Ebury botnet malware infected 400,000 Linux servers since 2009

Date: 15th May 2024 | Severity: High

Summary

A malware botnet known as ‘Ebury’ has infected almost 400,000 Linux servers since 2009, with roughly 100,000 still compromised as of late 2023.ESET researchers have been following the financially motivated malware operation for over a decade now, warning about significant updates in the payload’s capabilities in 2014 and again in 2017.

Attack Vectors

- Ebury attacks show a preference by the operators to breach hosting providers and perform supply chain attacks to clients renting virtual servers on the compromised provider.
- The initial compromise is performed via credential stuffing attacks, using stolen credentials to log into the servers.
- Once a server is compromised, the malware exfiltrates a list of inbound/outbound SSH connections from wtmp and the known hosts file and steals SSH authentication keys, which are then used to try to log into other systems.
- In cases where servers host cryptocurrency wallets, Ebury uses the captured credentials to empty the wallets automatically.
- ESET says Ebury targeted at least 200 servers using this method throughout 2023, including Bitcoin and Ethereum nodes.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• Libkeyutils[.]so • qimpj6kkofzf[.]biz • op3f1libgh[.]biz • larfj7g1vaz3y[.]net • vqvsaergek[.]info • pbcgmmympm[.]info • jmxkowzoen[.]info • tyixfhsfax[.]info • qgjhmerjec[.]info • njdyqrbioh[.]info • btloxcyrok[.]info • afwyhvinmw[.]info • wyfxanxjeu[.]info • qemyxsdigi[.]info
Hashes	• 98FBD545B5C1B1FE185730BA9B1CD4BEBFAE4476 • 44B04CFC095F93D17B1BD4F8820C16843FCBAC3E • 013647E5AD347539EEF6C5933B16AD01B1806C3C • 787A93F86E7F5FCF922E996B577DF532270C7184 • E7DEBD6E453192AD8376DB5BAB03ED0D87566591 • CD9A5B823906CC620B28D69DBDB11BD9FE6B3E03 • DDAE9417470F832DB550EFB716B5BAEAAAA35372 • 71CA9B7C418264C2C856D47483666D123861D476 • 4A7303DD8E7BBBF063463B3852245ABDD343F5B6 • DFAECF7EBFC169CDF923AF421EDD537CCE536A64 • 3137DCA3F6FBD566F4ED2F49076A63D84869E13C • 96FD9B3064F04EE3063B2B103F856BB729B58749 • 53829463A7DE8C4BACE97B1F6925728F3421DF53 • 947EEE633E9347F72625FB652F94488A4B2B37F0 • E39667AA137E315BC26EAEF791CCAB52938FD809 • 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

INDICATOR TYPE	INDICATORS
Hashes	• 9569A8411477305FACA78E1C944D479EFA028DFB • BCC3B83CFADBD58256FC41AF9F0BFF50AC1F148B • D392022D8B72BCDDB849A94829C87731874E94AC • D3D6567862B4B7811BEA76BE117E901B2B6B8399 • D901D65F7A7A49296A501420F6D32BBF968F5BDE • ED5662F3CF80B8108D2172FBCA6119E403205EAA • EDD2DE0FAFE84EA51029FFDE38ACBB5918108DF5 • FD6709AF6A8DC384B101A8E9ED36C1092533C404 • 04FF6202534A394586D826B320645AEC24CE7AA5 • 32BB38D7D6B03DB4779E7A7183E7FA42DFBAFFC2 • 59F238DA1FD822AAD6FA7DF78D823854EAF8762E • 6369AD38D39562DD9D6D3E2612496A5357FFC09B • 67C1905EF4D0422DBDFAC41DC80F9C4D5C69E288 • 6BEE8F88F3F145170CEF58D9F790DDD99CDFA547 • 72048DEABE7F37BBECBFDA1570E1AB6B366B72BD • 907822012D6A970D676B634903F099587ED9C335 • 9209D757770AAFCA0B84B9F63B8769DF8CAC3F1A • D8647E825EFE74BF1726C0C494E3C2588FFF2262 • 5c796dc566647dd0db74d5934e768f4dfafec0e5 • 615c6b022b0fac1ff55c25b0b16eb734aed02734 • d4eeada3d10e76a5755c6913267135a925e195c6 • 27ed035556abeeb98bc305930403a977b3cc2909 • 2f382e31f9ef3d418d31653ee124c0831b6c2273 • 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

INDICATOR TYPE	INDICATORS
Hashes	• e14da493d70ea4dd43e772117a61f9dbcff2c41c • f1ada064941f77929c49c8d773cbad9c15eba322 • 9e2af0910676ec2d92a1cad1ab89029bc036f599 • 5d3ec6c11c6b5e241df1cc19aa16d50652d6fac0 • d552cbadee27423772a37c59cb830703b757f35e • 1a9aff1c382a3b139b33eeccae954c2d65b64b90 • 2e571993e30742ee04500fbe4a40ee1b14fa64d7 • e2a204636bda486c43d7929880eba6cb8e9de068 • 0004b44d110ad9bc48864da3aea9d80edfceed3f • 03592b8147e2c84233da47f6e957acd192b3796a • 0eb1108a9d2c9fe1af4f031c84e30dcb43610302 • 10c6ce8ee3e5a7cb5eccf3dffd8f580e4fb49089 • 149cf77d2c6db226e172390a9b80bc949149e1dc • 1972616a731c9e8a3dbda8ece1072bd16c44aa35 • 24e3ebc0c5a28ba433dfa69c169a8dd90e05c429 • 4f40bb464526964ba49ed3a3b2b2b74491ea89a4 • 5b87807b4a1796cfb1843df03b3dca7b17995d20 • 62c4b65e0c4f52c744b498b555c20f0e76363147 • 78c63e9111a6701a8308ad7db193c6abb17c65c4 • 858c612fe020fd5089a05a3ec24a6577cbeaf7eb • 9018377c0190392cc95631170efb7d688c4fd393 • a51b1835abee79959e1f8e9293a9dcd8d8e18977 • a53a30f8cdf116de1b41224763c243dae16417e4 • ac96adbe1b4e73c95c28d87fa46dcf55d4f8eea2 • dd7846b3ec2e88083cae353c02c559e79124a745 • ddb9a74cd91217cfcf8d4ecb77ae2ae11b707cd7 • ee679661829405d4a57dbea7f39efeb526681a7f • fc39009542c62a93d472c32891b3811a4900628a • fdf91a8c0ff72c9d02467881b7f3c44a8a3c707a • 5196a8a034611aaa112232767aafd74b8ef71279 • 20467521bfd58e9ed388ce83467d73e8fd0293a7 • f634f305a655b06f2647b82b58f7d3920546ac89 • 25a819d658d02548b2e5bdb52d2002df2f65b03a • 6180d8c1c6967d15a0abb0895103ccc817e43362 • 051a89a7a335062829a8e938b8d4e3e2b532f6ff • 035327b42f6e910b652bbdde5d9c270cfbaa9669 • 1dd7a18125353d426b5314c4ba04d60674ffa837
IPs	• 213.232.235[.]104 • 45.59.120[.]146 • 141.255.166[.]187 • 146.70.124[.]102

Recommendation

- Install Antivirus and Antimalware Software: Keep your systems protected with reputable antivirus and antimalware software. Ensure that they are regularly updated to detect and remove the latest threats.

- Firewalls: Implement firewalls to monitor and control incoming and outgoing network traffic. This helps in blocking malicious connections and preventing unauthorized access to your systems.

- Regular Software Updates: Keep all software, including operating systems, web browsers, and plugins, up to date with the latest security patches. Vulnerabilities in outdated software are often exploited by malware user.

- Education: Educate employees and users about the risks of clicking on suspicious links, downloading attachments from unknown sources, and visiting untrusted websites. Phishing emails are a common method used to distribute malware.
- Network Segmentation: Segment your network to limit the spread of malware in case of an infection. This involves dividing your network into smaller subnetworks, each with its own security measures and access controls.
- Strong Authentication: Enforce strong authentication methods such as two-factor authentication (2FA) to prevent unauthorized access to sensitive systems and data.
- Monitoring and Detection: Implement monitoring tools to detect unusual network activity and behaviors that could indicate a botnet infection. This includes monitoring for large volumes of outgoing traffic, unusual connection patterns, and known command-and-control server communications.
- Endpoint Protection: Deploy endpoint protection solutions to secure devices such as computers, laptops, and mobile devices. These solutions help detect and block malware at the endpoint before it can cause harm.
- Regular Backups: Regularly back up your data and systems to ensure that you can quickly recover in the event of a successful malware attack. Store backups securely and test restoration procedures periodically.

Reference Links

- https://www.bleepingcomputer.com/news/security/ebury-botnet-malware-infected-400-000-linux-serverssince-2009/
- https://github.com/eset/malware-ioc/tree/master/windigo
- https://www.welivesecurity.com/en/eset-research/ebury-alive-unseen-400k-linux-servers-compromisedcryptotheft-financial-gain/