Hive Pro®

Threat Level

Red

CISA: AA24-060A

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

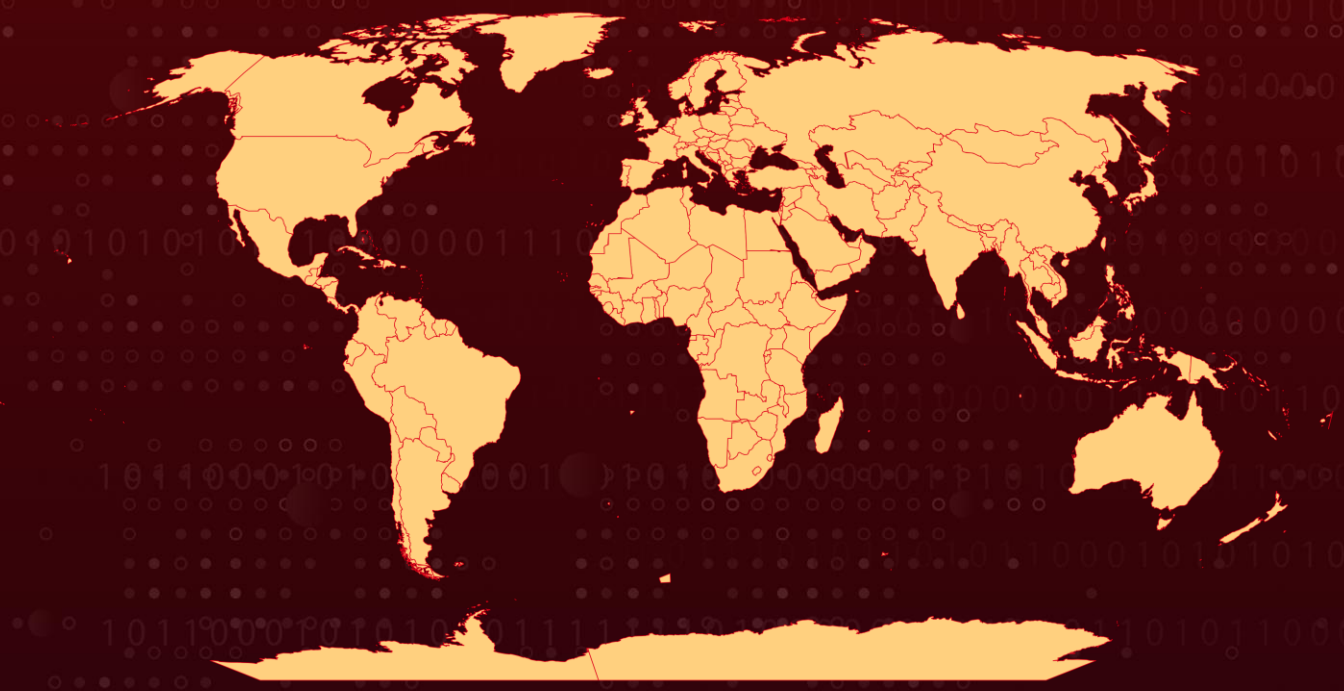
In-Depth Analysis of Phobos Ransomware

Date of Publication	Last Update Date	Admiralty Code	TA Number
October 19, 2023	March 5, 2024	A1	TA2023426

Summary

First Appearance: December 2018
Targeted Countries: Worldwide
Affected Platforms: Windows
Targeted Industries: Small- to medium-sized businesses, which usually includes Healthcare, Education, Government, Financial services, Retail, Manufacturing, Transportation, Energy, Technology, Professional services, Nonprofits
Malware: Phobos ransomware
Attack: Phobos ransomware, active since 2018, primarily targets small to medium-sized businesses with lower ransom demands. It uses compromised RDP connections, is distributed via a Ransomware as a Service model, and has recently adopted DLL sideloading for stealthy attacks.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2021-34527	Microsoft Windows Print Spooler Remote Code Execution Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2021-1675	Microsoft Windows Print Spooler Remote Code Execution Vulnerability	Microsoft Windows	✗	✓	✓
CVE-2017-0213	Microsoft Windows Privilege Escalation Vulnerability	Microsoft Windows	✗	✓	✓

Attack Details

#1

Phobos ransomware is an older ransomware family that has been active since late 2018. It shares similarities with Dharma ransomware, which evolved from CrySIS and was considered one of the most sophisticated ransomware strains during 2017-2018. Phobos primarily targets small to medium-sized businesses and typically demands lower ransoms compared to other ransomware groups.

#2

Phobos ransomware is distributed through an affiliate model, known as Ransomware as a Service (RaaS). Affiliates are provided with access to a control panel that allows them to generate custom ransomware builds for specific victims. Phobos actors tend to prioritize targeting servers rather than end-user computers, and it exclusively affects Windows operating systems.

#3

The initial access for Phobos can be gained through phishing emails containing malicious files, embedded backdoors like SmokeLoader, or by employing brute force methods to obtain RDP credentials or poor Remote Desktop (RDP) connections. Once remote access to a compromised server is established, the ransomware initiates privilege elevation without using User Account Control (UAC) bypass. The ransomware payload is then copied and executed with administrative privileges.

#4

Phobos ransomware is known for being a double extortion ransomware, where it first exfiltrates data and then encrypts files using the AES encryption method. Different variants may use various file extensions for encrypted files, including .phobos, .acute, and some may include the attacker's email address in the file names.

#5

In a recent development, Phobos ransomware has been distributed using DLL sideloading, leveraging a legitimate signed binary called WiseTurbo.exe to execute the malicious DLL NlogExt.dll. This attack technique is particularly dangerous as it leverages legitimate signed binaries to execute malicious code, making it challenging for security software to detect and prevent the attack. Phobos ransomware effortlessly integrates with a variety of open-source tools, such as Smokeloader, Cobalt Strike, and Bloodhound.

#6

Phobos ransomware has not only been a significant threat in its own right but has also served as a foundation for the development of other ransomware variants, including Eking ransomware, LIZARD ransomware, Makop ransomware (discovered in 2020), Fair ransomware (detected in March 2021), 8Base Ransomware (detected in March 2022), and Faust ransomware (detected in November 2022). In these more recent variants, developers incorporated new fileless and evasive techniques, demonstrating the ongoing evolution of this ransomware family.

Recommendations

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

Regularly Update and Patch Systems: Keep all software, including operating systems and applications, up to date with the latest security patches and updates. Vulnerabilities in outdated software can be exploited by Phobos.

Secure Remote Access: Implement application controls to manage and control the execution of software, including allowlisting remote access programs. Limit the use of Remote Desktop Protocol (RDP) and enforce best practices for its use. Apply phishing-resistant multifactor authentication for remote access. Log RDP login attempts.

Network Segmentation: Use network segmentation to isolate critical systems and data from less critical areas, helping to contain the spread of ransomware.

Endpoint Security: Deploy robust endpoint security solutions, including antivirus and anti-malware software, to detect and prevent Phobos ransomware infections.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0001 Initial Access	TA0011 Command and Control	TA0007 Discovery
TA0005 Defense Evasion	TA0010 Exfiltration	TA0009 Collection	TA0040 Impact
TA0003 Persistence	TA0004 Privilege Escalation	T1566 Phishing	T1048 Exfiltration Over Alternative Protocol
T1574.002 DLL Side-Loading	T1574 Hijack Execution Flow	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1562 Impair Defenses	T1548.002 Bypass User Account Control	T1486 Data Encrypted for Impact	T1027 Obfuscated Files or Information
T1566.001 Spearphishing Attachment	T1003 OS Credential Dumping	T1204.002 Malicious File	T1204 User Execution
T1110 Brute Force	T1105 Ingress Tool Transfer	T1071 Application Layer Protocol	T1102 Web Service
T1070.004 File Deletion	T1070 Indicator Removal	T1112 Modify Registry	T1082 System Information Discovery
T1490 Inhibit System Recovery	T1543.003 Windows Service	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution
T1543 Create or Modify System Process	T1218.014 MMC	T1078.004 Cloud Accounts	T1078 Valid Accounts
T1021.001 Remote Desktop Protocol	T1505.003 Web Shell	T1505 Server Software Component	T1046 Network Service Discovery
T1135 Network Share Discovery	T1021.002 SMB/Windows Admin Shares	T1021 Remote Services	T1001.003 Protocol Impersonation

T1003.001 LSASS Memory	**T1003.005** Cached Domain Credentials	**T1027.002** Software Packing	**T1027.009** Embedded Payloads
T1047 Windows Management Instrumentation	**T1055.002** Portable Executable Injection	**T1055.004** Asynchronous Procedure Call	**T1057** Process Discovery
T1059.003 Windows Command Shell	**T1071.002** File Transfer Protocols	**T1083** File and Directory Discovery	**T1087.002** Domain Account
T1106 Native API	**T1133** External Remote Services	**T1134.001** Token Impersonation/Theft	**T1134.002** Create Process with Token
T1140 Deobfuscate/Decode Files or Information	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1555.005** Password Managers
T1560 Archive Collected Data	**T1562.004** Disable or Modify System Firewall	**T1567.002** Exfiltration to Cloud Storage	**T1585** Establish Accounts
T1588.002 Tool	**T1593** Search Open Websites/Domains	**T1595.001** Scanning IP Blocks	**T1598** Phishing for Information
T1657 Financial Theft			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0000599cbc6e5b0633c5a6261c79e4d3d81005c77845c6b0679d854884a8e02f, 7451be9b65b956ee667081e1141531514b1ec348e7081b5a9cd1308a98eec8f0, 518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c, 9215550ce3b164972413a329ab697012e909d543e8ac05d9901095016dd3fc6c, 482754d66d01aa3579f007c2b3c3d0591865eb60ba60b9c28c66fe6f4ac53c52,

TYPE	VALUE
SHA256	c0539fd02ca0184925a932a9e926c681dc9c81b5de4624250f2dd885ca5c4763, 58626a9bfb48cd30acd0d95debcaefd188ae794e1e0072c5bde8adae9bccafa6, f3be35f8b8301e39dd3dffc9325553516a085c12dc15494a5e2fce73c770699ed, 518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c, 32a674b59c3f9a45efde48368b4de7e0e76c19e06b2f18afb6638d1a080b2eb3, 2704e269fb5cf9a02070a0ea07d82dc9d87f2cb95e60cb71d6c6d38b01869f66, fc4b14250db7f66107820ecc56026e6be3e8e0eb2d428719156cf1c53ae139c6, a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2, d0604a3864899ac9bf0a07e47330b62a3e76b61335d6dac2e9b5a796b9fcc164, 9215550ce3b164972413a329ab697012e909d543e8ac05d9901095016dd3fc6c, fd59543a425d2159dfadba8efd4d40178b609ef123a8bc5cf00fe3afef95623d, 482754d66d01aa3579f007c2b3c3d0591865eb60ba60b9c28c66fe6f4ac53c52, 2a50a42d3c44e6e3890a53228cb84f6fdb17e38b31422c68b8634a06d36cc324, 78732997a6c9d975b97da85fc511533d44083a9f9da60dae8393274a59b7bfce, 8f60d17bbaefd66fe94d34ea3262a1e94b0f8f0702c437d19d3e292c72f1cedc, 698b2a9cf9ce16f1cb5cff4576e902888cb14db7414b8e6ac4eb728f8c87d209, aedbddbf7494baaaf759a720d9cd17540d3c171b9cc52a02e0ef9a592bd9cd63, f595f91a9966808cc85d11981e66e98043af9aeaaaa3893ef058b9a79c474f17, d4cb20dba15d88c38c35be69fe04538b4f9bb0a12edb51ff23c0171b584edf08, 7e18ff461e3fc159c9b6634c9250600ea4c62da604885697c95d9bac794109b8, b0b7a65f4821d5c9e8c782ee5ccca1c1a6a05236c27a4a136eb370302db2b35e, f709d1f84e4f0a845ebb4a9fb1500aa2a9fd600e97cbea32ffc3e49c1084f467, ab3985e07195465b9a9d8c5a9959e783e2a30f6d6e7fdda3ab153de4d7fc6fe6, f5d99d4548470b4699b215453e9be29e48aa20616d45f704c335bd3bbe3e0a4f, 8e5f99b92349381fd772b1bdb18cce2c6595181fcad0f68de25593276d61620f,

TYPE	VALUE
SHA256	97a4d094f86b757b3fb0e189f2843a7af8d0ec43f9805214e89992528e83b5d7, 795b951e16aa4aa0557c24eedad4897e457864838393fcf66220da85ad8be9d8, 1c1eed8f9b2c44bb7290690521cc5f4e02929d5eeb3cc8fc2bf042cf3b789b8e, 681f180735ec833997bea4eb26c58f9c2e39980cd0a351e0b5cd99c502b33ae8, ebbbc1d293ce864c83cf874c3f8051dd636bd1303f013d3fa0cc97eada3266ac, 667F88E8DCD4A15529ED02BB20DA6AE2E5B195717EB630B20B9732C8573C4E83, 6E9C9B72D1BDB993184C7AA05D961E706A57B3BECF151CA4F883A80A07FDD955, 31dba1a23db70ffb952f0e597acf95d16ab60423018a83d0ccb4f57ce0471793, 56bd92cb5c9800338f01a5c8d6fdda4d602717d7a279ec499d15b8a2df36ec92, 62d67fe5548da330b0074f8fd162833e2675f8973899ae5778c10ef33a3f06af, 58626a9bfb48cd30acd0d95debcaefd188ae794e1e0072c5bde8adae9bccafa6, 94e5a07113b228991a294f9b972d2727695ecd68520f56741ae4ad649d5d529b, 52507e8ce8151bd4fa072949245a50f002ed7973b322968b9690927d061d506f, 703cb9286dd4c0219dcb85fc960d0d662a784b5d9bf3ab78b379ac195fc72595, a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2, 596f40f23a1284b4e844e4159f07b92d0bdcfdc7ce00180a2b70af4f6843bed4, 25dce15057f3e9f904ea28e039fe0d2945308d7f41ea5386e99af4840c2e6762, c918ba4319356db7b86b34849baba40eb2fdc96b05c5ead8bf7375373ced3bcd, e443920a2306dd8b0182dedadc7c1254bd9c43e576c4876a1970886d06b1cccf, ffbafce6dc32dd8e1dc28d5de250f08f2f32d12b061c3ad5d7ee8125298bfc07, 61f5fcb639e3ad7b671a16e243bf0731e1759dcffde00eb14df56415856edbdb, 02db45a4a6821114adc7aad6eb875ff0db66f0ce1e63387dd02fd499e9a0b745, e30169690074a26afb368ec33e8195a89bd33a48f879913a100a67a960d033bb, 43f846c12c24a078ebe33f71e8ea3b4f75107aeb275e2c3cd9dc61617c9757fc,

TYPE	VALUE
SHA256	9d298673b975048819034f7e746f9a2f4e011ae47ba87b48b9375e151326e7b1, 69e479f062e247568bb995ee0eed042d5cf1e37f4f41843981b52c55c10f6c7a, 409ef3b1cf30687fde062ac12af5ceebe5f91dd261f515231d172a4c0687ce72, 97e4ffdb8be8d108e5c81af0d8edda6e3bed9f37e170a05221199742f4de309c, a394878332e9c10950a04d9d735d23dc65e8d102fbfd04b790af7db40b60c5d5, 88d3bdfba7c8f0a49e6a296662e4d5ac13440ab38235602d75dbff3342cd2642, 55135de67a5816c6622ae671c934d5a2bfac1b8f3f09083f64a3ae5997bfbfdf, b4965b7fb169577c87cc40e303a002e497fb4812a1376b73e9ba85813917c733, 3b272c1e76e72bf4acc236b2305dd1c6b12dae729620e6c82f25b74a38b73044, 6575de46c36289308b49fa67bce7cf2c964d53678933914274879006994 8bef7, 35920652147ca2dc1150f8605ed50036a8c50d869f328dc9912628a33db40b3a, f6b60839de0ac933f0788bc1e12dee859950010f938a05544ad51c424954b9a6, 7f8f8c82fec8acbb0947a192dd5cbe8b95ffdba4e252b582eae127f1c062399b, 2cadd0ff146e1cdf1270894be4fb1523bfdcc7a31760e0ca5cfd9d8e6b525c21, 4ff1f8a052addbc5a0388dfa7f32cc493d7947c43dc7096baa070bfc4ae0a14e, cfc5fb8385f662b109c6cf866ff70e598964dd37dc3498d5bd45ad2c8f4c7d59, b93fcbafc42d24b88abeb354defad342110bb3928e7e24de4315b905dc74dd86, f0aec57001a184ea82122a59c6e5be48042f75d6f11a40125995ba9531aab718, ccc167391bb396f08e365eec5421786ccf1578ba8d3250debb9321767d33dff2, 4ce04ba4acc3645c66c9da89eb05e7708408e4463b5a901fc15be2479b9bdaf5, 2eff58738b5a7717a3fcdf7a4171c6fa18492bc200eddc26bf608fa35d28466e, F17D535192C421BF7C587C11190AE3BA6CC7EEE392DCCD86AD981D3547868D49, d7cb8a2d60e1818d0638a4c38cd6fae475dc83ab7b2bde9827ecc4e4a7ce6ed7, 32c9c069c7fe9ffdd9086b957e45c03993863730cd1eed4815e226dc1b7b436e, 691eaa4c48666b69ca180b9aae1a4035fefb29cef1f0a3cfbc91c020b0b09f40,

TYPE	VALUE
SHA256	883162246c3d0a2c10e5c35a2a43ff444a24dbcf9e64dc5cc09009b9cd0ab48e, 0b4c743246478a6a8c9fa3ff8e04f297507c2f0ea5d61a1284fe65387d172f81, 527918fbd218787f202dcfb20024375238aca2dc64c1661bdc71f8833240e7f8, f0d6846da6d45180a695201888edc4f9c512fb0d11ed56394aae9daa874ba88c, fab5850b79de211ba1d789f80a4684657b3a79c849d46761decb2de95931162b, 51220927e71a1b8c5cc0ca85c454dc93f3aaae25bb3ec0dc3a9837236687d45f, f97cc59b803e60dcca4461975ecd5e6fc4c64dc31db89e187e5874503af1eb4d, 9f67b6057e5b5dc4b2ec3b370ca3062e0bed91a934b227911af2a3de17164ee5, 9ab71ecc8338329b63410ba744c564c014eb5628eeed774302ef99bcc4e44d00, fe025cd046edabab5a07d058bfcbb884c144511581d5206681064355fb2834bc, 9f40b69060a52731107baec84a0c0f8a1bfc1a62e8471b9cd69509aade9cb7f1,
MD5	AAA058858261D7C0E73FA1B8264A9A3D, 1A75878DEA8F5580C25E0B9F1C734949, 25674F5426C59051960F0D00F06F0B77, 9DE437C0A1F9E633186F5F631D32AF8A, 792b27b961ee8ae67855b952859053c7, 86e50a7bd09c2a5fc2eac716c29ea6c7, 6ad6c98f75c3133b94026c2fdd06a6f1, d62a9ae1380402cc467cced405ba4aa0, 840d99c89f366505d06259a89273f8b1, 4f25e57d4f754f0cea4f30d9da4156fd, 373a7a21c65d50861b0f7fa81d998165, 90bfa1d3b743c1546a053a206e49cac6, 4942b6f7a7b009cf5bb1ef7d31270b98, 733035ba7c294dd365d2a9601b900b4a, 471cb7869b9c4078717156e809e24001, 719000d0db27119867daf91dd1e8a20b, 2ec9ad510241a00a53f3090af9899250
Emails	cadillac[.]407@aol[.]com, OttoZimmerman@protonmail[.]ch, ofizducwe111988@aol[.]com, FobosAmerika@protonmail[.]ch, posiccimen1982@aol[.]com, kipp[.]swindlehurst@aol[.]com, lachneyorlachb@aol[.]com, abbott_wearing@aol[.]com, decryptyourfiles@firemail[.]cc, 1decryption1[@]protonmail[.]com[.], AlbetPattisson1981@protonmail[.]com,

TYPE	VALUE
Emails	henryk@onionmail[.]org, atomicday@tuta[.]io, info@fobos[.]one, axdus@tuta[.]io, it.issues.solving@outlook[.]com, barenuckles@tutanota[.]com, JohnWilliams1887@gmx[.]com, Bernard.bunyan@aol[.]com, jonson_eight@gmx[.]us, bill.g@gmx[.]com, joshuabernandead@gmx[.]com, bill.g@msgsafe[.]io, LettoIntago@onionmail[.]com, bill.g@onionmail[.]org, Luiza.li@tutanota[.]com, bill.gTeam@gmx[.]com, MatheusCosta0194@gmx[.]com, blair_lockyer@aol[.]com, mccreight.ellery@tutanota[.]com, CarlJohnson1948@gmx[.]com, megaport@tuta[.]io, cashonlycash@gmx[.]com, miadowson@tuta[.]io, chocolate_muffin@tutanota[.]com, MichaelWayne1973@tutanota[.]com, claredrinkall@aol[.]com, normanbaker1929@gmx[.]com, clausmeyer070@cock[.]li, nud_satanakia@keemail[.]me, colexpro@keemail[.]me, please@countermail[.]com, cox.barthel@aol[.]com, precorpman@onionmail[.]org, crashonlycash@gmx[.]com, recovery2021@inboxhub[.]net, everymoment@tuta[.]io, recovery2021@onionmail[.]org, expertbox@tuta[.]io, SamuelWhite1821@tutanota[.]com, fastway@tuta[.]io, SaraConor@gmx[.]com, fquatela@techie[.]com, secdatltd@gmx[.]com, fredmoneco@tutanota[.]com, skymix@tuta[.]io, getdata@gmx[.]com, sory@countermail[.]com, greenbookBTC@gmx[.]com, spacegroup@tuta[.]io, greenbookBTC@protonmail[.]com, stafordpalin@protonmail[.]com, helperfiles@gmx[.]com,

TYPE	VALUE
Emails	starcomp@keemail[.]me, helpermail@onionmail[.]org, xdone@tutamail[.]com, helpfiles@onionmail[.]org, xgen@tuta[.]io, helpfiles102030@inboxhub[.]net, xspacegroup@protonmail[.]com, helpforyou@gmx[.]com, zgen@tuta[.]io, helpforyou@onionmail[.]org, zodiacx@tuta[.]io
IPv4	104[.]26[.]5[.]223, 185[.]112[.]82[.]235, 185[.]112[.]82[.]236, 185[.]112[.]82[.]237, 194[.]165[.]16[.]4, 45[.]9[.]74[.]14, 147[.]78[.]47[.]224, 185[.]202[.]0[.]111, 185[.]202[.]0[.]111
URLs	hxxps://paste[.]ee/r/1q1gD hxxps://paste[.]ee/r/OwAyf hxxps://www[.]patreon[.]com/ccatss hxxp://178[.]62[.]19[.]66/campo/v/v hxxps://icq[.]im/HORSEMONEY/
File Paths	%LocalAppData%\horsemoney[.]exe, %AppData%\Microsoft\Windows\StartMenu\Programs\Startup\horsemoney[.]exe, %AllUsersProfile%\Microsoft\Windows\StartMenu\Programs\StartUp\horsemoney[.]exe
Registry Keys	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Windows\CurrentVersion\Run\horsemoney, HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Windows\CurrentVersion\Run\horsemoney, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Phobos exe name>, C:/Users\Admin\AppData\Local\directory
Domains	adstat477d[.]xyz, demstat577d[.]xyz, serverxlogs21[.]xyz

Patch Details

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0213

References

https://www.hhs.gov/sites/default/files/overview-phobos-ransomware.pdf

https://www.fortinet.com/blog/threat-research/deep-analysis-the-eking-variant-of-phobos-ransomware

https://www.hivepro.com/surge-in-8base-ransomware-group-activity/

https://www.securin.io/ragnar-locker-ransomware-hits-customer-care-giant-ttec/

https://blogs.blackberry.com/en/2021/09/threat-thursday-phobos-ransomware

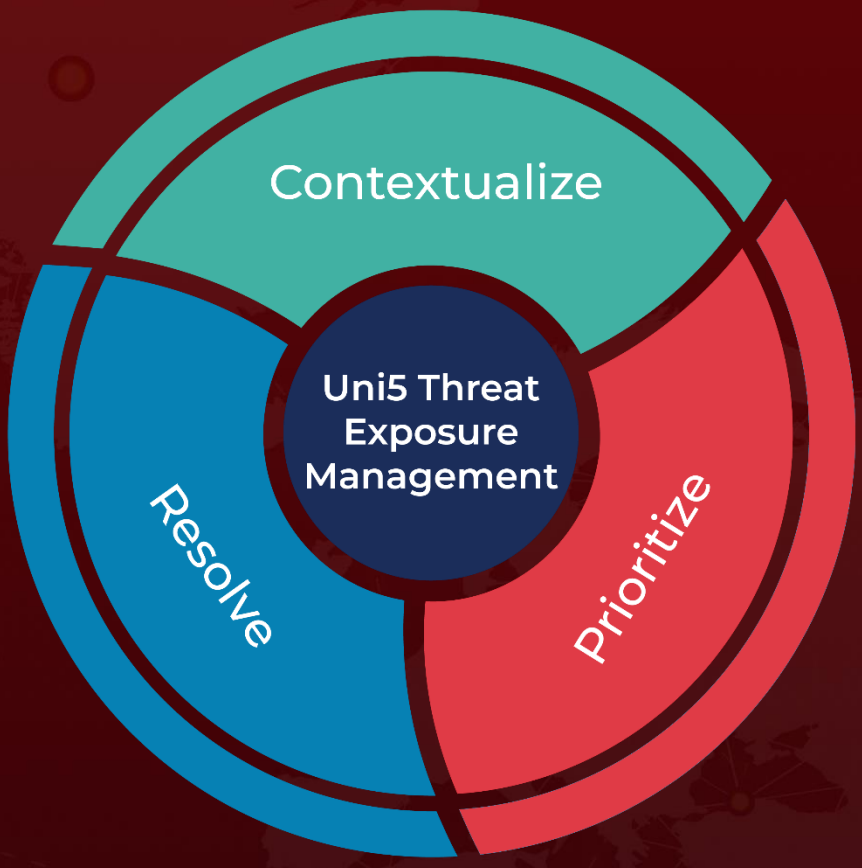
https://twitter.com/pcrisk/status/1592036465139236866

https://www.cisa.gov/sites/default/files/2024-02/aa24-060a-stopransomware-phobos-ransomware_1.pdf

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

October 19, 2023 . 8:00 AM

More at www.hivepro.com