PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

128-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°128	Fecha: 01-06-2024
		Página: 4 de 13

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ebury está vivo: 400.000 servidores Linux comprometidos para robar criptomonedas		
Tipo de Ataque	Backdoors	Abreviatura	Backdoors
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Sub familia	C04
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Una vulnerabilidad oculta en la puerta trasera SSH permaneció escondida durante dos años en kernel.org, poniendo en riesgo la integridad de sistemas y datos. Es una de las campañas de server-side malware más avanzadas, con cientos de miles de servidores comprometidos como una botnet para enviar spam, y se ha diversificado para incluir el robo de tarjetas de crédito y criptomonedas.

Ebury, activo desde al menos 2009, es un ladrón de credenciales y puerta trasera OpenSSH. Se utiliza para implementar malware adicional para monetizar la botnet (como módulos para la redirección del tráfico web), tráfico proxy para spam, realizar ataques de adversario en el medio (AitM) y host que soporta infraestructura maliciosa. En ataques AitM, ESET ha observado más de 200 objetivos en más de 75 redes en 34 países entre febrero de 2022 y mayo de 2023.

2. DETALLES:

La puerta trasera Ebury, una herramienta conocida como rootkit, fue instalada en servidores de kernel.org sin ser detectada durante al menos dos años. Esta puerta trasera es un programa que se utiliza para obtener acceso root a los sistemas y permite a los atacantes ejecutar comandos con permisos elevados.

Fue instalada mediante la explotación de vulnerabilidades no parcheadas en el software del servidor, permitiendo realizar ataques malintencionados, como el envío de spam, el robo de credenciales y la interceptación de tráfico web.

La detección de estas vulnerabilidades es crucial para evitar la instalación de puertas traseras como Ebury. Los administradores de sistemas deben realizar regularmente scans de seguridad y pruebas de vulnerabilidad para detectar y parchear cualquier vulnerabilidad no detectada.

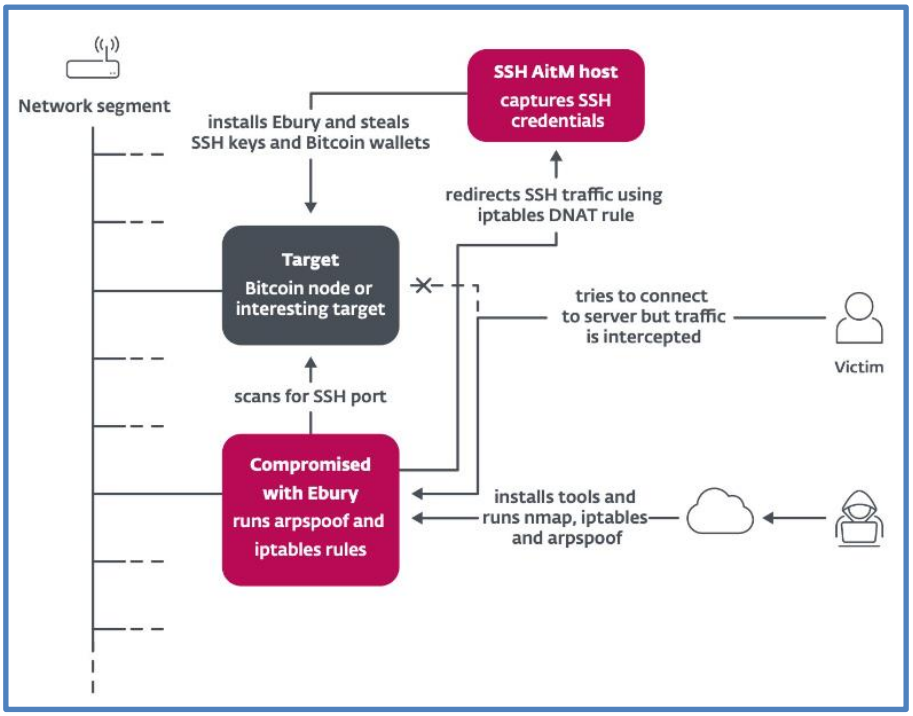
La detección temprana y la respuesta rápida son clave para mitigar el impacto de un ataque. Además, es fundamental que los usuarios y los desarrolladores trabajen juntos para crear soluciones seguras y confiables.

La Ebury también se utiliza para interceptar credenciales SSH y realizar ataques AitM (Adversario en el medio, MiTM bidireccional) para obtener información confidencial y redirigirlo a un servidor utilizado para capturar credenciales, como se resume en la Figura.

Los operadores de Ebury aprovechan los servidores comprometidos por Ebury existentes en el mismo segmento de red que su objetivo para realizar la suplantación de ARP. Según la telemetría de Internet, en 2023 se atacaron más de 200 servidores. Entre los objetivos se encuentran nodos de Bitcoin y Ethereum. Ebury roba automáticamente las carteras de criptomonedas alojadas en el servidor atacado una vez que la víctima teclea la contraseña para iniciar sesión en él.

La detección de la puerta trasera Ebury fue posible gracias a una colaboración entre los investigadores de ESET y otros expertos en seguridad informática.

Se descubrió que la puerta trasera había sido instalada en al menos 400.000 servidores que ejecutan Linux y en varios cientos de sistemas basados en FreeBSD, OpenBSD y Solaris.



"Hemos documentado casos en los que Ebury comprometió la infraestructura de los proveedores de hosting. En estos casos, hemos visto a Ebury implementarse en servidores alquilados por esos proveedores, sin avisar a los arrendatarios. Esto dio lugar a casos en los que los actores de Ebury pudieron comprometer miles de servidores a la vez", afirma Marc-Etienne M. Léveillé , el investigador de ESET que investigó Ebury durante más de una década. No existe ningún límite geográfico para Ebury; Hay servidores comprometidos con Ebury en casi todos los países del mundo. Cada vez que un proveedor de alojamiento se veía comprometido, se producía una gran cantidad de servidores comprometidos en los mismos centros de datos.

Al mismo tiempo, ninguna vertical parece más específica que otras. Las víctimas incluyen universidades, pequeñas y grandes empresas, proveedores de servicios de Internet, comerciantes de criptomonedas, nodos de salida Tor, proveedores de alojamiento compartido y proveedores de servidores dedicados, por nombrar algunos.

"Ebury plantea una seria amenaza y un desafío para la comunidad de seguridad de Linux. No existe una solución sencilla que haga que Ebury sea ineficaz, pero se pueden aplicar algunas medidas de mitigación para minimizar su propagación e impacto", concluye Léveillé.

Indicadores de Compromiso del malware Ebury

TIPO	INDICADOR
FileHash-MD5	0037f06b555a17a4b28a9570e7103ba2
FileHash-MD5	01e56e46518100bd61206703019fb7ff
FileHash-MD5	0760a8e598be0afdf15042e6c9dc5495
FileHash-MD5	09168b56c06554feec0da573e51dd726
FileHash-MD5	1551e1ef7983b68edd83e94ef1bdd57f
FileHash-MD5	1595fc797ca6c949725b863f159e4005
FileHash-MD5	15b9b930f3f18484b16173d576ec519e
FileHash-MD5	1785109e71a8f6eb6fb1ba7cce7c51e6
FileHash-MD5	1954547f20f9096a5b03df2f9a67d287
FileHash-MD5	1a4feb94c6944e56efc591566707fae4
FileHash-MD5	1f1c100ea006bc5667da22e9273825ca
FileHash-MD5	2118f2d0efbcdf0eed0af9c881229153

FileHash-MD5	22bfc05ab0fa217ba95577a3929c459e
FileHash-MD5	240a89bdf5495a047366ff0086eb4cd7
FileHash-MD5	27a0b1c7424a382a8e23f2ed8cf55754
FileHash-MD5	2d04c66588b798c1ec1dd61b48285a77
FileHash-MD5	3268342d6b5e41621115d8ee9ac2082a
FileHash-MD5	37a603a4cb5cad123851059228007735
FileHash-MD5	39da046a5704631618aaca63976be52d
FileHash-MD5	3c5bd51b484ba2d8cfd385bd2dcb19dd
FileHash-MD5	3dbb8c0b659f0003e38eda7086f1c07f
FileHash-MD5	414caaee14f943c6e6559df8b1cacef4
FileHash-MD5	44ef105d55622f52a9f7f6278ebae891
FileHash-MD5	4c2c2a490c3b945167524ea32c2fec44
FileHash-MD5	4d485629fdad9ee8de9003b58078fd0c
FileHash-MD5	4d822c8bded445a3abbd505bf5ebe20d
FileHash-MD5	4fa6b65d9ebd5aea9b3704216e39fdf6
FileHash-MD5	57dc029c964ff92ceffa1e494f14cccc
FileHash-MD5	59794dbf332046b5599fd21e88953877
FileHash-MD5	66a89e7f45fb44213b35e436106dfd71
FileHash-MD5	67ffc442b94bb3faabceacbbaa742327
FileHash-MD5	6852e9b0c1fa792e0bd6ba1b3c8e8b39
FileHash-MD5	6ac6a33dc08e508e58ae6060999d6211
FileHash-MD5	6b8b8cdce7c2c734b82ad3d03365ade0
FileHash-MD5	728fc6e23a1644d43c8aa564037ee89e
FileHash-MD5	7544034b10cfe7eff16061e337b3183b
FileHash-MD5	7a4c666db0a8f3667ccb679039e1331c
FileHash-MD5	874930210b25f4bc150f3f41e25a8530
FileHash-MD5	9403538430da045ecef82ff07595425a
FileHash-MD5	95e4c551fc9f4d2f693970c8314e37eb
FileHash-MD5	97ee396569742b37d1f2b4c1a53169e5
FileHash-MD5	98fd5feb0a14646d9700ad5b094a3a47
FileHash-MD5	9b3b341a21253397daf80b1d54906a2f
FileHash-MD5	9b422cf2918ffbd0461fff577da84f36
FileHash-MD5	9b4924dfeee4ddcb89e3773c5da5063d
FileHash-MD5	9ccb159e60edfe7c3519ac77feacc6d0
FileHash-MD5	a0170202d50841ea0dcc49fb06c59672
FileHash-MD5	a0488c9e9995860dd51f219170928a1e
FileHash-MD5	a44c4cfbc1270515a98f7dcc30373772
FileHash-MD5	a5c1c55cb491030a8956d22b76005fca
FileHash-MD5	ab3c3366abb8202dfcb15be34c17f68d
FileHash-MD5	abef69b85582f6dd04e6c274496cb35b
FileHash-MD5	b196a26780b6348f815bdbbb09cd811c
FileHash-MD5	b2637ca7941a048a490b96004b835297
FileHash-MD5	b831f74d80c60b6b25edcf6e5343f1c9
FileHash-MD5	bbec45f7d69f3dcd0ff2028a4e2e7520

FileHash-MD5	c155591d5ad3765d770e5dbcba8bb0eb
FileHash-MD5	c321614a1144004feb76abdceb049373
FileHash-MD5	c74e1d007a26e3488987456ecadcaea5
FileHash-MD5	cb5b1283a5509f745686fdf0d5fcbd95
FileHash-MD5	cf859b3b662dd55d35a56af8bf030d99
FileHash-MD5	d72751d864d283eb085083e70be59294
FileHash-MD5	da0bdbde8860c94b9fe7320a9e784ae5
FileHash-MD5	e019a2e17432f80a161faa4ec5b09200
FileHash-MD5	e765bb2954b386bd1a4e8e510d38b80d
FileHash-MD5	e77a33419876dcd678a425fe50652eed
FileHash-MD5	e8715c88846802fb05b7904833ee18d7
FileHash-MD5	e8f97a7b7846297850b5ed372f5d1c03
FileHash-MD5	ece07f84edbde75d6883324c91b1ccdd
FileHash-MD5	ecea5cc15532ffac4b8159bf860c63c1
FileHash-MD5	f0ea6708046cc2f2bce4efb7fbeb769e
FileHash-MD5	f5810fc515225dd4b607298b5f448f30
FileHash-MD5	fb4dd618ddcf8792ef4f0f9b77446304
FileHash-SHA1	0004b44d110ad9bc48864da3aea9d80edfceed3f
FileHash-SHA1	035327b42f6e910b652bbdde5d9c270cfbaa9669
FileHash-SHA1	03592b8147e2c84233da47f6e957acd192b3796a
FileHash-SHA1	051a89a7a335062829a8e938b8d4e3e2b532f6ff
FileHash-SHA1	09c8af3be4327c83d4a7124a678bbc81e12a1de4
FileHash-SHA1	0daa51519797cefedd52864be0da7fa1a93ca30b
FileHash-SHA1	0eb1108a9d2c9fe1af4f031c84e30dcb43610302
FileHash-SHA1	10c6ce8ee3e5a7cb5eccf3dffd8f580e4fb49089
FileHash-SHA1	149cf77d2c6db226e172390a9b80bc949149e1dc
FileHash-SHA1	1972616a731c9e8a3dbda8ece1072bd16c44aa35
FileHash-SHA1	1a9aff1c382a3b139b33eeccae954c2d65b64b90
FileHash-SHA1	1dd7a18125353d426b5314c4ba04d60674ffa837
FileHash-SHA1	20467521bfd58e9ed388ce83467d73e8fd0293a7
FileHash-SHA1	24e3ebc0c5a28ba433dfa69c169a8dd90e05c429
FileHash-SHA1	25a819d658d02548b2e5bdb52d2002df2f65b03a
FileHash-SHA1	267d010201c9ff53f8dc3fb0a48145dc49f9de1e
FileHash-SHA1	27ed035556abeeb98bc305930403a977b3cc2909
FileHash-SHA1	2e571993e30742ee04500fbe4a40ee1b14fa64d7
FileHash-SHA1	2f382e31f9ef3d418d31653ee124c0831b6c2273
FileHash-SHA1	2fc132440bafdbc72f4d4e8dcb2563cc0a6e096b
FileHash-SHA1	39ec9e03edb25f1c316822605fe4df7a7b1ad94a
FileHash-SHA1	3c5ec2ab2c34ab57cba69bb2dee70c980f26b1bf
FileHash-SHA1	42123cbf9d51fb3dea312290920b57bd5646cefb
FileHash-SHA1	44b340e90edba5b9f8cf7c2c01cb4d45dd25189e
FileHash-SHA1	471ee431030332dd636b8af24a428556ee72df37
FileHash-SHA1	4d12f98fd49e58e0635c6adce292cc56a31da2a2
FileHash-SHA1	4f40bb464526964ba49ed3a3b2b2b74491ea89a4
FileHash-SHA1	5196a8a034611aaa112232767aafd74b8ef71279

FileHash-SHA1	575bb6e681b5f1e1b774fee0fa5c4fe538308814
FileHash-SHA1	58f185c3fe9ce0fb7cac9e433fb881effad31421
FileHash-SHA1	5b87807b4a1796cfb1843df03b3dca7b17995d20
FileHash-SHA1	5d3ec6c11c6b5e241df1cc19aa16d50652d6fac0
FileHash-SHA1	6180d8c1c6967d15a0abb0895103ccc817e43362
FileHash-SHA1	62c4b65e0c4f52c744b498b555c20f0e76363147
FileHash-SHA1	7248e6eada8c70e7a468c0b6df2b50cf8c562bc9
FileHash-SHA1	7314eadbdf18da424c4d8510afcc9fe5fcb56b39
FileHash-SHA1	74aa801c89d07fa5a9692f8b41cb8dd07e77e407
FileHash-SHA1	74cd5ae9f6bbdf27b4eaf45c4a22c6aae07345a2
FileHash-SHA1	78c63e9111a6701a8308ad7db193c6abb17c65c4
FileHash-SHA1	7adb38bf14e6bf0d5b24fa3f3c9abed78c061ad1
FileHash-SHA1	858c612fe020fd5089a05a3ec24a6577cbeaf7eb
FileHash-SHA1	899b860ef9d23095edb6b941866ea841d64d1b26
FileHash-SHA1	8daad0a043237c5e3c760133754528b97efad459
FileHash-SHA1	8f75993437c7983ac35759fe9c5245295d411d35
FileHash-SHA1	9018377c0190392cc95631170efb7d688c4fd393
FileHash-SHA1	98cdbf1e0d202f5948552cebaa9f0315b7a3731d
FileHash-SHA1	9bb6a2157c6a3df16c8d2ad107f957153cba4236
FileHash-SHA1	9e2af0910676ec2d92a1cad1ab89029bc036f599
FileHash-SHA1	a51b1835abee79959e1f8e9293a9dcd8d8e18977
FileHash-SHA1	a53a30f8cdf116de1b41224763c243dae16417e4
FileHash-SHA1	a7b8d06e2c0124e6a0f9021c911b36166a8b62c5
FileHash-SHA1	ac96adbe1b4e73c95c28d87fa46dcf55d4f8eea2
FileHash-SHA1	adfcd3e591330b8d84ab2ab1f7814d36e7b7e89f
FileHash-SHA1	b8508fc2090ddee19a19659ea794f60f0c2c23ff
FileHash-SHA1	bbce62fb1fc8bbed9b40cfb998822c266b95d148
FileHash-SHA1	bd867907a5059ab1850918d24b4b9bbe33c16b76
FileHash-SHA1	bf1466936e3bd882b47210c12bf06cb63f7624c0
FileHash-SHA1	c4c28d0372aee7001c44a1659097c948df91985d
FileHash-SHA1	cd9a5b823906cc620b28d69dbdb11bd9fe6b3e03
FileHash-SHA1	d4eeada3d10e76a5755c6913267135a925e195c6
FileHash-SHA1	d552cbadee27423772a37c59cb830703b757f35e
FileHash-SHA1	dd7846b3ec2e88083cae353c02c559e79124a745
FileHash-SHA1	ddb9a74cd91217cfcf8d4ecb77ae2ae11b707cd7
FileHash-SHA1	e14da493d70ea4dd43e772117a61f9dbcff2c41c
FileHash-SHA1	e2a204636bda486c43d7929880eba6cb8e9de068
FileHash-SHA1	eb352686d1050b4ab289fe8f5b78f39e9c85fb55
FileHash-SHA1	ebc45dd1723178f50b6d6f1abfb0b5a728c01968
FileHash-SHA1	ee679661829405d4a57dbea7f39efeb526681a7f
FileHash-SHA1	f1ada064941f77929c49c8d773cbad9c15eba322
FileHash-SHA1	f634f305a655b06f2647b82b58f7d3920546ac89
FileHash-SHA1	fa6707c7ef12ce9b0f7152ca300ebb2bc026ce0b
FileHash-SHA1	fc39009542c62a93d472c32891b3811a4900628a
FileHash-SHA1	fdf91a8c0ff72c9d02467881b7f3c44a8a3c707a

FileHash-SHA1	e39667aa137e315bc26eaef791ccab52938fd809
FileHash-SHA1	9c8af3be4327c83d4a7124a678bbc81e12a1de4
FileHash-SHA256	003245047359e17706e4504f8988905a219fcb48865afea934e6aafa7f97cef6
FileHash-SHA256	01f8a935832048a6c116b376db82a83890e6375586e830e87ca3c244b71392b5
FileHash-SHA256	024f0e8e28b340a657d7e955edb37b9e819507aec00148d49f524e53301e8930
FileHash-SHA256	02b0e3b6c60b53aa4daf5534459b595f9aa8e73ab257ed8a580090b0cf6fb213
FileHash-SHA256	0395e1c8f0bab7970782f9ce37fd2b5763b514bc52577e19d4d0d18c7b857546
FileHash-SHA256	06243598428c70ae07ec6651549378ee18d8b4ad4474b48a4ecf80775075a0ec
FileHash-SHA256	07a1a43bbcc747520a5afb91bd050c51541922cf4f4cf715dc6916e66dd204a9
FileHash-SHA256	0e45d547d54241595a1b2504d1c1f6991296a2b0196f0e653773615a8e3f39d1
FileHash-SHA256	0fba87d17bfc539680ed32df31b5b6b42ce5709eed7e4fc3d08d980f92267e42
FileHash-SHA256	107d3db3f4f760c212a2a2baa407e2414b4d83822134353b68f4079e5c4f4deb
FileHash-SHA256	10f7b527ccd1f846a5da8df25d6edecc7370cd98f9c25b5626fa88d152f42a95
FileHash-SHA256	11ac32b7d5d1db9ab0b403a3e9637a7ada87c329c030fa0b491d335485dd5f42
FileHash-SHA256	1272daef8e1a8143c967676b120cc69be39031efe03593e1006f185e48f428e1
FileHash-SHA256	1471ec61976665e1e088a757d74c718aff82a737c66669f4a7460609fcdb43e4
FileHash-SHA256	15298ef46a68803a3eeeac84e22df6836b991650f78ec2d1de379b0e6a86ef86
FileHash-SHA256	1bc7eb07aaad906ca9822b827b9f0a0c6ea323ce4914f8aa5cf1df69f2462bd6
FileHash-SHA256	1d6a0e9565b80e265fd5b193f2b1ba703afd0e5e284b2ea3e52925d73d2a60fb
FileHash-SHA256	1da2b0f230fdb695e161767a4fd7ed80fee1153a70a78032e4219c4898c3532d
FileHash-SHA256	1ea1c30e5dfa4a42dd3d393e508a75bcee1658a1a13ddc1b593f609b8648f9fc
FileHash-SHA256	1fa6d970dcc2bcccedbd545c85b3184dc3663ebdade04ed18410d0329ecbef81
FileHash-SHA256	2343255b3e2c6380454bf56fecb3e1368261b15b08f59f9b7eb37bc8acaae01a
FileHash-SHA256	2596956e0eb0f1e59d3275e557caf9974942db3d6927e2215243034f5c792916
FileHash-SHA256	290b03d8d8082d3dd06c4b18287a3fb726b2eee7b9373b15fab93d9e4a4b5df9
FileHash-SHA256	291be73e079ea1c39825da77b0628443c3800658846aaf76c2eb29b3a7deeeed
FileHash-SHA256	2ddb50f2d60c4b8bc50aa03206c6397b56fdda210bd2a935de5fb419a52fa56d
FileHash-SHA256	3127d2211bfea0d1a132d53e709c0d11dddfa32f497c4ab7f348350144b07d65
FileHash-SHA256	33ded5914025e70f6f5f109ea85179fb6373bb757da95e89958bf7a957b446bc
FileHash-SHA256	347c4fb37590644e2658cc97b38d5b0e09bb1f2f84928bfb3a64b0ca34fdb0b2
FileHash-SHA256	348148cc3efef8d544708ada0c2cb34b8d508f0715c2fb6e33b325a1247e7163
FileHash-SHA256	38faa26350e17dd0cc9fc714b1ef800cf599397dcfb71b94812feae38ba78996
FileHash-SHA256	3913e9bf43ec6a73584b9d621f396ee035d8bd1d28a99421e405c226cd321b98
FileHash-SHA256	397062b0ba3040e5a1d64b851d6b51f39df4d8ca1046f33f2186abfbae720ca4
FileHash-SHA256	398811f4fe60d8088cf19a50208927761bd8d8dc73ce9ee77b407aaee91a3516
FileHash-SHA256	3bc5b33247ed6a4b22890ad47b9bcf7209a1d0f767cc441cf4d2206557ddadba
FileHash-SHA256	3d6692b7a25809789b6bd899e2c28f52c40b87dbad751558cbb22fedb3b67a7b
FileHash-SHA256	3ea7ccf3932f76b2f0af7cd33f3c0efed4dd339dba238a91ada2a0c7a1ffac0e
FileHash-SHA256	4109cebe6ee503691bf53704a249893395f618221a160e32488eb48ca6954fcc
FileHash-SHA256	435be2e2b5b15862dc37f3e3e85e549448804141897a4e732be0bd8792a5e97e
FileHash-SHA256	463907381e95aa22f9f3c2b395d1030328ed055c1a53766e85e134ea24c33920
FileHash-SHA256	4665484cfebbdce0c899b12c42e11183c29637fad23f60e5465df9a9fad63dcc
FileHash-SHA256	490a4a7fc04bb2a67e8f3c1ac71386ef2783aa886dfac01448a56a3108c5deae
FileHash-SHA256	49b47a373448c946e2005c0516ddbe204279c1e68d34cfa8df8f28eb24ca6a82
FileHash-SHA256	4b9ae4cac87f54e86ee0e42181fda4551eafc265793889cba78876e5660c391e

FileHash-SHA256	4c7409753c40e78586d8421ac61e874c0d877758118de239f6ae566e020a9444
FileHash-SHA256	4d986f3407cf76de0318e7c84ed142e7bc1f8ac6bc99793ffef76ba904eaad5b
FileHash-SHA256	4f8b94046ed3c803eafbeddaf8d6e488076af5b38e499e6d59755f737a2a62e0
FileHash-SHA256	5082f3417f8aaf781b4ef7a6cd53133593881ed9e488da9c12937bfe8cf17a58
FileHash-SHA256	50ebb172d4c4e13879599981adfd4ff93e22091b29eb8c8ecde04e930932a38a
FileHash-SHA256	59b01225155517c5ece002407f669bffeca741862c5a2881631e3a14b65d1290
FileHash-SHA256	5a7627820254abea2ae180e6ef5db029f2a612b510736723f0d94c2e49f09065
FileHash-SHA256	5a9ea0c4103b96434c4d99aebafbbb61475ad0844e6bd8c649e96a145e6462d2
FileHash-SHA256	5c6c2c266e142be253cba020420744b02f821b0993fc9f4bff9ff5e356780282
FileHash-SHA256	5f27e51636de85a3dcc821f0dc0b46a5cbd63bde3b5ea0c10c393d25e5305463
FileHash-SHA256	5ff94822492a058246fa34129d0f3ec6e0f0461ef2526d2914e126eddbc7e16d
FileHash-SHA256	5ff9ed0b3f0b84de100b3ee47274437a2944c23a832b2bba2153992047223ecb
FileHash-SHA256	6061844bf4d4b4367bb04dd8ecffae648d45161e17d7177dd03cf20429c782f3
FileHash-SHA256	6275c888fca6fc10baa70954e22ec42cb09e7e4fbcc1110dee49ebc2941ea3d4
FileHash-SHA256	64c548dd113403f146971a03b09033e0fe73ce653f2110ebafd773d969c44f04
FileHash-SHA256	669119b2a9d5b6e1b764acf7582574345ff5470d8717da53a8330f358ffb8904
FileHash-SHA256	671c9fc9a4e82499b71cee43abfbbf86d1dc01a0dbc500f265f7867715f819f9
FileHash-SHA256	6b8e01987c5631e97d9bc488142a4db5c3abed013fda125471e5ccb1f6e2f6b3
FileHash-SHA256	6e5a89b4f161529e233f342abc048c2e6584eb7a93f4feac258a34e992b66ee1
FileHash-SHA256	6eb60410a7129de4207c37a1ae96121c8a873df1cc96214f5c1de623fa8133d7
FileHash-SHA256	6ff082ff2a6fe8e1d22b186bf0250ee4d78cba006d4752190d7e637ffde14bb4
FileHash-SHA256	7542573b7dcb1ff964a8112dbf242830e882f7d4de6d241e17469043f3a0da7e
FileHash-SHA256	771d40f210cd69a416b8171d73776efac4d6bdde952940e69c4cf36de56e8999
FileHash-SHA256	78bc52158716a514987415afd75fdea43fef73b7f215174218881881ba82500b
FileHash-SHA256	7a472fb0415345e9396e708621218783cb0459e7b883ab9ded648c4712aa2475
FileHash-SHA256	7b3cd8c1bd0249df458084f28d91648ad14e1baf455fdd53b174481d540070c6
FileHash-SHA256	7ca7a529194978a67dd3b99f2a1c9f7b5f17215af49ec452521e442c2ffd815a
FileHash-SHA256	7cdfdab7ddef2c8bf3bca9242bad47173eaec883cffa04c7e4fade9e7868bf78
FileHash-SHA256	7e1c91e249b5a01a726dcf97f76f2f434d60385a4a060cb0272e715c82b8d914
FileHash-SHA256	7e9398404707c57d2a3f71ee8548045eb5b42f8c5439ebf5d5e8227738554021
FileHash-SHA256	7eaf3408cc13b8c36fafbdc0343053e82fb647b0b64e63a99bb0e90ba47c13a6
FileHash-SHA256	7f6328ae015850ab7d4340411e1d3ba4985ee00a0e3e4334719d9a88ef0441d9
FileHash-SHA256	803828547baf601f31f1e203db9e5c312d1c9e223539f439a3c9079e1a91ecdf
FileHash-SHA256	817a971b0a74dfa8465c505da84c99bd30f9e34c5f8d0ad8651b932c45e95283
FileHash-SHA256	82b70aed01d65d7b83aa21f89f65ebcc3b6622efe7d977540cdf8c4e90d31de7
FileHash-SHA256	83d269ae06d961850aa6be078f6d80a180d086b0c5a306a5692e726d55e82761
FileHash-SHA256	84876a1bcfeee7940cf9f250914360153c1317bc4c9ecb6ccf18f65d8f66e9f9
FileHash-SHA256	868d3366e421238864483a08f48b4c0a933418f6bf64b7b3e291d7dae9906d6e
FileHash-SHA256	8cc01a0c2a3d20e2e1c29e4960e362d0258694538a23cd703f503f6969aeb356
FileHash-SHA256	91998d2f23556e3703e89b7987a87d3286ffe9b3416923e3dc3f9b86a595ce92
FileHash-SHA256	927269995c67da90e44e4b74f035e6c8931f8bc25db43c1e1503cf8cda201c06
FileHash-SHA256	998f74471bb96102781eb62713f57483dc6a6d1f27c429a957eb23bb124d7709
FileHash-SHA256	9bc6400910443c471578695f90cbe97b94866219108664df8a8d918578280a66
FileHash-SHA256	9db0797cea658b62496dea9817c4fe4e752df7f5e5a08839d37d46ca69ae125a
FileHash-SHA256	9dba448f82bd693484fdb303694e185e9eb5b9146c0b39974aa8a8ceea0a6589

FileHash-SHA256	9e091c5f5a66c31a822ce5714c740c69e37b3128ac2e445391a9d9dcc1194fcd
FileHash-SHA256	a2830a75fc7115aa2ac46e26391cdf7e5ab6dea73acf70b6af347a4e3766a953
FileHash-SHA256	afbef5352942dde22e5cfa802c057917fccb17623f3e8ead165fd17371d851f3
FileHash-SHA256	b20a25779dc2af69ebdbbe2884d9fe316477157d6dab1102d2371a65c256d8d1
FileHash-SHA256	b56ef85a632e2accdfb515fc2e9bea45f50f76635d999ec55ca85dc1883743dc
FileHash-SHA256	b5a19a8a8250c9cd1d129f41e11b07f81508bc4d59d420c8834170e22b0bb1a0
FileHash-SHA256	bb06015d766bd6365f87b645dec7e7a469b216505921de1e3e78f0c1a6f5fc7c
FileHash-SHA256	bc6067d11ae5802fc7a174d0c4abf40bf68974dceeba8d11fa6185709f412011
FileHash-SHA256	be4f0d9baec7a194fc7f2decb3c0a238919ba7ca87676344879b6f130f0a6654
FileHash-SHA256	bed696e1a0a8a23e82a17176770f2271286b87878a2415b096efe09258b1b4e9
FileHash-SHA256	bf4e30636cfc5b6a78067827f8d4b6a2639e4328b142deca1305a619ca001328
FileHash-SHA256	bfefe897282c69afafc163aacb5c938e27dbbf62ad8dcb17e583b09cc1bd1493
FileHash-SHA256	c00d0403fa426be3dc6219a5cb6390948fde6167314db4cb6fd3230c7cb698e2
FileHash-SHA256	c26ee35b75973d6d463cd39afd6764f23622f52cdd54f495cf232a741284bed1
FileHash-SHA256	c69f9eeb6f9d936ec33405a632f8f081ccd1eaa43fb88bc8daf5e27a73937eca
FileHash-SHA256	c72973ac18d02c56b623bb402dc18d07ca8fa57f2f6b95b4f8341bd7b88334a0
FileHash-SHA256	c9a85949f61102bc27df7739c05c03620ba4f711d90ac9d4e9edff117332fe2e
FileHash-SHA256	c9ce4fd2476cc781064f1da7f6e784b38c70b7fea4f48332afae921d9e4c3dfa
FileHash-SHA256	c9cfa1f9d8b36ca653fa31d4796b23c12fb2e0a36acf4228982d8a92ba805f7b
FileHash-SHA256	cb2f1a7ef1733faed91961ab63174e22e6fabfe658d631b5d5e3f7573418bfd5
FileHash-SHA256	cef981a137bac96e1c2bf053da4e10c254c8d7892227e21dd5fcfb9b7ea32923
FileHash-SHA256	cfb64b329b95cfb7dbfac7fa61025b0cddfce3c77db1d224e839fa59defe8336
FileHash-SHA256	d2bc83cf8d2e785a58ab3d88ced60f1635fd25918a67820d9da0a9c6d4eea6e9
FileHash-SHA256	d3f0668fee0a2bd7fc819ea1d913c6b0d51702a5afab659a7b6a6c118749cbd6
FileHash-SHA256	d4859d47ee892be52dc936653a5e33674fa2836291e1cb145b47114438749f72
FileHash-SHA256	d99a13872fd36e9f9712bc10e583836db3649198d25f71097bd5e0c96c786fef
FileHash-SHA256	dae9068440615750cbff522faa093a320a61185320aaa3a68499f31302a52fda
FileHash-SHA256	db0ff03216625bce95640c4b9931e4720684791f68cfa4adbb260b4135425521
FileHash-SHA256	db3e9c6e4b9d3b699e2940196b07a5a1cde19f6b60b83163882b736c61ca43e1
FileHash-SHA256	dd642bb34500e23a829fd33782ff4b9dd97285c350964707d74b50ce72d8a22c
FileHash-SHA256	ddd172c1483a5c4afc4b7ddfc8ecb6f23b789ad3751a392fbc07933619d5e42e
FileHash-SHA256	de6f016a167555a1c35f5e9d54c6874f2db1d142a833139bc57032f9dc56c3fe
FileHash-SHA256	e06115a553def25a846468290795f1a36b67dbbe7012d612d5cb7675c9170cd0
FileHash-SHA256	e06c312ca77aa439175da4792ee5ea055ee78a6efb087f1126a8ade683cab249
FileHash-SHA256	e2c40cb7fe69fa985a3d77fb083f3f2ab2c5d8848df3c432a94c6ef50f96dae6
FileHash-SHA256	e33a1aeed5e3d670cfe002cd98ab1dd106e83a08be4def552ccec461ed2e9611
FileHash-SHA256	e3a3776a15abdee85ed2d949ae32e5312ab3a6660f10b9269f03baaeecf8ac9a
FileHash-SHA256	e4618296202c53b9d8714e3028ea6c290ab83f637557e1f97dea82a6fefea8fe
FileHash-SHA256	e67d20a83bcb45439c94f03b68af263055fc7ac6b60fd3882525c27e36254fa7
FileHash-SHA256	e69323fb1f891726ae7589b97ebd46d1aafec87793be2b68f9b033c360e0a4d2
FileHash-SHA256	e8e40b73fd8b903282bd9e1de138b417f50efbf594134273e6d54b865837e4f9
FileHash-SHA256	ecd5a6de365683bfaeaaf555ae5dba39bf1c3591816e1549bdf521e0ae87fe5f
FileHash-SHA256	ecdcf256c822a9d9f3ce011fd98f22b3ca3e345b34b2c17fa34471ab7f65edb3
FileHash-SHA256	f2176ac3ffe8ae723f095c23c97410f20a2b500a22415e70b975faa727d0add3
FileHash-SHA256	f270258ba7902927ac917c1782b8bbfe0619d11b968758a984c9dc7f8693cea8

FileHash-SHA256	f36808dbd52c9074e87fd365a91168daadbb63681a08a9eeba5977f0731a1c04
FileHash-SHA256	f6404d673cec28aaf21336f95baf2f9ebc1c2f8f55ffbd4eb2c4c9c1c0053de6
FileHash-SHA256	f9aa316f3b0c7bfc7fef2fe6e442519a4661de5d5ed1165423b1dfe9795e4166
FileHash-SHA256	fbcdccbdc7506720cfb1f37843f88a39d8cb6e551e7224e813a6bbc81e9b7813
FileHash-SHA256	fcd24de593f6fa2dd14612050dd79192d2e6d6e5170d171712b1f658c4daa4d9
FileHash-SHA256	fe4a4de274d61f3b2fe2a9103ed4cc66dfd92382057ad1a0920e8271e28c2a5b
FileHash-SHA256	ff72489289b1aef791630546223b2f917f98ceb7c2e391737bb8ff9a15cd1593
YARA	onimiki

3. RECOMENDACIONES:

- Realizar escaneos de malware en sistemas y dispositivos para detectar
- posibles intrusiones o software malicioso que pueda estar instalado debido a la exposición de las
- credenciales.
- Realizar actividades de implementación de parches y
- actualizaciones de seguridad hasta la vigilancia proactiva de actividad sospechosa en la red.
- Configurar en los equipos de seguridad (Firewall) la restricción de los Indicadores de Compromiso listados, a fin de mitigar las afectaciones del malware.

Fuente de Información:	• hxxps://informaticasegura.es/noticias/puerta-trasera-ssh • hxxps://www.linkedin.com/pulse/la-botnet-ebury-compromete-m%C3%A1s-de-400000-servidores-linux-ehcgroup-txatc/ • hxxps://www.welivesecurity.com/es/investigaciones/ebury-400000-servidores-linux-comprometidos-robar-criptomonedas/

Índice alfabético