HC3: Analyst Note

November 1, 2023 TLP:CLEAR Report: 202311011500

8Base Ransomware

Executive Summary

A recent attack on a U.S.-based medical facility in October 2023 highlights the potential threat of the ransomware gang, 8Base, to the Healthcare and Public Health (HPH) sector. Active since March 2022, 8Base became highly active in the summer of 2023, focusing their indiscriminate targeting on multiple sectors primarily across the United States. This surge in operational activity included the group's engagement in double extortion tactics as an affiliate of Ransomware-as-a-Service (RaaS) groups against mostly small- to medium-sized companies. While similarities exist between 8Base and other ransomware gangs, the group's identity, methods, and motivations remain largely unknown. What follows is an overview of the group, possible connections to other threat actors, an analysis of their ransomware attacks, their target industries and victim countries, impacts to the HPH sector, MITRE ATT&CK techniques, indicators of compromise, and recommended defenses and mitigations against the group.

Overview

8Base is not a ransomware operation, but a data-extortion cybercrime operation. They quickly become a notorious actor on the cyber threat landscape due to the significant number of victims claimed on their data leak site. While operating largely under the radar for the past year, 8Base resurfaced and was attributed to a massive spike in activity in May and June 2023. Notably, 8Base, alongside Cl0p and LockBit, were responsible for 48% of all recorded cyberattacks in July 2023 alone. On their leak site, the ransomware gang describes themselves as "...honest and simple pentesters. We offer companies the most loyal conditions for the return of their data." They claim to only target companies that have neglected the privacy and importance of the data of their employees and customers. Despite their aggressive portfolio of victims, the origins of the group and the identities of the operators remain a mystery. Cybersecurity researchers state that the speed and efficiency of the group's current operations does not indicate the start of a new group, but rather signifies the continuation of a well-established, mature organization.

8Base at a Glance	
Name(s)	8Base, EightBase, 8Base Ransomware
Threat Type	Ransomware Double extortion
Distribution Methods	Phishing e-mails Exploit kits Drive-by downloads
Ransomware Strains	Multiple ransomware strains, including a variant known as Phobos.
Target Sectors	Small- to medium-sized businesses (SMBs) across various sectors, including professional, scientific, technical, manufacturing, construction, and healthcare.
Target Countries	Mostly the United States, Brazil, and the United Kingdom, but also China, India, and Australia, among others. Notably, no ex-Soviet or Commonwealth of Independent States (CIS) countries have been targeted.

HC3: Analyst Note

November 1, 2023 TLP:CLEAR Report: 202311011500

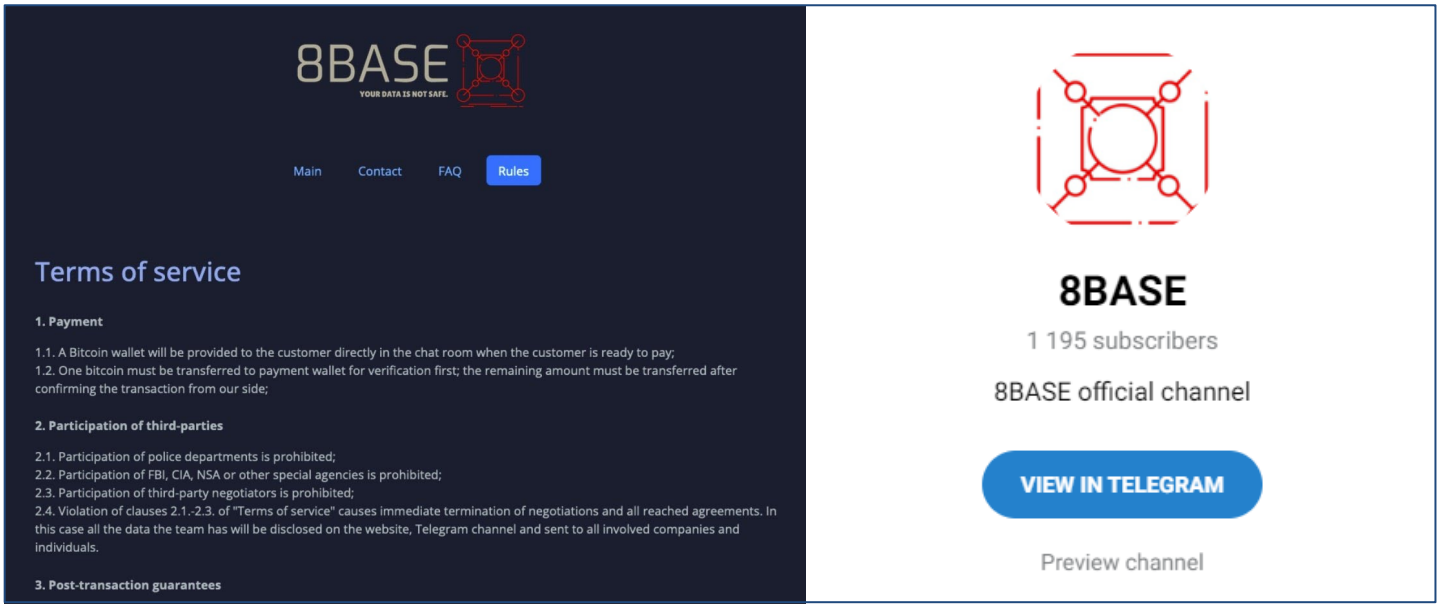


Figure 1: 8Base Tor Site *(Source: SentinelOne)* and 8Base Telegram Channel *(Source: Telegram)*

Associations and Affiliates

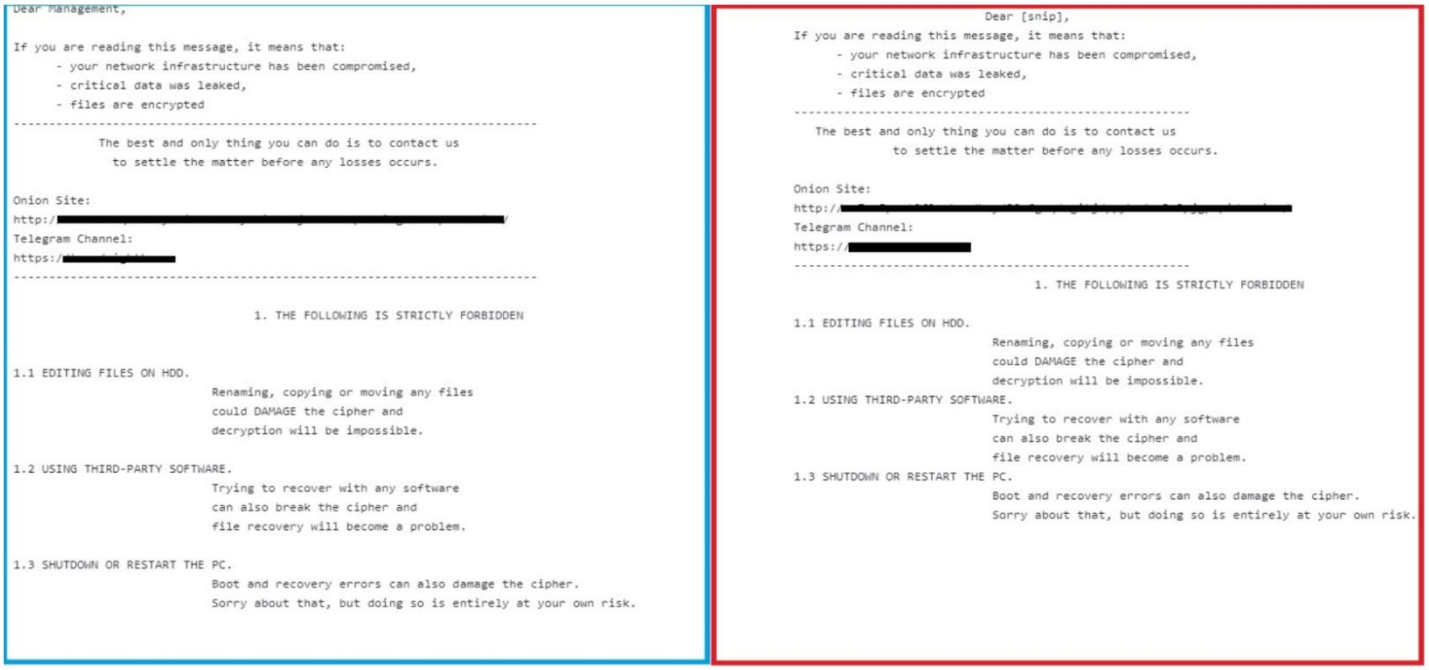
Some aspects of 8Base's current operations resemble previous ransomware attacks, specifically incidents pertaining to the threat actors RansomHouse and Phobos. Like 8Base, it is unknown whether RansomHouse is a ransomware group or a data-extortion cybercrime operation. This enigmatic and alleged group is known for buying already-leaked data, partnering with data leak sites, and extorting companies for money. Based on 8Base's leak site and public accounts (including a Telegram and a non-defunct Twitter handle), along with the group's communications, cybersecurity researchers posit that the group's syntax is like that of RansomHouse.

The first similarity was identified by cybersecurity researchers during a ransom note comparison project utilizing Natural Language Processing model Doc2Vec. Doc2Vec is an unsupervised machine learning algorithm that converts documents to vectors and can be used to identify similarities in documents. During this analysis, the ransom notes of 8Base had a 99% match with the RansomHouse ransom note. Interestingly, a second ransom note of 8Base also matched that of the threat group, Phobos.

The second similarity pertained to both group's respective leak sites. The verbiage is copied word for word from RansomHouse's welcome page to 8Base's welcome page. This was the case for their Terms of Service and FAQ pages as well. Despite the similarity between the two, it is unknown whether 8Base is an offshoot of RansomHouse or merely a copycat. Like 8Base, RansomHouse is known for using a wide variety of ransomware that is available on the dark web and does not have its own signature ransomware as a basis for comparison. When comparing the two threat actor groups, there are two major differences. The first is that RansomHouse advertises its partnerships and is openly recruiting for partnerships, whereas 8Base does not. The second difference is that despite the groups' leak sites containing identical language, the layout, design and structure of both differ.

HC3: Analyst Note

November 1, 2023 TLP:CLEAR Report: 202311011500



Dear Management,

If you are reading this message, it means that:
- your network infrastructure has been compromised,
- critical data was leaked,
- files are encrypted

The best and only thing you can do is to contact us
to settle the matter before any losses occurs.

Onion Site:
http:/[redacted]
Telegram Channel:
https:/[redacted]

---

1. THE FOLLOWING IS STRICTLY FORBIDDEN

1.1 EDITING FILES ON HDD.
Renaming, copying or moving any files
could DAMAGE the cipher and
decryption will be impossible.

1.2 USING THIRD-PARTY SOFTWARE.
Trying to recover with any software
can also break the cipher and
file recovery will become a problem.

1.3 SHUTDOWN OR RESTART THE PC.
Boot and recovery errors can also damage the cipher.
Sorry about that, but doing so is entirely at your own risk.

Dear [snip],

If you are reading this message, it means that:
- your network infrastructure has been compromised,
- critical data was leaked,
- files are encrypted

The best and only thing you can do is to contact us
to settle the matter before any losses occurs.

Onion Site:
http://[redacted]
Telegram Channel:
https://[redacted]

---

1. THE FOLLOWING IS STRICTLY FORBIDDEN

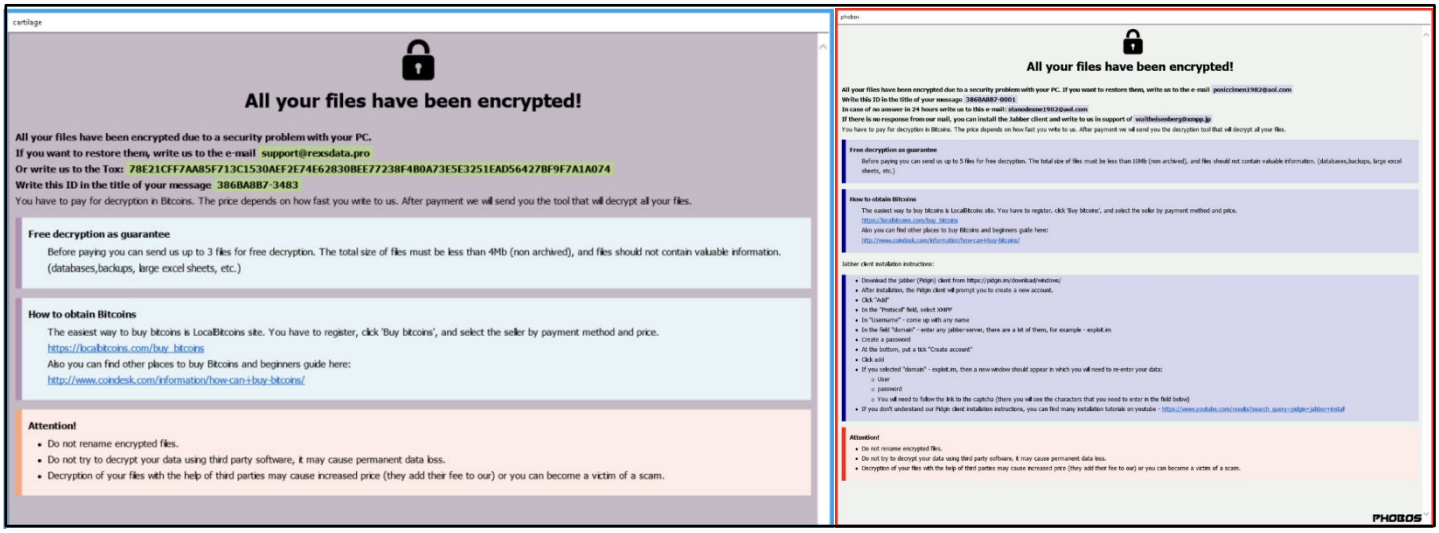
1.1 EDITING FILES ON HDD.
Renaming, copying or moving any files
could DAMAGE the cipher and
decryption will be impossible.

1.2 USING THIRD-PARTY SOFTWARE.
Trying to recover with any software
can also break the cipher and
file recovery will become a problem.

1.3 SHUTDOWN OR RESTART THE PC.
Boot and recovery errors can also damage the cipher.
Sorry about that, but doing so is entirely at your own risk.

Figure 2: An 8Base ransom note (left) compared to a RansomHouse ransom note (right). *(Source: VMWare)*

When searching for a sample of ransomware used by 8Base, a Phobos sample using a ".8base" file extension on encrypted files was recovered by cybersecurity researchers. Comparison of Phobos to the 8Base sample revealed that 8Base was using Phobos ransomware version 2.9.1 with SmokeLoader for initial obfuscation on ingress, unpacking, and loading of the ransomware. With Phobos ransomware being available as a Ransomware-as-a-Service (RaaS), this is not a surprise. Actors can customize parts to their needs, as seen in the 8Base ransom note. Although their ransom notes were similar, key differences included Jabber instructions and "phobos" in the top and bottom corners of the Phobos ransomware, while 8Base has "cartilage" in the top corner, a purple background, and no Jabber instructions.



cartilage

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC.
If you want to restore them, write us to the e-mail support@rexsdata.pro
Or write us to the Tox: 78E21CFF7AA85F713C1530AEF2E74E62830BEE77238F4B0A73E5E3251EAD56427BF9F7A1A074
Write this ID in the title of your message 386BA8B7-3483
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 3 files for free decryption. The total size of files must be less than 4Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

phobos

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail posiccimen1982@aol.com
Write this ID in the title of your message 386BA8B7-0001
In case of no answer in 24 hours write us to this e-mail: dianedeane1982@aol.com
If there is no response from our mail, you can install the Jabber client and write to us in support of waltheisenberg@xmpp.jp
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Jabber client installation instructions:

- Download the Jabber (Pidgin) client from https://pidgin.im/download/windows/
- After installation, the Pidgin client will prompt you to create a new account.
- Click "Add"
- In the "Protocol" field, select XMPP
- In "Username" - come up with any name
- In the field "domain" - enter any jabber-server, there are a lot of them, for example - exploit.im
- Create a password
- At the bottom, put a tick "Create account"
- Click add
- If you selected "domain" - exploit.im, then a new window should appear in which you will need to re-enter your data:
  - User
  - password
  - You will need to follow the link to the captcha (there you will see the characters that you need to enter in the field below)
- If you don't understand our Pidgin client installation instructions, you can find many installation tutorials on youtube - https://www.youtube.com/results?search_query=pidgin+jabber+install

Attention!
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

PHOBOS

Figure 3: 8Base (left) compared to Phobos (right) ransom notes *(Source: VMWare)*

Even though 8Base added their own branding customization by appending ".8base" to their encrypted files, the

format of the entire appended portion was the same as Phobos, which included an ID section, an email address, and the file extension.

Figure 4: An 8Base file extension (top) compared to a Phobos file extension (bottom). *(Source: VMWare)*

Technical Details

8Base ransomware payloads will enumerate all available local drives, encrypting standard data file extensions in a rapid and efficient manner using AES256 in CBC mode. Any attached share or drive volume will be subject to the encryption process. Once encrypted, files will have the .8base extension appended to them, at times accompanied by the victim ID and attacker email address.

Local firewall rules will be modified with the following command, issued by the ransomware: netsh advfirewall set currentprofile state off.

The above command allows the threat actor to evade Windows Defender's Advanced Firewall capabilities. The ransomware will attempt to remove Volume Shadow Copies (VSS) via the following commands: vssadmin.exe delete shadows /all /quiet wmic shadowcopy delete.

Payloads have been observed attempting either one or both of these methods: WMIC and VSSADMIN. In addition, BCDEDIT.EXE is used to modify the infected host's startup policy, disabling recovery mode and related features via the following: bcdedit /set {default} bootstatuspolicy ignoreallfailures.

Persistence is achieved via entries in the Windows Startup folder and in the registry. For example, a copy of the ransom payload will be written to: %AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\

This is in addition to writing copies of itself to %AppData%\Local\ and other locations deemed necessary by the threat actors. 8Base ransom notes are written to affected folders as both text and .HTA files.

Target Countries and Industries

According to the group's attacks, 8Base mostly targets SMB companies based in the United States, Brazil, and the United Kingdom. Other affected countries include Australia, Germany, Canada, and China, amongst others. Notably, no ex-Soviet or CIS countries have been targeted. While no known correlation to Russia or other Russian-speaking RaaS groups or affiliates exists, this geographic exclusionary pattern is a hallmark for many Russian-speaking threat actors.

When looking at the companies attacked by the group, most of them are SMB companies that operate under the professional services industry, such as accounting, law and legal services, business services, etc. Apart from professional services, companies operating in the fields of manufacturing, construction, finance and insurance, and healthcare industries also seem to be affected to a great extent.

HC3: Analyst Note

November 1, 2023 TLP:CLEAR Report: 202311011500

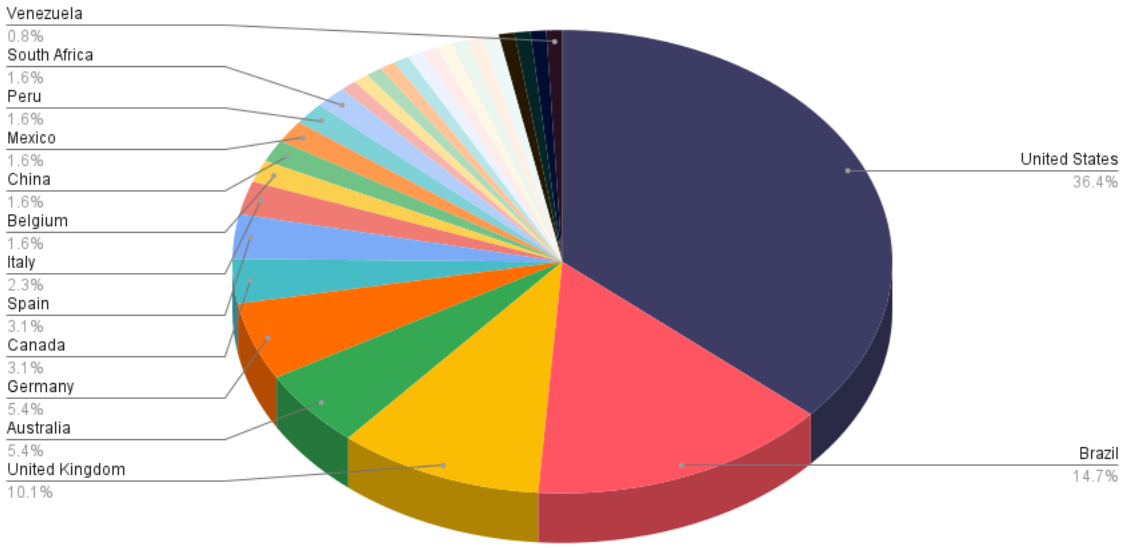


Figure 5: Affected country distribution from 8Base ransomware. *(Source: SOCRadar)*

Impact to Healthcare and Public Health Sector

The leak site associated with this ransomware group contains posts that can be traced back to March 2022, indicating that the group has potentially been active for at least a year without publicly disclosing its victims. It is worth noting that the group's Telegram channel was only created in May 2023, suggesting that they may have recently started to publicly disclose their victims. Since their first known activity back in March 2022, the group remained relatively quiet, with few notable attacks. However, in June 2023, the ransomware operation saw a sharp increase in activity, targeting many companies in various industries, including the HPH sector.

MITRE ATT&CK Techniques

Several cybersecurity researchers have annotated specific MITRE ATT&CK techniques.

MITRE ATT&CK TTPs of 8Base Ransomware *(Source: SOCRadar)*	
Reconnaissance	Active Scanning (T1595)
	Phishing for Information (T1598)
Resource Development	Acquire Infrastructure (T1583)
	Develop Capabilities (T1587)
Initial Access	Phishing: Spearphishing Attachment (T1566.001)
Execution	Scheduled Task/Job (T1053)
	Command and Scripting Interpreter (T1059)
	Shared Modules (T1129)
Persistence	Scheduled Task/Job (T1053)
	Boot or Logon Autostart Execution (T1547)
	Registry Run Keys/Startup Folder (T1547.001)
Privilege Escalation	Scheduled Task/Job (T1053)
	Boot or Logon Autostart Execution (T1547)
	Registry Run Keys/Startup Folder (T1547.001)
Defense Evasion	Masquerading (T1036)

	File Deletion (T1070.004)
	Modify Registry (T1112)
	Indirect Command Execution (T1202)
	File and Directory Permissions Modifications (T1222)
	Virtualization/Sandbox Evasion (T1497)
	Impair Defenses (T1562)
	Disable or Modify Tools (T1562.001)
	Disable or Modify System Firewall (T1562.004)
	Hide Artifacts (T1564)
	Hidden Files and Directories (T1564.001)
Credential Access	OS Credential Dumping (T1003)
	Input Capture (T1056)
Discovery	Process Discovery (T1057)
	System Information Discovery (T1082)
	File and Directory Discovery (T1083)
	Virtualization/Sandbox Evasion (T1497)
	Security Software Discovery (T1518.001)
Lateral Movement	Taint Shared Content (T1080)
Collection	Data from Local System (T1005)
	Input Capture (T1056)
	Data Staged (T1074)
	Archive Collected Data (T1560)
Command and Control	Application Layer Protocol (T1071)
	Web Protocols (T1071.001)
Exfiltration	Exfiltration Over C2 Channel (T1041)
Impact	Data Destruction (T1485)
	Inhibit System Recovery (T1490)

MITRE ATT&CK TTPs of 8Base Ransomware *(Source: VMWare)*		
Tactic	Technique	Description
TA00003 Persistence	T1547.001 Registry Run Keys / Startup Folder	Adds the following: %AppData%\Local\{malware} %ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup\{malware} %AppData%\Roaming\Microsoft\Start Menu\Programs\Startup\{malware}
TA0007 Discovery	T1135 Network Share Discovery	Uses WNetEnumResource() to crawl network resources
TA0004 Privilege Escalation	T1134.001 Token Impersonation/Theft	Uses DuplicateToken() to adjusts token privileges
TA0005 Defense Evasion	T1562.001 Disable or Modify Tools	Terminates a long list of processes, which are a mix of commonly used applications (example: MS Office applications) and security software.
TA0005 Defense Evasion	T1027.002 Obfuscated File or Information: Software Packing	SmokeLoader unpacks and loads Phobos to memory

HC3: Analyst Note

November 1, 2023 TLP:CLEAR Report: 202311011500

TA0040 Impact	T1490 Inhibit System Recovery	Runs: wmic shadowcopy delete wbadmin delete catalog -quiet vssadmin delete shadows /all /quiet bcdedit /set {default} recoveryenabled no bcdedit /set {default} bootstatuspolicy ignoreallfailures
TA0040 Impact	T1486 Data Encrypted for Impact	Uses AES to Encrypt Files

MITRE ATT&CK TTPs of 8Base Ransomware *(Source: Avertium)*				
Persistence	Discovery	Privilege Escalation	Defense Evasion	Impact
T1547.001: Registry Run Keys/Startup Folder	T1135: Network Share Discovery	T1134.001: Token Impersonation/Theft	T1562.001: Disable or Modify Tools	T1490: Inhibit System Recovery
			T1027.002: Obfuscated File or Information: Software Packing	T1486: Data Encrypted for Impact

Indicators of Compromise (IOC)

8Base IOCs *(Source: SOCRadar)*	
IOC Type	IOC
URL	hxxp[:]//dexblog45[.]xyz/statweb255/
URL	hxxp[:]//sentrex219[.]xyz/777/mtx5sfN.exe
URL	hxxp[:]//sentrex219[.]xyz/777/skx2auB.exe
IP	45.131.66[.]120
IP	45.89.125[.]136
FileName	8A26.exe
FileName	8B7F.exe
Hash	9769C181ECEF69544BBB2F974B8C0E10
Hash	5D0F447F4CCC89D7D79C0565372195240CDFA25F
Hash	E142F4E8EB3FB4323FB377138F53DB66E3E6EC9E82930F4B23DD91A5F7BD45D0

8Base IOCs *(Source: VMWare)*		
Indicator	Type	Context
518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c	SHA-256	8Base Ransomware (Phobos variant)
5BA74A5693F4810A8EB9B9EEB1D69D943CF5BBC46F319A32802C23C7654194B0	SHA-256	8Base ransom note (RansomHouse variant)
20110FF550A2290C5992A5BB6BB44056	MD5	8Base ransom note (RansomHouse variant)
3D2B088A397E9C7E9AD130E178F885FEEBD9688B	SHA-1	8Base ransom note (RansomHouse variant)
e142f4e8eb3fb4323fb377138f53db66e3e6ec9e82930f4b23dd91a5f7bd45d0	SHA-256	8Base ransomware (Phobos variant)
5d0f447f4ccc89d7d79c0565372195240cdfa25f	SHA-1	8Base ransomware (Phobos variant)
9769c181ecef69544bbb2f974b8c0e10	MD5	8Base ransomware

HC3: Analyst Note

November 1, 2023 TLP:CLEAR Report: 202311011500

		(Phobos variant)
C6BD5B8E14551EB899BBE4DECB6942581D28B2A42B159146BBC28316E6E14A64	SHA-256	8Base ransomware (Phobos variant)
518544E56E8CCEE401FFA1B0A01A10CE23E49EC21EC441C6C7C3951B01C1B19C	SHA-256	8Base ransomware (Phobos variant)
AFDDEC37CDC1D196A1136E2252E925C0DCFE587963069D78775E0F174AE9CFE3	SHA-256	8Base ransomware (Phobos variant)
wlaexfpxrs[.]org	Data POST to URL	8Base ransomware referred domain (Phobos variant)
admhexlogs25[.]xyz	Data GET request to URL	8Base ransomware referred domain
admlogs25[.]xyz	Data GET request to URL	8Base ransomware referred domain
admlog2[.]xyz	Data GET request to URL	8Base ransomware referred domain
dnm777[.]xyz	Data GET request to URL	8Base ransomware referred domain
serverlogs37[.]xyz	Data POST to URL	8Base ransomware referred domain
9f1a.exe	File Name	8Base ransomware dropped file
d6ff.exe	File Name	8Base ransomware dropped file
3c1e.exe	File Name	8Base ransomware dropped file
dexblog[.]xyz	Data GET request to URL	8Base ransomware referred domain
blogstat355[.]xyz	Data GET request to URL	8Base ransomware referred domain
blogstatserv25[.]xyz	Data GET request to URL	8Base ransomware referred domain

8Base IOCs *(Source: Avertium)*	
SHA-256	518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c
	5BA74A5693F4810A8EB9B9EEB1D69D943CF5BBC46F319A32802C23C7654194B0
	e142f4e8eb3fb4323fb377138f53db66e3e6ec9e82930f4b23dd91a5f7bd45d0
	5d0f447f4ccc89d7d79c0565372195240cdfa25f

HC3: Analyst Note

November 1, 2023 TLP:CLEAR Report: 202311011500

	C6BD5B8E14551EB899BBE4DECB6942581D28B2A42B159146BBC28316E6E14A64
	518544E56E8CCEE401FFA1B0A01A10CE23E49EC21EC441C6C7C3951B01C1B19C
	AFDDEC37CDC1D196A1136E2252E925C0DCFE587963069D78775E0F174AE9CFE3
MD5	20110FF550A2290C5992A5BB6BB44056
	9769c181ecef69544bbb2f974b8c0e10
URLs	wlaexfpxrs[.]org
	admhexlogs25[.]xyz
	admlogs25[.]xyz
	admlog2[.]xyz
	dnm777[.]xyz
	serverlogs37[.]xyz
	dexblog[.]xyz
	blogstat355[.]xyz
	blogstatserv25[.]xyz
File Name	3c1e.exe
	d6ff.exe
	9f1a.exe

Defense and Mitigations

Detecting 8Base ransomware requires a combination of technical and operational measures designed to identify and flag suspicious activity on the network. This allows the organization to take appropriate action, and to prevent or mitigate the impact of the ransomware attack. It is important to take a multi-layered approach, which includes the following steps:

1. Use anti-malware software or other security tools capable of detecting and blocking known ransomware variants. These tools may use signatures, heuristics, or machine learning algorithms to identify and block suspicious files or activities.
2. Monitor network traffic and look for indicators of compromise, such as unusual network traffic patterns or communication with known command-and-control servers.
3. Conduct regular security audits and assessments to identify network and system vulnerabilities, and to ensure that all security controls are in place and functioning properly.
4. Educate and train employees on cybersecurity best practices, including identifying and reporting suspicious emails or other threats.
5. Implement a robust backup and recovery plan to ensure that the organization has a copy of its data and can restore it in case of an attack.

Some best practices for protecting against 8Base and mitigating the impact of a successful attack include:

- **Educate employees:** Employees should be educated on the risks of ransomware, and on how to identify and avoid phishing emails, malicious attachments, and other threats. They should be encouraged to report suspicious emails or attachments, and to avoid opening them, or clicking on links or buttons in them.

- **Implement strong passwords:** Organizations should implement strong, unique passwords for all user accounts, and should regularly update and rotate these passwords. Passwords should be at least eight characters long and should include a combination of uppercase and lowercase letters, numbers, and special characters.

- **Enable multi-factor authentication:** Organizations should enable multi-factor authentication (MFA) for all user accounts, to provide an additional layer of security. This can be done using mobile apps like Google Authenticator or Microsoft Authenticator, or by using physical tokens or smart cards.

- **Update and patch systems:** Organizations should regularly update and patch their systems to fix any known vulnerabilities and to prevent attackers from exploiting them. This includes updating the operating system, applications, and firmware on all devices, and disabling any unnecessary or unused services or protocols.

- **Implement backup and disaster recovery:** Organizations should implement regular backup and disaster recovery (BDR) processes to ensure that they can recover from ransomware attacks or other disasters. This includes creating regular backups of all data and systems, and storing these backups in a secure, offsite location. The backups should be tested regularly to ensure that they are working, and that they can be restored quickly and easily.

The Way Forward

8Base may be new to the cyber threat landscape, but in its short existence, it has proven to be a formidable adversary. Any disruption to an organization's operations can lead to severe consequences, especially to the HPH sector. Whether it is affiliated to or an off-shoot of other threat actors, 8Base's focus on data exfiltration instead of file encryption highlights the need to prioritize cyber security best practices, and prevent unauthorized access to an organization's systems and networks. The value of HPH data, in particular, signals that the healthcare industry will remain a viable target to this threat actor. In addition to the aforementioned defense and mitigation strategies, HC3 recommends that HPH organizations utilize resources from CISA Stop Ransomware, HHS 405(d), and the H-ISAC to proactively and reactively aid healthcare organizations with cybersecurity awareness and guidance. The probability of cyber threat actors targeting any industry remains high, but especially so for the Healthcare and Public Health sector. Prioritizing security by maintaining awareness of the threat landscape, assessing their current situation, and providing staff with the tools and resources necessary to prevent a cyberattack remain the best ways forward for healthcare organizations.

Relevant HHS Reports

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

References

"8Base claims to have stolen patient data and employee info from Kansas Medical Center." DataBreaches.net July 11, 2023. https://www.databreaches.net/8base-claims-to-have-stolen-patient-data-and-employee-info-from-kansas-medical-center/

"8Base Ransomware: In-Depth Analysis, Detection, and Mitigation." SentinelOne. Accessed October 23, 2023. https://www.sentinelone.com/anthology/8base/

Abraham, Jorg. "8Base Ransomware Surge; SmugX Targeting European Governments, Russian-Linked DDoS Warning." EclecticIQ. July 5, 2023. https://blog.eclecticiq.com/8base-ransomware-surge-smugx-targeting-european-governments

"Dark Web Profile: 8Base Ransomware." SOCRadar. July 27, 2023. https://socradar.io/dark-web-profile-8base-ransomware/

"The Double Extortion Group, 8Base." Avertium. August 1, 2023. https://explore.avertium.com/resource/the-double-extortion-group-8base

Medium User: Intidhar. "Threat Actors Series: 8Base." Medium. July 2, 2023. https://medium.com/@intidhar/threat-actors-series-8base-4425e5640e62

Khaitan, Ashish. "8Base Ransomware Group Conducts Arbitrary Cyber Attacks, Enlists 7 New Organizations as Victims." The Cyber Express. July 13, 2023. https://thecyberexpress.com/8base-ransomware-group-cyber-attack-series/

Lakshmanan, Ravie. "8Base Ransomware Spikes in Activity, Threatens U.S. and Brazilian Businesses." The Hacker News. June 28, 2023. https://thehackernews.com/2023/06/8base-ransomware-spikes-in-activity.html

"Oregon Sports Medicine allegedly hit by 8Base threat actors." DataBreaches.net. August 8, 2023. https://www.databreaches.net/oregon-sports-medicine-allegedly-hit-by-8base-threat-actors/

Osborne, Charlie. "Ransomware attacks broke records in July, mainly driven by this one group." ZDNet. August 23, 2023. https://www.zdnet.com/article/ransomware-attacks-broke-records-in-july-mainly-driven-by-this-one-group/

Riley, Duncan. "Canadian dental service pays ransom in 8base ransomware attack." Silicon Angle. August 13, 2023. https://siliconangle.com/2023/08/13/canadian-dental-service-pays-ransom-8base-ransomware-attack/

Snyder, Deborah and Fae Carlisle, Dana Behling, Bria Beathley. "8Base Ransomware: A Heavy Hitting Player." VMWare. June 28, 2023. https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html

Telegram User: 8Base. Telegram. Accessed October 23, 2023. https://t.me/eightbase

Toulas, Bill. "8Base ransomware gang escalates double extortion attacks in June." BleepingComputer. June 28, 2023. https://www.bleepingcomputer.com/news/security/8base-ransomware-gang-escalates-double-extortion-attacks-in-june/

X User: @8BASEHOME. Twitter. Accessed October 23, 2023. https://twitter.com/8BASEHOME

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback