Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

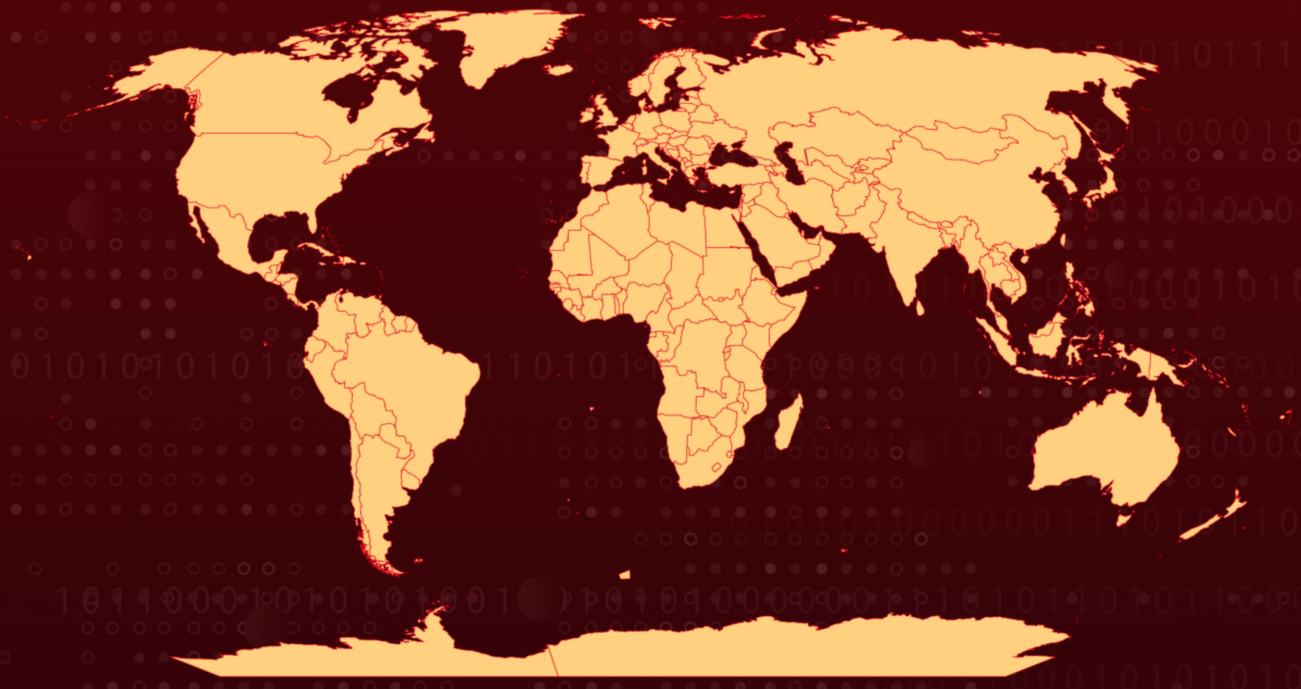
Unveiling New Big Head Ransomware Variants and Their Stealthy Tactics

Date of Publication	Admiralty Code	TA Number
July 10, 2023	A1	TA2023292

Summary

First Appearance: May 12, 2023
Attack Region: Worldwide
Affected Platform: Windows
Malware: Big Head Ransomware
Attack: The emergence of Big Head ransomware and its variants suggests a shared source, distributed through deceptive Windows update and Word installer disguises. The threat actor engages via email and Telegram, showcasing the malware on a YouTube channel, while a potential connection to Bahasa-speaking countries remains speculative.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

A new ransomware family called Big Head and its variants have been discovered. The variants share a common contact email in their ransom notes, suggesting they originate from the same malware developer. Multiple versions of this malware have been identified, and they are likely distributed through malvertisements posing as fake Windows updates and Word installers.

#2

The analysis focuses on three samples of the Big Head ransomware, describing their functionalities and routines. The first sample is a .NET compiled binary that checks for a specific mutex name and performs various actions, such as creating a registry key and encrypting files with the extension ".r3d".

#3

It also drops additional encrypted binaries and modifies the system's wallpaper. The second sample exhibits both ransomware and stealer behaviors, encrypting files and collecting information using different dropped files. The third sample incorporates a file infector named Neshta and displays a unique wallpaper and ransom note.

#4

The ransomware utilizes techniques like AES encryption, Base64 encoding, and deceptive tactics, such as displaying a fake Windows update screen. Each variant of the Big Head ransomware has distinct features, including backdoors, trojan spy and/or info stealers, and file infectors.

#5

The threat actor behind the Big Head ransomware is known to communicate with victims through email and Telegram. The actor's YouTube channel demonstrates the malware they possess, and their Telegram username is provided in the video comments. The actor may engage in transactions on Telegram, but their specific connection to countries using the Bahasa language remains speculative.

Recommendations

Keep your systems and software up to date: Regularly install updates for your operating system, applications, and security software. This helps patch vulnerabilities that malware can exploit.

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

TA0003 Persistence	**TA0010** Exfiltration	**TA0005** Defense Evasion	**TA0002** Execution
TA0007 Discovery	**TA0001** Initial Access	**TA0009** Collection	**TA0040** Impact
T1127 Trusted Developer Utilities Proxy Execution	**T1027** Obfuscated Files or Information	**T1176** Browser Extensions	**T1547** Boot or Logon Autostart Execution
T1562 Impair Defenses	**T1486** Data Encrypted for Impact	**T1560** Archive Collected Data	**T1070** Indicator Removal
T1055 Process Injection	**T1547.001** Registry Run Keys / Startup Folder	**T1140** Deobfuscate/Decode Files or Information	**T1490** Inhibit System Recovery
T1059.006 Python	**T1059** Command and Scripting Interpreter	**T1218** System Binary Proxy Execution	**T1562.001** Disable or Modify Tools
T1113 Screen Capture	**T1036** Masquerading		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	6d27c1b457a34ce9edfb4060d9e04eb44d021a7b03223ee72ca569c8c4215438, 2a36d1be9330a77f0bc0f7fdc0e903ddd99fcee0b9c93cb69d2f0773f0afd254, 39caec2f2e9fda6e6a7ce8f22e29e1c77c8f1b4bde80c91f6f78cc819f031756, b8e456861a5fb452bcf08d7b37277972a4a06b0a928d57c5ec30afa101d77ead, ff900b9224fde97889d37b81855a976cddf64be50af280e04ce53c587d978840, 980bac6c9afe8efc9c6fe459a5f77213b0d8524eb00de82437288eb96138b9a2, f354148b5f0eab5af22e8152438468ae8976db84c65415d3f4a469b35e31710f, f59c45b71eb62326d74e83a87f821603bf277465863bfc9c1dcb38a97b0b359d, 40e5050b894cb70c93260645bf9804f50580050eb131e24f30cb91eec9ad1a6e, 64aac04ffb290a23ab9f537b1143a4556e6893d9ff7685a11c2c0931d978a931, 64246b9455d76a094376b04a2584d16771cd6164db72287492078719a0c749ab, 627b920845683bd7303d33946ff52fb2ea595208452285457aa5ccd9c01c3b0a, 037f9434e83919506544aa04fecd7f56446a7cc65ee03ac0a11570cf4f607853, 0dbfd3479cfaf0856eb8a75f0ad4fccb5fd6bd17164bcfa6a5a386ed7378958d, 159fbb0d04c1a77d434ce3810d1e2c659fda0a5703c9d06f89ee8dc556783614, 1942aac761bc2e21cf303e987ef2a7740a33c388af28ba57787f10b1804ea38e, 1ada91cb860cd3318adbb4b6fd097d31ad39c2718b16c136c16407762251c5db, 1c8bc3890f3f202e459fb87acec4602955697eef3b08c93c15ebb0facb019845, 226bec8acd653ea9f4b7ea4eaa75703696863841853f488b0b7d892a6be3832a, 40d11a20bd5ca039a15a0de0b1cb83814fa9b1d102585db114bba4c5895a8a44, 603fcc53fd7848cd300dad85bef9a6b80acaa7984aa9cb9217cdd012ff1ce5f0, 6698f8ffb7ba04c2496634ff69b0a3de9537716cfc8f76d1cfea419dbd880c94

TYPE	VALUE
SHA256	66bb57338bec9110839dc9a83f85b05362ab53686ff7b864d302a217cafb7531, 6b3bf710cf4a0806b2c5eaa26d2d91ca57575248ff0298f6dee7180456f37d2e, 6b771983142c7fa72ce209df8423460189c14ec635d6235bf60386317357428a, 806f64fda529d92c16fac02e9ddaf468a8cc6cbc710dc0f3be55aec01ed65235, 9a7889147fa53311ba7ec8166c785f7a935c35eba4a877c1313a8d2e80e3230d, 9aa38796e0ce4866cff8763b026272eb568fa79d8a147f7d61824752ad6d8f09, 9c1c527a826d16419009a1b7797ed20990b9a04344da9c32deea00378a6eeee2, bcf8464d042171d7ecaada848b5403b6a810a91f7fd8f298b611e94fa7250463, be6416218e2b1a879e33e0517bcacaefccab6ad2f511de07eebd88821027f92d, cf9410565f8a06af92d65e118bd2dbaeb146d7e51de2c35ba84b47cfa8e4f53b, dcfa0fca8c1dd710b4f40784d286c39e5d07b87700bdc87a48659c0426ec6cb6, f6a2ec226c84762458d53f5536f0a19e34b2a9b03d574ae78e89098af20bcaa3

References

https://www.trendmicro.com/en_us/research/23/g/tailing-big-head-ransomware-variants-tactics-and-impact.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/g/tailing-big-head-ransomwares-variants-tactics-and-impact/IOCs-tailing-big-head-ransomware-variants-tactics-and-impact.txt

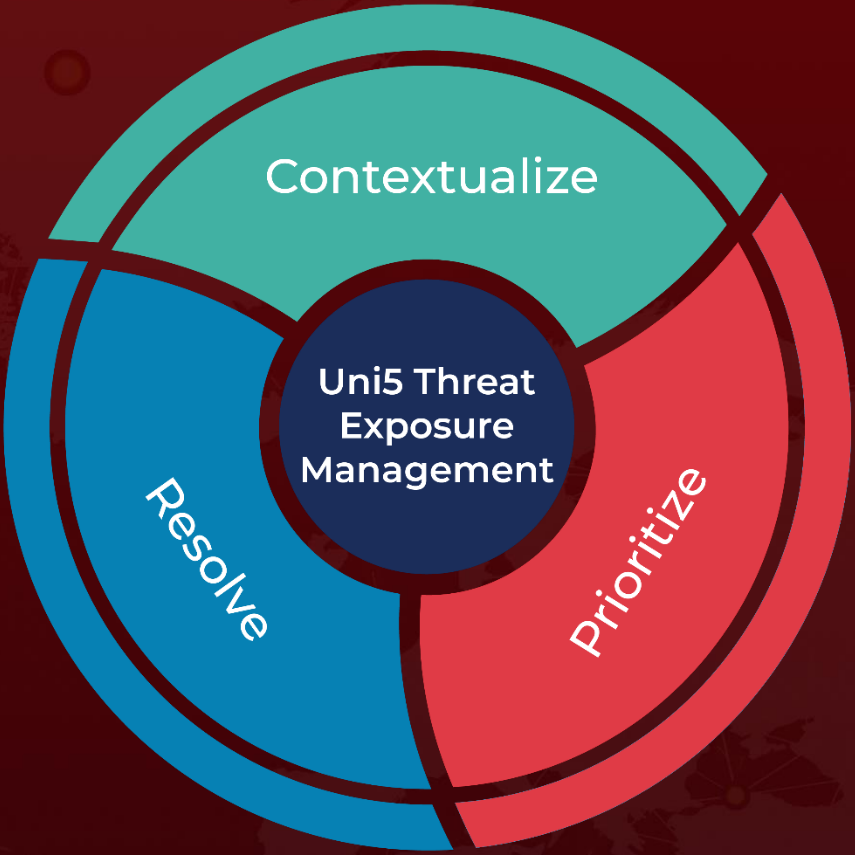
https://twitter.com/pcrisk/status/1656883712771129349?s=20

https://www.fortinet.com/blog/threat-research/fortiguard-labs-ransomware-roundup-big-head

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 10, 2023 • 7:30 AM

More at www.hivepro.com