Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

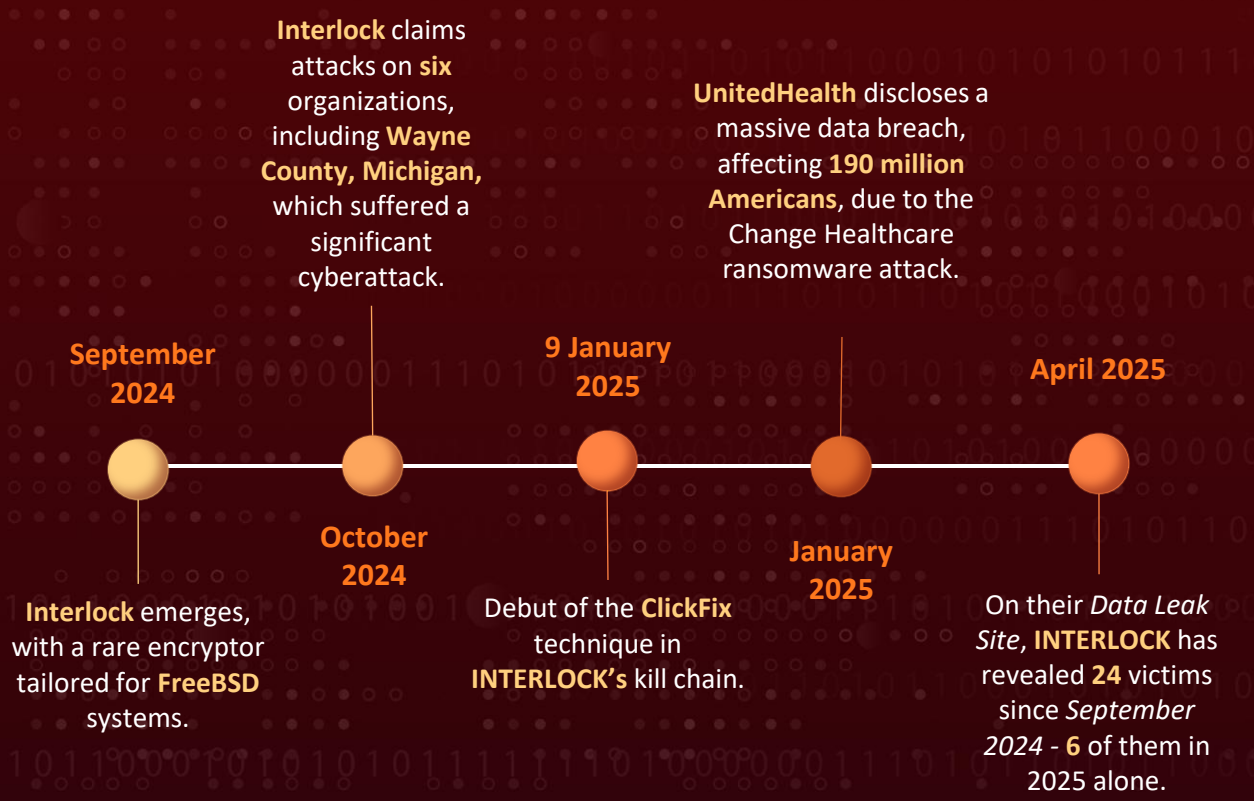
INTERLOCK's Double Punch: Encryption and Exposure at Scale

Date of Publication	Admiralty Code	TA Number
April 18, 2025	A1	TA2025120

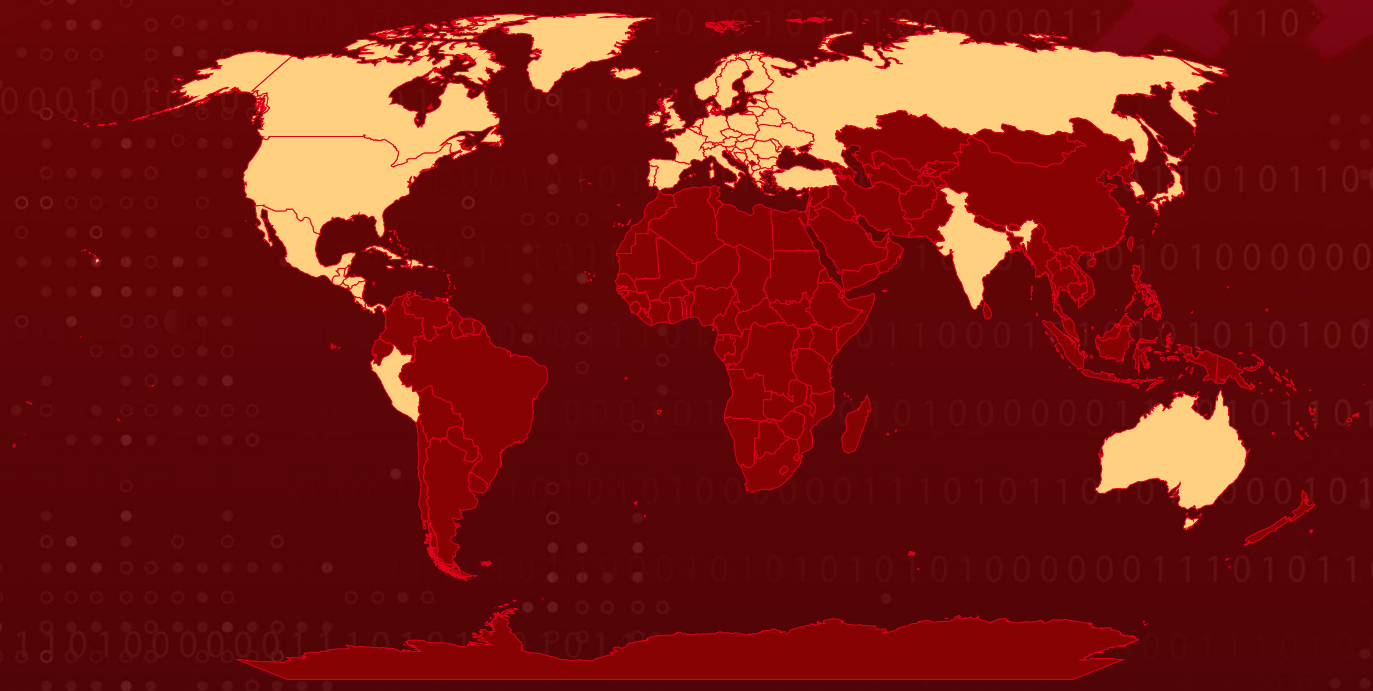
Summary

Active Since: September 2024
Malware: Interlock ransomware, BerserkStealer, LummaStealer
Ransom: $100,000 to $1,000,000
Affected Platforms: Microsoft Windows, Linux
Targeted Industries: Aerospace, Banking, Defense, Education, Engineering, Finance, Food Service, Government, Healthcare, Hospitals, Human Resources, Legal, Manufacturing, Media, Real Estate, Retail, Technology, Transportation
Targeted Regions: North America, Europe, and parts of Asia
Attack: INTERLOCK is a rising ransomware group gaining attention for its uncommon focus on FreeBSD systems and refined double-extortion tactics. By combining technical precision with calculated social engineering and supporting its operations with an active data leak site, INTERLOCK is quickly establishing itself as a notable and methodical player in the modern threat landscape.

Attack Timeline



Attack Regions



Attack Details

#1 A ransomware group known as INTERLOCK first surfaced in September 2024. Since then, the group has employed a double-extortion strategy, encrypting victims' files while simultaneously exfiltrating sensitive data to increase leverage in ransom negotiations.

#2 What sets INTERLOCK apart from other ransomware operators is its unusual focus on FreeBSD systems. The ransomware has been compiled for both Windows and Linux operating systems, with the Windows version, written in C/C++, being more frequently deployed.

#3 The group's infection chain is both strategic and deceptive. INTERLOCK compromises legitimate websites to host fake browser update installers, posing as updates for popular browsers like Google Chrome or Microsoft Edge.

#4 By early 2025, INTERLOCK was seen deploying its ransomware using increasingly sophisticated techniques. On January 9th, a killchain involving the ClickFix method was attributed to the group. ***ClickFix*** is a growing social engineering tactic wherein users are tricked into executing harmful code through fake prompts or CAPTCHA verifications.

#5 This technique has gained traction since August 2024 and has also been used by the North Korean ***Lazarus Group*** and in the ***ClearFake*** infostealer campaign. INTERLOCK, in particular, uses this method to distribute fake installers, further increasing the chances of successful compromise.

#6 Beyond ransomware deployment, the group has enhanced its toolset with additional malware such as LummaStealer and BerserkStealer - credential harvesting tools used to aid lateral movement within compromised networks. Remote access is typically maintained through RDP using stolen credentials, with tools like PuTTY and AnyDesk employed to reinforce control.

#7 To maintain consistency and intimidation, INTERLOCK appends encrypted files with a distinctive extension initially ".interlock," and in more recent versions, ".!NT3R10CK." After encryption, ransom notes are dropped into each directory. The content of these messages has evolved over time, with filenames changing from !__README__!.txt to FIRST_READ_ME.txt and later _QUICK_GUIDE_.txt.

#8 INTERLOCK operates a Data Leak Site (DLS) titled the "Worldwide Secrets Blog," where stolen data is published to coerce payment and shame uncooperative targets. The site also serves as a negotiation portal. INTERLOCK has swiftly established itself as a formidable and innovative player in the ransomware ecosystem.

Recommendations

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Regularly Test Backup Restores: Conduct frequent tests to verify the integrity of backup data and ensure that restoration processes work as intended. This practice helps identify any issues before an actual data recovery scenario arises.

Fortifying Internal Boundaries and External Gateways: Enforce strict egress filtering to block malware from reaching command-and-control (C2) servers. Segment networks to isolate admin, user, and server zones, reducing lateral movement. Deploy IDS/IPS with updated signatures to detect ransomware activity and suspicious encrypted traffic.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact	T1566 Phishing
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1203 Exploitation for Client Execution	T1053 Scheduled Task/Job
T1053.005 Scheduled Task	T1543 Create or Modify System Process	T1037 Boot or Logon Initialization Scripts	T1070 Indicator Removal
T1070.004 File Deletion	T1027 Obfuscated Files or Information	T1036 Masquerading	T1036.005 Match Legitimate Name or Location
T1555 Credentials from Password Stores	T1083 File and Directory Discovery	T1049 System Network Connections Discovery	T1082 System Information Discovery
T1115 Clipboard Data	T1021 Remote Services	T1105 Ingress Tool Transfer	T1005 Data from Local System
T1041 Exfiltration Over C2 Channel	T1486 Data Encrypted for Impact	T1491 Defacement	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	045c041354a6d6b47e91e1124a7dc77397c18e0695ccbc73f87b12a0a1079d46, 04bae0045b86456d6000378a2e37d58b1fa617101543ad23bcec862300b87be3, 05c99f2c1a218ce4a985fd03a3a510c2eaf08ef4772f93ef4f2d5da6cd9b86a1, 074d26b9b128be8e4a77d73dcac31307f28b0e8b8097622c02267be349fe4b4f, 09793a85d372f044fe53c4b47c47049c6bc13d1141334727800b2e32e6d92342, 0fff8fb05cee8dc4a4f7a8f23fa2d67571f360a3025b6d515f9ef37dfdb4e2ea, 1105a3050e6c842fb9411d4f21fd6fdb119861c15f7743e244180a4e64b19b83, 17db9d121fb3eb5033307fdb53df67402bcbc9d8970f45d8142b78c83769b7af, 25a1d86248b7cf5f870dbc9960ce336266473bd40be3a8dcb35e6be88c9df261, 28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f, 299a8ef490076664675e3b52d6767bf89ddfa6accf291818c537a600a96290d2, 2f03b5d1081dfde3d1296dace404b362188b4a941530746d7b14711b42bc53ad, 2faef6a1a0c00f8d44955c243df3c098f0fccd20c59677d274a43023002a4e90, 31f49c74046cc61bf102f3b9f2ce06471b0372d794139325e71c2dacca7bd00a, 33dc991e61ba714812aa536821b073e4274951a1e4a9bc68f71a802d034f4fb9, 351b8a0081fd9f5c35497f5183fb14aef73c1af75628ae689c9218689db01cd9, 39539766ae8f5256e6f21d853b8b7ea8f003d29f6d7cd57d1ecb621dc2b97c89, 3a560ca66f61ba5dceb6016703e0346ff8fe1144bd356a40f740149a2a878fe5, 464ca510a465a38689bd61988b7d366a8fd7e26ca805850b3adb418e95307601, 4672fe8b37b71be834825a2477d956e0f76f7d2016c194f1538139d21703fd6e, 4a97599ff5823166112d9221d0e824af7896f6ca40cd3948ec129533787a3ea9,

TYPE	VALUE
SHA256	5627457a12c562b7a08f634878758d268b9fde44ce35292e887ca13741c5f942, 576d07cc8919c68914bf08663e0afd00d9f9fbf5263b5cccbded5d373905a296, 5c697162527a468a52c9e7b7dc3257dae4ae5142db62257753969d47f1db533e, 5cbc2ae758043bb58664c28f32136e9cada50a8dc36c69670ddef0a3ef6757d8, 60af8899b49013e9deb1d5cac58562d7ed12bfda1187627e9d25714b26218f0d, 61d092e5c7c8200377a8bd9c10288c2766186a11153dcaa04ae9d1200db7b1c5, 61f8224108602eb1f74cb525731c9937c2ffd9a7654cb0257624507c0fdb5610, 62971070d6a8b9fca8a50b9cd8e91545bfcc2c2b6665f134c112081f54e6bf31, 68366ced818508de187167d8f9106be7801b8dcf1f03ae169459c7336d6e69de, 6933141fbdcdcaa9e92d6586dd549ac1cb21583ba9a27aa23cf133ecfdf36ddf, 6e4ca569ab809ba3545860d26180316366803c231a2e3a66b4906adc5826a397, 71f773b4e9178dcedd402c94fb9384aea6312d8a93f95f3f9dc1249fd4933658, 7501623230eef2f6125dcf5b5d867991bdf333d878706d77c1690b632195c3ff, 7890b116d13a52efe696ce1e2c0ed83029775cf4bea836ce551e71d222ee116f, 7d750012afc9f680615fe3a23505f13ab738beef50cd92ebc864755af0775193, 7d9f3701bf6f43ab84ce02ce4915dc0703504263db2e1eb65f4f7c791565f731, 8251186b3196e3fefb0dbfcf71dfccc2c1cd66515686c9af8a6fb48766c739c6, 888842bc1f6fcb354431919080858c623def305bed2214f11b93591859d4dee2, 9031652af104aa207d6dad1c402db86c557323b2567c0cc93d022f01ae926e9a, 91fcf70c1775dcaaaa4d3de17d87d67976b0cec9939dedfb86f093ab388ed3b0, 958ff93e92ee8bed7819555603ea612f263c1b9c673566f5c506288b5318eff8, 9e387f1564f9e38ba87dbafbde3731db2e844ff3800500d6707028bb065c070b, a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642,

TYPE	VALUE
SHA256	a5623b6a6f289bb328e4007385bdb1659407a9e825990a0faaef3625a2e782cf, a760e28145620fccd072a415031cec4036fc09e8530c93d85f5d1509d62fe551, b35da0c1a515286a2b3021cf518140a59a63b470a9d611303304918be9354d68, b36c20c757c4780f89272ce224a29a5a61b6273336789357419 6debde19383fe, b3a512b9f4705d1947fbbbc42accdbd6bd95af1b07cec09d75af501746fecdd5, b85586f95412bc69f3dceb0539f27c79c74e318b249554f0eace45f3f073c039, be6e5cede4e6a8b807062db211eb3e8825a6cc00d71ddf7bcd63971d76219a25, c9920e995fbc98cd3883ef4c4520300d5e82bab5d2a5c781e9e9fe694a43e82f, d1cd8c4574c3290ae16bf4e718c5e89dadef5b2fd4eea2211a19a6180ff8ee5b, d4f3d0446e08dbf1a7ccb6da09e756ff75eae3b04dafe2c2a69d6919052d2ebf, dee5915b76dd3bae3d3cedc0c1d1b055daab5852cba4868c92eb88b9a84a0b00, df41085a8aa9ee9da6a03db08ad910b6ef5fcdc8fee7ebb19744331c5e70c782, e307d3e9b8de59311c692b2ab0ee864f0d469066e041141d577b65b43a4b3ffa, e668e30b4e111e16b4017cd49dd90c39f9988f8a44cd9cc16b95b7b451862b74, e69491a61ebc4a9ffc17884063c69a5489a83dd6d71295b4216962a43242a6c8, e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1, e9ff4d40aeec2ff9d2886c7e7aea7634d8997a14ca3740645fd3101808cc187b, eaca86a3f397d10d9188be9fcd2af1a7a30a9b573b2282b0b8300efeb5ff1efd, eb1cdf3118271d754cf0a1777652f83c3d11dc1f9a2b51e81e37602c43b47692, eb587b2603dfc14b420865bb862fc905cb85fe7b4b5a781a19929fc2da88eb34, f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e, f02622129e7774b7673e2a9f62bb4a208d4a142b5d925532c7920481549bd07b, f1df43fe0f95de6badfb710827cdc7272e6654f108ef2cfcb2a01aca089f0624,

TYPE	VALUE
SHA256	f613966b6ed1f080aacba005b1e48268ef662fffdf9894382299645f42900848, f6c7ecff7b07cba12bd79833a23d12d5fcd12a75a3394d923b994ba0ed535db3, f962e15c6efebb3c29fe399bb168066042b616affddd83f72570c979184ec55c, fdd4e0bb2a4475e4e44154d7bf29490de98496553af3c8807f999ab8b920263f
IPv4	140[.]82[.]14[.]117, 159[.]223[.]46[.]184, 168[.]119[.]96[.]41, 177[.]136[.]225[.]153, 188[.]34[.]195[.]44, 193[.]149[.]180[.]158, 195[.]201[.]21[.]34, 206[.]206[.]123[.]65, 212[.]104[.]133[.]72, 212[.]237[.]217[.]182, 216[.]245[.]184[.]170, 216[.]245[.]184[.]181, 23[.]227[.]203[.]162, 23[.]95[.]182[.]59, 45[.]61[.]136[.]202, 49[.]12[.]102[.]206, 49[.]12[.]69[.]80, 5[.]252[.]177[.]228, 64[.]94[.]84[.]85, 65[.]108[.]80[.]58, 65[.]109[.]226[.]176, 65[.]38[.]120[.]47, 80[.]87[.]206[.]189, 84[.]200[.]24[.]41, 85[.]239[.]52[.]252, 96[.]62[.]214[.]11
Domains	analytical-russell-cincinnati-settings[.]trycloudflare[.]com, bristol-weed-martin-know[.]trycloudflare[.]com, california-appeals-pilot-harper[.]trycloudflare[.]com, casting-advisors-older-invitations[.]trycloudflare[.]com, complement-parliamentary-chairs-hc[.]trycloudflare[.]com, fotos-phillips-princess-baker[.]trycloudflare[.]com, investigators-boxing-trademark-threatened[.]trycloudflare[.]com, lancaster-sean-initial-ru[.]trycloudflare[.]com, medicine-podcasts-halo-expected[.]trycloudflare[.]com, mortgage-i-concrete-origins[.]trycloudflare[.]com, musicians-implied-less-model[.]trycloudflare[.]com,

TYPE	VALUE
Domains	open-exceptions-cleared-feelings[.]trycloudflare[.]com, photo-auction-visual-gains[.]trycloudflare[.]com, pipe-hawaii-monkey-automatic[.]trycloudflare[.]com, refrigerator-cheers-indicator-ferrari[.]trycloudflare[.]com, scientific-shown-desperate-ratio[.]trycloudflare[.]com, securities-variance-vocal-temporal[.]trycloudflare[.]com, speak-head-somebody-stays[.]trycloudflare[.]com, strain-brighton-focused-kw[.]trycloudflare[.]com, sublime-forecasts-pale-scored[.]trycloudflare[.]com, suffering-arnold-satisfaction-prior[.]trycloudflare[.]com, una-idol-ta-missile[.]trycloudflare[.]com, views-ethics-orientation-roommate[.]trycloudflare[.]com, washing-cartridges-watts-flags[.]trycloudflare[.]com, www[.]sublime-forecasts-pale-scored[.]trycloudflare[.]com
URLs	hxxp[:]//162[.]55[.]47[.]21[:]8080/1742688720, hxxp[:]//45[.]61[.]136[.]228[:]8080/recaptha, hxxp[:]//64[.]95[.]10[.]95[:]8080/misteams, hxxp[:]//64[.]95[.]10[.]95[:]8080/recaptch, hxxp[:]//topsportracing[.]com/az10, hxxp[:]//topsportracing[.]com/wp-az, hxxps[:]//advanceipscaner[.]com/additional-check[.]html, hxxps[:]//airbluefootgear[.]com/wp-includes/images/xits[.]php, hxxps[:]//album-anthony-rn-submission[.]trycloudflare[.]com/25423565, hxxps[:]//apple-online[.]shop/ChromeSetup[.]exe hxxps[:]//apple-online[.]shop/MSTeamsSetup[.]exe, hxxps[:]//apple-online[.]shop/MicrosoftEdgeSetup[.]exe, hxxps[:]//dc-broader-green-norwegian[.]trycloudflare[.]com/12341234, hxxps[:]//diff-beats-belize-chapter[.]trycloudflare[.]com/12341234, hxxps[:]//ecologilives[.]com/additional-check[.]html, hxxps[:]//forest-offensive-height-lexxers[.]trycloudflare[.]com/12341234, hxxps[:]//lcd-add-palace-switching[.]trycloudflare[.]com/12341234, hxxps[:]//metro-offset-imposed-behind[.]trycloudflare[.]com/ytjstast, hxxps[:]//microsoft-msteams[.]com/additional-check[.]html, hxxps[:]//microsxxeams[.]com/additional-check[.]html, hxxps[:]//phones-pichunter-businesses-drop[.]trycloudflare[.]com/12341234, hxxps[:]//pub-motorola-viking-charger[.]trycloudflare[.]com/12341234, hxxps[:]//santa-reflection-capitol-classifieds[.]trycloudflare[.]com/12341234, hxxps[:]//spa-step-hopkins-islands[.]trycloudflare[.]com/erfgtrxx, hxxp[:]//23[.]95[.]182[.]59/31279geuwtoisgdehbiuowaehsgdb/cht,

TYPE	VALUE
URLs	hxxp[:]//23[.]95[.]182[.]59/31279geuwtoisgdehbiuowaehsgdb/klg, hxxps[:]//apple-online[.]shop/ChromeSetup[.]exe, hxxps[:]//rvthereyet[.]com/wp-admin/images/rsggj[.]php
TOR Address	ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion
Email	interlock[@]2mail[.]co

Recent Breaches

https://andrettikarting.com/
https://domanbm.com/
https://driveproducts.com/
https://domanbm.com/
https://www.cherokee1.org/
https://www.nationaldefensecorp.com/
https://www.generalformulations.com/
https://www.pmacanada.com/
https://www.aztecschools.com/
https://hancock.k12.mn.us/
https://www.waynecounty.com/
https://www.smeg.com/
https://siegelcompanies.com/

References

https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/

https://www.fortinet.com/blog/threat-research/ransomware-roundup-interlock

https://hivepro.com/threat-advisory/clickfix-con-phishing-scam-turns-video-calls-into-malware-havens/

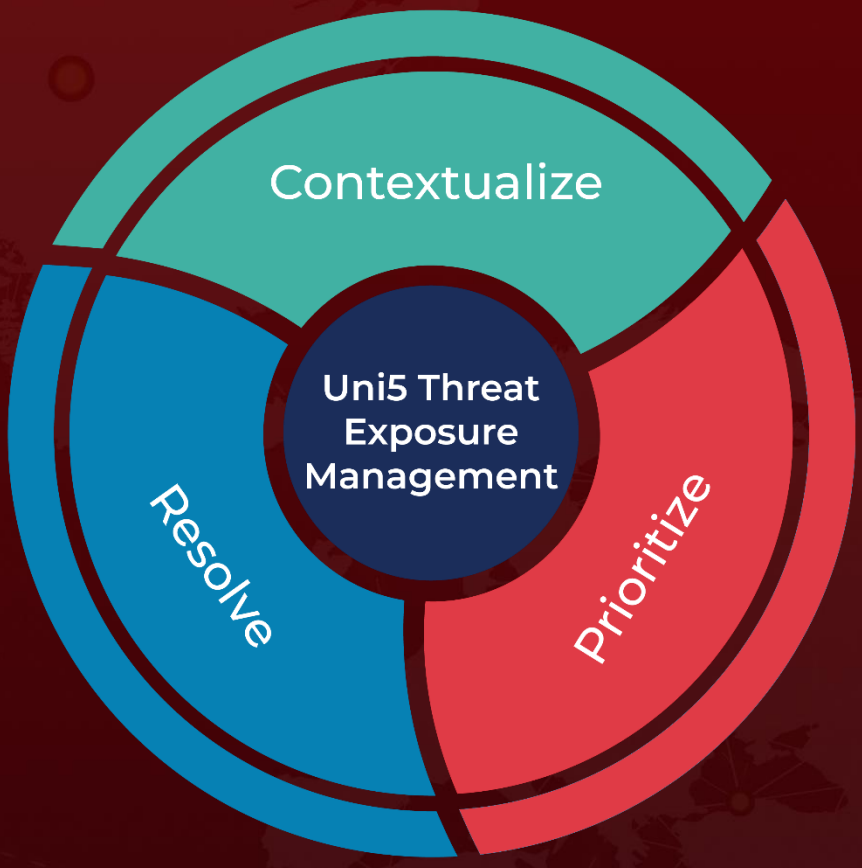
https://hivepro.com/threat-advisory/clearfake-blockchain-powered-malware-lures-thousands-with-fake-security-prompts/

https://hivepro.com/threat-advisory/clickfake-interview-lazarus-groups-new-crypto-heist-via-fake-job-offers/

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

April 18, 2025 • 6:00 AM

More at www.hivepro.com