Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

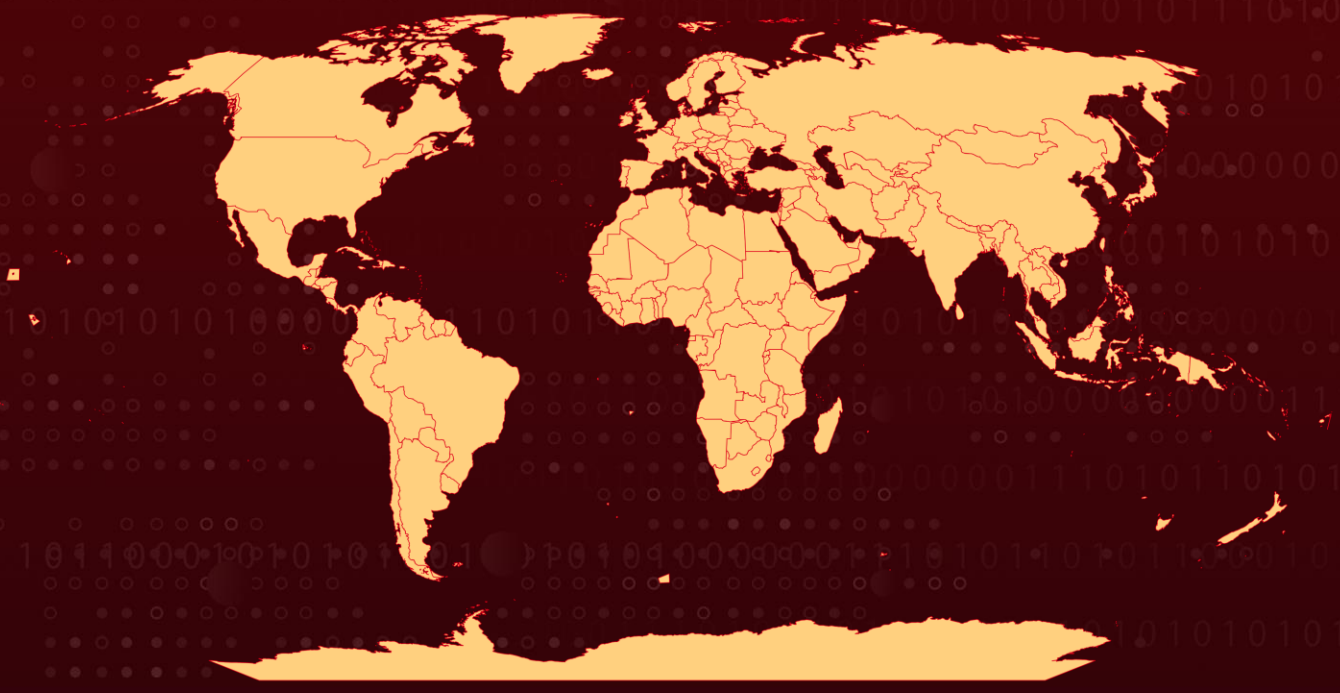
Ebury A Potent Linux Botnet Infects Over 400K Servers

Date of Publication	Admiralty Code	TA Number
May 16, 2024	A1	TA2024190

Summary

First Seen: 2009
Targeted Regions: Worldwide
Malware: Ebury Botnet
Affected Platform: Linux
Attack: A large malware campaign targeting Linux servers, called Ebury, has been active since 2009. Over 400,000 servers have been compromised historically, with over 100,000 still infected at the end of 2023. This financially motivated malware allows attackers to steal cryptocurrency and credit card information. Ebury is a versatile threat, capable of stealing credentials, spreading spam, redirecting web traffic, and even granting complete control of compromised servers.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	MICRO PATCH
CVE-2021-45467	CentOS Web Panel Pre-Authentication File Inclusion Vulnerability	CentOS Web Panel	✗	✗	✓
CVE-2016-5195	Dirty COW (Linux Kernel Race Condition Vulnerability)	Linux Kernel	✓	✓	✓

Attack Details

#1

Ebury is a sophisticated Linux malware botnet that has been infecting Linux servers, first documented over a decade ago as part of a campaign named “Operation Windigo”. It's estimated to have compromised over 400,000 servers since 2009, with more than 100,000 still infected as of late 2023. Ebury targets servers across various sectors, including shared hosting providers and those hosting cryptocurrency wallets, aiming for financial gain by stealing credentials, redirecting web traffic for spam, and harvesting valuable financial data like credit cards and cryptocurrency.

#2

Ebury uses a variety of sneaky tactics to infect systems, including exploiting software vulnerabilities, using stolen credentials, and even hiding behind fake identities. Once inside a server, Ebury can steal login information, act as a backdoor for further attacks, and deploy additional tools to steal credit card details and reroute traffic.

#3

Ebury's latest version 1.8, emerged in late 2023, boasting enhanced sophistication with new obfuscation techniques and a domain generation algorithm (DGA). These advancements fortify its ability to evade detection and endure blocking attempts. Recent malware modules affiliated with Ebury, per ESET, include HelimodProxy, facilitating traffic proxying and spam campaigns, HelimodRedirect, which diverts HTTP traffic to malicious sites, HelimodSteal, targeting sensitive data from web forms, KernelRedirect, manipulating HTTP traffic at the kernel level, and FrizzySteal, intercepting and exfiltrates HTTP requests.

#4

Additionally, Ebury has expanded its monetization efforts by deploying multiple malware families to steal financial details from transactional websites. Updates to Ebury itself, such as new obfuscation techniques and a userland rootkit, further enhance its ability to evade detection. Despite efforts to thwart it, Ebury remains a potent threat in the cybersecurity landscape.

Recommendations

Regular Software Updates: Ensure that all software and applications running on servers are regularly updated to patch known vulnerabilities. Regular updates can help mitigate the risk of exploitation by malware like Ebury, which often leverages software vulnerabilities for infiltration.

Strong Authentication Practices: Enforce strong authentication practices such as multi-factor authentication (MFA) and regular password changes to prevent unauthorized access via stolen credentials. Implementing robust access controls can help mitigate the risk of Ebury using stolen credentials to infiltrate servers.

Network Monitoring and Intrusion Detection: Implement robust network monitoring and intrusion detection systems to detect suspicious activity indicative of Ebury's presence. This includes monitoring for unusual network traffic patterns, unexpected system behaviors, and unauthorized access attempts.

Endpoint Detection and Response (EDR): Utilize EDR solutions in block mode to detect and block malicious artifacts associated with Ebury. EDR enhances threat detection and response capabilities.

Implement Attack Surface Reduction: Employ attack surface reduction rules to prevent common attack techniques used by Ebury. These measures can help in blocking credential stealing from critical system components.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0010 Exfiltration	TA0040 Impact	T1190 Exploit Public-Facing Application	T1078 Valid Accounts

T1565.002 Transmitted Data Manipulation	T1565 Data Manipulation	T1592.002 Software	T1592 Gather Victim Host Information
T1592.004 Client Configurations	T1583.006 Web Services	T1583 Acquire Infrastructure	T1583.001 Domains
T1583.004 Server	T1583.003 Virtual Private Server	T1584.004 Server	T1584 Compromise Infrastructure
T1587 Develop Capabilities	T1587.004 Exploits	T1587.001 Malware	T1059.004 Unix Shell
T1059 Command and Scripting Interpreter	T1609 Container Administration Command	T1129 Shared Modules	T1554 Compromise Client Software Binary
T1574 Hijack Execution Flow	T1574.006 Dynamic Linker Hijacking	T1068 Exploitation for Privilege Escalation	T1562.004 Disable or Modify System Firewall
T1562.001 Disable or Modify Tools	T1562 Impair Defenses	T1562.006 Indicator Blocking	T1070 Indicator Removal
T1070.002 Clear Linux or Mac System Logs	T1070.006 Timestomp	T1036 Masquerading	T1036.005 Match Legitimate Name or Location
T1027 Obfuscated Files or Information	T1027.001 Binary Padding	T1027.002 Software Packing	T1027.007 Dynamic API Resolution
T1014 Rootkit	T1622 Debugger Evasion	T1556 Modify Authentication Process	T1557 Adversary-in-the-Middle
T1110 Brute Force	T1110.001 Password Guessing	T1110.004 Credential Stuffing	T1557.002 ARP Cache Poisoning
T1212 Exploitation for Credential Access	T1040 Network Sniffing	T1003.008 /etc/passwd and /etc/shadow	T1003 OS Credential Dumping

T1552 Unsecured Credentials	T1552.001 Credentials In Files	T1552.004 Private Keys	T1018 Remote System Discovery
T1082 System Information Discovery	T1016.001 Internet Connection Discovery	T1016 System Network Configuration Discovery	T1021 Remote Services
T1056 Input Capture	T1056.004 Credential API Hooking	T1021.004 SSH	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1568.002 Domain Generation Algorithms	T1568 Dynamic Resolution	T1568.003 DNS Calculation
T1573 Encrypted Channel	T1573.002 Asymmetric Cryptography	T1090.003 Multi-hop Proxy	T1048 Exfiltration Over Alternative Protocol
T1048.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	T1041 Exfiltration Over C2 Channel	T1560.001 Archive via Utility	T1560 Archive Collected Data

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	98FBD545B5C1B1FE185730BA9B1CD4BEBFAE4476, 44B04CFC095F93D17B1BD4F8820C16843FCBAC3E, 013647E5AD347539EEF6C5933B16AD01B1806C3C, 787A93F86E7F5FCF922E996B577DF532270C7184, E7DEBD6E453192AD8376DB5BAB03ED0D87566591, CD9A5B823906CC620B28D69DBDB11BD9FE6B3E03, DDAE9417470F832DB550EFB716B5BAEAAAA35372, 71CA9B7C418264C2C856D47483666D123861D476, 4A7303DD8E7BBBF063463B3852245ABDD343F5B6, DFAECF7EBFC169CDF923AF421EDD537CCE536A64, 3137DCA3F6FBD566F4ED2F49076A63D84869E13C, 96FD9B3064F04EE3063B2B103F856BB729B58749, 53829463A7DE8C4BACE97B1F6925728F3421DF53, 947EEE633E9347F72625FB652F94488A4B2B37F0, E39667AA137E315BC26EAEF791CCAB52938FD809,

TYPE	VALUE
SHA1	0B91C3C2627F9948B8F3446822F99FAF88081267, 580E6075C65D867667D507E2B00C8EEF79C907A1, 3988D1A743E83D532130BC8090A7BC7001FE1BB0, 429A81BBD18A35C3C4D1DCB8BC76F5A7D9724A79, 16EE09926A2109262686D58974079ADC25E31AA1, EC4941BDD9FFB241968FD59A28B70BCE288ED261, A64D6C7444FC2404A589ED7F8527E698682A3E68, 15560B44286122FA0679C6C2368817CE2DC747E6, 94532111459E024BCB7E2025A6C145876A46F829, AD350D7DA4BF1F7080026B683F93401CD735E974, 75E8A197B6A9A7903CA43782BDD77CD9611FEFE0, CFB48909B978E91CFC6FFCAF2E4B04F27F503B34, D39959356283DB4B3184BDB15E890E74CF1EA65C, 070F85BF02AD3FB0978785B3272D7B08F5C47A1A, 10F94157365E6A1BBB101B3222EE3C3C675B9829, 12666F2FBEFC55F1DDB4BA86B5D85DB733889162, 22BB2E0D1E1B0B009464E2919A381C4951D7D90D, 2DBF91347FA987E6199DAE5141641D04D0C963FF, 535C5588ED2EF9A4E960882C23E3104E81F2C079, AA0EC27C26E5484B4EB23D8424B2412221D5C7FC, 4F92498FB8C1BFED97F18CFB7B36AF899F70F582, 12EA4595C6F38E60C23F09B2F08D78BA6EB0C1B3, 1918E40580291D0299A78DDFB9123923F832CEB3, 20599D89E4F648CF0F6EB46DEE67DB63984A8C36, 6FF132E50EFA5ABF534A005CB58C9C5B5FC39BEC, 9569A8411477305FACA78E1C944D479EFA028DFB, BCC3B83CFADBD58256FC41AF9F0BFF50AC1F148B, D392022D8B72BCDDB849A94829C87731874E94AC, D3D6567862B4B7811BEA76BE117E901B2B6B8399, D901D65F7A7A49296A501420F6D32BBF968F5BDE, ED5662F3CF80B8108D2172FBCA6119E403205EAA, EDD2DE0FAFE84EA51029FFDE38ACBB5918108DF5, FD6709AF6A8DC384B101A8E9ED36C1092533C404, 04FF6202534A394586D826B320645AEC24CE7AA5, 32BB38D7D6B03DB4779E7A7183E7FA42DFBAFFC2, 59F238DA1FD822AAD6FA7DF78D823854EAF8762E, 6369AD38D39562DD9D6D3E2612496A5357FFC09B, 67C1905EF4D0422DBDFAC41DC80F9C4D5C69E288, 6BEE8F88F3F145170CEF58D9F790DDD99CDFA547, 72048DEABE7F37BBECBFDA1570E1AB6B366B72BD, 907822012D6A970D676B634903F099587ED9C335, 9209D757770AAFCA0B84B9F63B8769DF8CAC3F1A, D8647E825EFE74BF1726C0C494E3C2588FFF2262, 5c796dc566647dd0db74d5934e768f4dfafec0e5, 615c6b022b0fac1ff55c25b0b16eb734aed02734, d4eeada3d10e76a5755c6913267135a925e195c6, 27ed035556abeeb98bc305930403a977b3cc2909, 2f382e31f9ef3d418d31653ee124c0831b6c2273,

TYPE	VALUE
SHA1	7248e6eada8c70e7a468c0b6df2b50cf8c562bc9, e8d3c369a231552081b14076cf3eaa8901e6a1cd, 1d3aafce8cd33cf51b70558f33ec93c431a982ef, a559ee8c2662ee8f3c73428eaf07d4359958cae1, 17c40a5858a960afd19cc02e07d3a5e47b2ab97a, eb352686d1050b4ab289fe8f5b78f39e9c85fb55, 44b340e90edba5b9f8cf7c2c01cb4d45dd25189e, e8d392ae654f62c6d44c00da517f6f4f33fe7fed, b58725399531d38ca11d8651213b4483130c98e2, 98cdbf1e0d202f5948552cebaa9f0315b7a3731d , 4d12f98fd49e58e0635c6adce292cc56a31da2a2 , 0daa51519797cefedd52864be0da7fa1a93ca30b , 7314eadbdf18da424c4d8510afcc9fe5fcb56b39 , 575bb6e681b5f1e1b774fee0fa5c4fe538308814 , fa6707c7ef12ce9b0f7152ca300ebb2bc026ce0b , c4c28d0372aee7001c44a1659097c948df91985d , 267d010201c9ff53f8dc3fb0a48145dc49f9de1e , 471ee431030332dd636b8af24a428556ee72df37 , 58f185c3fe9ce0fb7cac9e433fb881effad31421 , 09c8af3be4327c83d4a7124a678bbc81e12a1de4 , 2fc132440bafdbc72f4d4e8dcb2563cc0a6e096b , 39ec9e03edb25f1c316822605fe4df7a7b1ad94a , 3c5ec2ab2c34ab57cba69bb2dee70c980f26b1bf , 74aa801c89d07fa5a9692f8b41cb8dd07e77e407 , 7adb38bf14e6bf0d5b24fa3f3c9abed78c061ad1 , 899b860ef9d23095edb6b941866ea841d64d1b26 , 8daad0a043237c5e3c760133754528b97efad459 , 8f75993437c7983ac35759fe9c5245295d411d35 , 9bb6a2157c6a3df16c8d2ad107f957153cba4236 , a7b8d06e2c0124e6a0f9021c911b36166a8b62c5 , adfcd3e591330b8d84ab2ab1f7814d36e7b7e89f , b8508fc2090ddee19a19659ea794f60f0c2c23ff , bbce62fb1fc8bbed9b40cfb998822c266b95d148 , bf1466936e3bd882b47210c12bf06cb63f7624c0 , e14da493d70ea4dd43e772117a61f9dbcff2c41c , f1ada064941f77929c49c8d773cbad9c15eba322 , 9e2af0910676ec2d92a1cad1ab89029bc036f599 , 5d3ec6c11c6b5e241df1cc19aa16d50652d6fac0 , d552cbadee27423772a37c59cb830703b757f35e , 1a9aff1c382a3b139b33eeccae954c2d65b64b90 , 2e571993e30742ee04500fbe4a40ee1b14fa64d7 , e2a204636bda486c43d7929880eba6cb8e9de068 , 0004b44d110ad9bc48864da3aea9d80edfceed3f, 03592b8147e2c84233da47f6e957acd192b3796a, 0eb1108a9d2c9fe1af4f031c84e30dcb43610302, 10c6ce8ee3e5a7cb5eccf3dffd8f580e4fb49089, 149cf77d2c6db226e172390a9b80bc949149e1dc,

TYPE	VALUE
SHA1	1972616a731c9e8a3dbda8ece1072bd16c44aa35, 24e3ebc0c5a28ba433dfa69c169a8dd90e05c429, 4f40bb464526964ba49ed3a3b2b2b74491ea89a4, 5b87807b4a1796cfb1843df03b3dca7b17995d20, 62c4b65e0c4f52c744b498b555c20f0e76363147, 78c63e9111a6701a8308ad7db193c6abb17c65c4, 858c612fe020fd5089a05a3ec24a6577cbeaf7eb, 9018377c0190392cc95631170efb7d688c4fd393, a51b1835abee79959e1f8e9293a9dcd8d8e18977, a53a30f8cdf116de1b41224763c243dae16417e4, ac96adbe1b4e73c95c28d87fa46dcf55d4f8eea2, dd7846b3ec2e88083cae353c02c559e79124a745, ddb9a74cd91217cfcf8d4ecb77ae2ae11b707cd7, ee679661829405d4a57dbea7f39efeb526681a7f, fc39009542c62a93d472c32891b3811a4900628a, fdf91a8c0ff72c9d02467881b7f3c44a8a3c707a, 42123cbf9d51fb3dea312290920b57bd5646cefb, ebc45dd1723178f50b6d6f1abfb0b5a728c01968, 5bdf483279a4a816ed4f8a235e799d5068d14f64, bd867907a5059ab1850918d24b4b9bbe33c16b76, a0f18b5ee2d347961b7109a22ea06cca962693d2, 74cd5ae9f6bbdf27b4eaf45c4a22c6aae07345a2, 5196a8a034611aaa112232767aafd74b8ef71279, 20467521bfd58e9ed388ce83467d73e8fd0293a7, f634f305a655b06f2647b82b58f7d3920546ac89, 25a819d658d02548b2e5bdb52d2002df2f65b03a, 6180d8c1c6967d15a0abb0895103ccc817e43362, 051a89a7a335062829a8e938b8d4e3e2b532f6ff, 035327b42f6e910b652bbdde5d9c270cfbaa9669, 1dd7a18125353d426b5314c4ba04d60674ffa837
IPv4	45[.]59[.]120[.]146, 141[.]255[.]166[.]187, 146[.]70[.]124[.]102, 185[.]59[.]103[.]8, 195[.]123[.]225[.]83, 213[.]232[.]235[.]104, 185[.]145[.]245[.]167, 135[.]181[.]148[.]230, 141[.]164[.]52[.]243
File path	/dev/event-E4LgEFWIcy, /dev/event/loop0, /dev/stats-MxPAxNpy3x, /proc/udevd, /proc/ulog, /run/systemd/journal-YAjXO8luqOa, /run/systemd/journal/dlog, /run/systemd/log,

TYPE	VALUE
File path	/run/systemd/log-90zMvYX7uL, /run/systemd/log-wuO3nuFBHN, /tmp/dbus-0m9eDQpdXZ, /tmp/dbus-9XZXkmdfpN, /tmp/dbus-VdyGBaqZws, /tmp/dbus-Xrga2cOewg, /tmp/dbus-ZP7tFO4xsL, /tmp/dbus-kZ8VEtJDOJ, /tmp/dbus-luzG4UqDt8, /tmp/dbus-n3UUkeqEZG, /tmp/dbus-vBWUDhHCHp, /bin/hostname, /bin/sync, /sbin/auditd, /sbin/rsyslogd, /sbin/udevd, /usr/lib/systemd/systemd-udevd, /usr/sbin/acpid, /usr/sbin/anacron, /usr/sbin/arpd, /usr/sbin/atd, /usr/sbin/crond
File name	libstz[.]so, libkeyutils[.]so, libllz564, libsbr[.]so, libkeystats[.]so, librwctl[.]so, ibz[.]so, mod_dir[.]so, mod_auth_basic[.]so, mod_authn_file[.]so, mod_authz_host[.]so, mod_authz_user[.]so, mod_env[.]so, iptables-multi-1[.]4[.]7, iptables-multi, nf_conntrack6[.]ko, libcurl[.]so[.]4[.]6[.]0, libcurl[.]so[.]4[.]4[.]0, libcurl[.]so[.]4[.]5[.]0, libns2[.]so, libns5[.]so, libpw3[.]so, libpw5[.]so, libslr[.]so, libkeyutils[.]so[.]1[.]5

TYPE	VALUE
Domains	o5o8c1berdn[.]net, mag8u1tejdt[.]biz, a1t9y1xendd[.]info, map9u1tejdt[.]net, o5tac1berdn[.]biz, k2zbz1yeodm[.]info, a1hcy1xendd[.]net, k2rdz1yeodm[.]biz, o5dec1berdn[.]info, maefu1tejdt[.]net, a1z1h2xendd[.]biz, mae2d2tejdt[.]info, o5e4l2berdn[.]net, k2t6i2yeodm[.]biz, a1k8h2xendd[.]info, k2qai2yeodm[.]net, o5lcl2berdn[.]biz, maved2tejdt[.]info, q5ncv0dekcm8a1p[.]biz, oaxey7m0lde8s1v[.]info, c1b1jfi2pdi8w1f[.]net, oap3p6f5lde8s1v[.]biz, q5y6vdf7tdm8a1p[.]info, m2w9c4qaqdj8x1o[.]net, c1jczbhcpdi8w1f[.]biz, m2lfk2jfqdj8x1o[.]info, q5o2uad1cem8a1p[.]net, oah5w1w4uee8s1v[.]biz, c1v9l8s6yei8w1f[.]info, oafcffg8uee8s1v[.]net, q5w0g7cbcem8a1p[.]biz, m2d4berdzej8x1o[.]info, c1m8k5q0hfi8w1f[.]net, m2kcjcj2ifj8x1o[.]biz, q5w0f4n5lfm8a1p[.]info, oay4vbx7dfe8s1v[.]net, c1v9j2pahfi8w1f[.]biz, o8rad5ccx9f3r[.]net, zbqaf5zcv9s3x[.]biz, c0dbq5vcj9o3e[.]info, x7sbu5hcg9b3f[.]net, h0nct5rca9y3f[.]biz, ubjcl5ucn9g3m[.]info, f8wda5yck9i3h[.]net, m7lea5yck9i3l[.]biz, b8dfs5ecw9p3o[.]info, abo0u6ach9k3w[.]net, idkff7m1lac3g[.]biz,

TYPE	VALUE
Domains	u2s0k8d1ial3r[.]info, h9g0q8a1hat3s[.]net, f2y1j8v1saa3t[.]biz, xdc1h8n1baw3m[.]info, raj2p8z1aae3b[.]net, o9f3v8r1oaj3p[.]biz, tav4h8n1baw3r[.]info, hdm5o8e1tas3n[.]net, v2a7q8a1hat3u[.]biz, z9w8l8k1zaf3g[.]info, y2fad8b1gak3f[.]net, odrbz8i1jap3e[.]biz, uajdm8w1kax3j[.]info, c9xfb8u1cad3m[.]net, fas1k9i1jap3u[.]biz, zdm3u9x1fag3i[.]info, b2z6m9k1zaf3v[.]net, qimpj6kkofzf[.]biz, op3f1libgh[.]biz, larfj7g1vaz3y[.]net, pbarsec[.]com, checklicence[.]net

Patch Links

https://control-webpanel.com/changelog

http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=19be0eaffa3ac7d8eb6784ad9bdbc7d67ed8e619

References

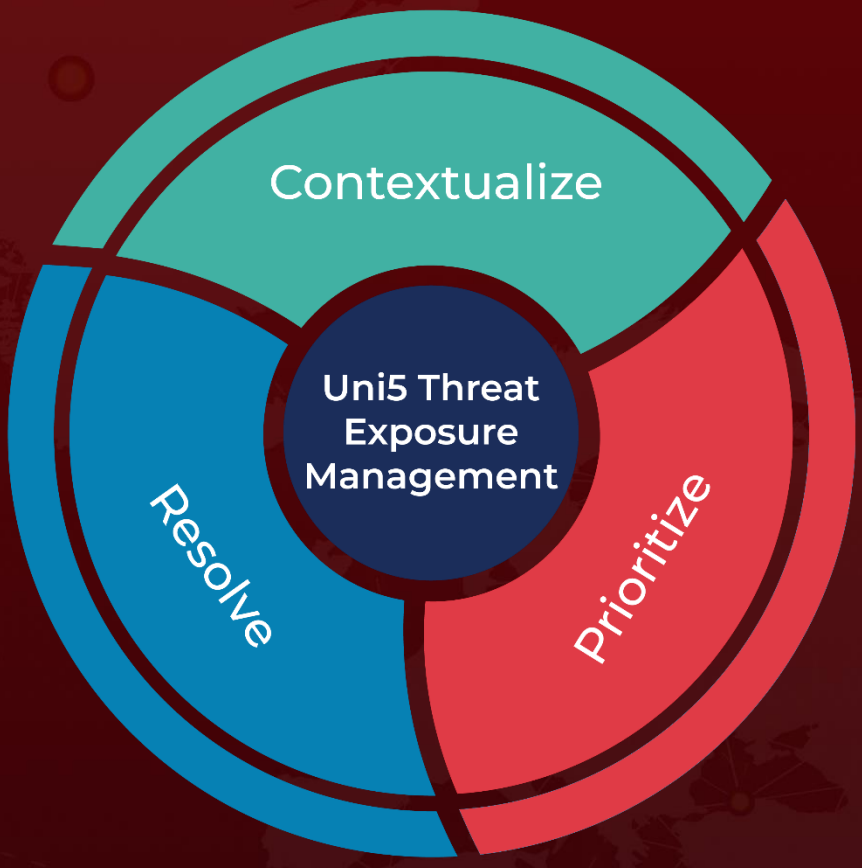
https://www.welivesecurity.com/en/eset-research/ebury-alive-unseen-400k-linux-servers-compromised-cryptotheft-financial-gain/

https://web-assets.esetstatic.com/wls/en/papers/white-papers/ebury-is-alive-but-unseen.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

May 16, 2024 • 9:30 AM

More at www.hivepro.com