate, Construction, Hospitality, Non-Profit, Automotive, Engineering, Food
Actor Details: 8Base Ransomware group define themselves as “honest and simple pentesters” have spiked their activities recently and was observed to be within top 2 performing ransom groups.

Actor Map



Actor Details

#1 The 8Base ransomware group is relatively unknown, their social media accounts dating back to 2014 however, their cyber activity was first observed in March 2022 and has been steadily increasing since then. They have recently gained attention as top performing ransomware groups, ranking second in terms of capturing victims.

#2 They encrypt and exfiltrate Victim data and have started employing name-and-shame technique to compel victims for ransom. The group is resembling some similarity to Ransom House as ransom notes were found to be 99% linguistically similar and leak-site content is also similar.

#3 8Base group uses multiple ransomware strain and seems to be acquiring arsenal from ransomware-as-a-service market. They customize the Ransomware with their branding and recently used a customized version of the Phobos v2.9.1 ransomware, which is loaded via SmokeLoader.

#4 8Base Group created a leak site recently and is active on social medial platform since May. The leak site has a page dedicated to victims and its downloads, a set of rules for negotiating, and will only accept a ransom payment in Bitcoin. employ double-extortion technique. It targets mostly small and medium enterprises.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
8Base	-	United States, Brazil, Australia, Germany, United Kingdom, Mexico, Portugal, Belgium, Egypt, China, Spain, Madagascar, France, Peru, Canada, Turkey, Guatemala, Venezuela, India, Italy	Business Services, Finance, Manufacturing, Technology, Healthcare, Real Estate, Construction, Hospitality, Non-Profit, Automotive, Engineering, Food
	MOTIVE		
	Monetary Gains		

Recommendations

Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. Ransomware groups often exploit known vulnerabilities to gain initial access to systems. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited.

Conduct Regular Data Backups: Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom.

Protect your Backups: Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Invasion	TA0007 Discovery	TA0010 Exfiltration	TA0040 Impact
T1588 Obtain Capabilities	T1588.001 Malware	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1134 Access Token Manipulation	T1134.001 Token Impersonation/ Theft	T1562 Impair Defenses	T1562.001 Disable or Modify Tools
T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1135 Network Share Discovery	T1486 Data Encrypted for Impact
T1490 Inhibit System Recovery	T1561 Disk Wipe		

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	20110FF550A2290C5992A5BB6BB44056, 9769c181ecef69544bbb2f974b8c0e10
SHA1	3D2B088A397E9C7E9AD130E178F885FEEBD9688B, 5d0f447f4ccc89d7d79c0565372195240cdfa25f
SHA256	518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c, 5BA74A5693F4810A8EB9B9EEB1D69D943CF5BBC46F319A32802C23C7654194B0, e142f4e8eb3fb4323fb377138f53db66e3e6ec9e82930f4b23dd91a5f7bd45d0, C6BD5B8E14551EB899BBE4DECB6942581D28B2A42B159146BBC28316E6E14A64, 518544E56E8CCEE401FFA1B0A01A10CE23E49EC21EC441C6C7C3951B01C1B19C, AFDDEC37CDC1D196A1136E2252E925C0DCFE587963069D78775E0F174AE9CFE3,
URL	wlaexfpxrs[.]org, admhexlogs25[.]xyz, admlogs25[.]xyz, admlog2[.]xyz, dnm777[.]xyz, serverlogs37[.]xyz, dexblog[.]xyz, blogstat355[.]xyz, blogstatserv25[.]xyz
File Name	9f1a.exe, d6ff.exe, 3c1e.exe

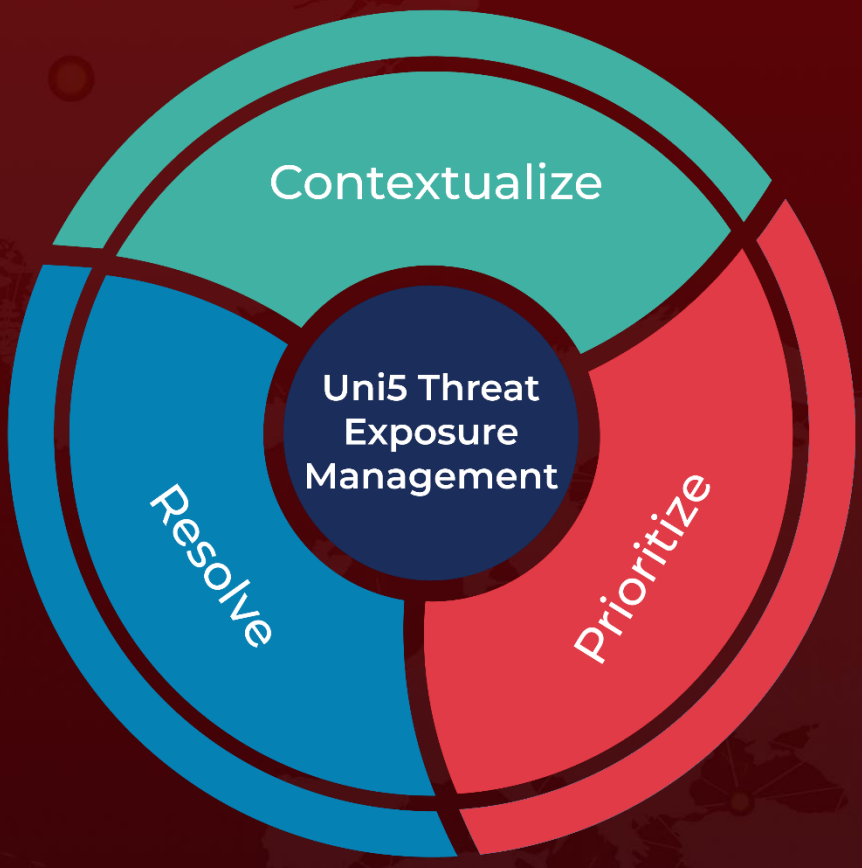
References

https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 7, 2023 • 02:30 AM

More at www.hivepro.com