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

177-2024-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°177	Fecha: 01-08-2024
		Página: 4 de 17

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La amenaza cibernética el ransomware Akira		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Desde marzo del 2023, el ransomware Akira ha afectado a una amplia gama de empresas y entidades de infraestructura crítica en América del Norte, Europa y Australia. Al 1 de enero del 2024, el grupo de Ransomware ha afectado a más de 250 organizaciones y ha obtenido aproximadamente 42 millones de dólares (USD) en ganancias por ransomware. Actualmente se ha monitoreado una serie de ataques en México, Argentina y algunos países de Centro América.

2. DETALLES:

El FBI y los investigadores de ciberseguridad han observado que los actores de amenazas de Akira obtienen acceso inicial a las organizaciones a través de un servicio de red privada virtual (VPN) sin autenticación multifactor (MFA) configurada, principalmente utilizando vulnerabilidades conocidas de Cisco CVE-2020-3259 y CVE-2023-20269. Los métodos adicionales de acceso inicial incluyen el uso de servicios externos como el Protocolo de escritorio remoto (RDP), phishing selectivo y el abuso de credenciales válidas.

Una vez obtenido el acceso inicial, los actores de amenazas de Akira intentan abusar de las funciones de los controladores de dominio mediante la creación de nuevas cuentas de dominio para establecer la persistencia. En algunos casos, el FBI identificó a los actores de amenazas de Akira creando una cuenta administrativa denominada itadm.

Los actores de amenazas de Akira aprovechan herramientas como FileZilla, WinRAR, WinSCP y RClone para exfiltrar datos. Para establecer canales de comando y control, los actores de amenazas aprovechan herramientas fácilmente disponibles como AnyDesk, MobaXterm, RustDesk, Ngrok y Cloudflare Tunnel, lo que permite la exfiltración a través de varios protocolos como el Protocolo de transferencia de archivos (FTP), el Protocolo de transferencia segura de archivos (SFTP) y servicios de almacenamiento en la nube como Mega para conectarse a servidores de exfiltración.

Los actores de amenazas de Akira utilizan un modelo de doble extorsión y cifran los sistemas después de exfiltrar los datos.

Los actores de amenazas de Akira utilizan un sofisticado esquema de cifrado híbrido para bloquear los datos. Esto implica la combinación de un cifrado de flujo ChaCha20 con un criptosistema de clave pública RSA para lograr un intercambio de claves rápido y seguro.

Los archivos cifrados se adjuntan con una extensión .akira o .powerranges. Para inhibir aún más la recuperación del sistema, el cifrador de Akira (w.exe) utiliza comandos de PowerShell para eliminar las instantáneas de volumen (VSS) en los sistemas Windows. Además, aparece una nota de rescate con el nombre fn.txt tanto en el directorio raíz como en el directorio de inicio de cada usuario (C:\Users).

Indicadores de Compromiso:

Dominio:

- winscp.com
- royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid.onion
- akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion
- aci-bd.com
- adcom911.org

- advantageresourcing.com
- akronlibrary.org
- brokerstrust.ca
- carusocarsharing.com
- cicesp.com
- compassinf.com
- cvalley.net
- ellispatents.co.uk
- familydaycare.com
- fersten.com
- garciahamiltonassociates.com
- gcesg.com
- greenfiber.com
- gregorypoole.com
- harbro.co.uk
- harmony.co.za
- hssstaffing.com
- imatica.com
- itwfoodequipment.com
- knpgroup.com
- lewisyoung.com
- maltproducts.com
- mcps.k12.va.us
- newworldtravel.com
- perpetualgroup.com
- refractron.com
- sklifescienceinc.com
- stoughtontrailers.com
- thelabconsulting.com
- theperrylawfirm.com
- tmptoronto.com
- wilcom.com
- a123systems.com
- accuridecorp.com
- americansteelandaluminum.com
- ascendpkg.com
- becht.com
- beltrailway.com
- caminonuevo.org
- cequint.com
- chowc.org
- civicsd.com
- clifton.k12.nj.us
- cutler-smith.com
- divvies.com
- donsmobileglass.com
- draje.ir
- energyone.com
- gruskingroup.com

- guidoco.com
- habasit.com
- handiquilter.com
- healix.net
- hsml.com
- kouryengineering.com
- kreacta.com
- murphyplywood.com
- nycon.com
- otech.com
- papelpresena.com
- parathon.com
- pennypublications.com
- pinnergy.com
- polish.org
- protectorfire.com.au
- raddning.com
- rcpsg.ac.uk
- rentonschools.us
- revpl.lt
- rimss.com
- ritefl.com
- riverscasino.com
- southlandintegrated.org
- ssmtax.com
- tallyenergy.com
- tedkomp.se
- tenniscanada.com
- tgrwa.com
- timeco.com
- ultimus.com
- ventureinsga.com
- verticaldev.com
- vossenterprises.com
- vossenterprisesinc.com
- wetreatyourfeet.com

FileHash-MD5:

- 77a243cb73f6bdd610eeb10786b752fb
- 0a6757bea01c2c48b50b7ec2bc39e31c
- 6615ea2fa3b879d27687a7ce917e93b0
- aee6801792d67607f228be8cec8291f9
- b87639f9a6cf5ba8c9e1f297c5745a67
- 00141f86063092192baf046fd998a2d1
- 0885b3153e61caa56117770247be0444
- 150f078e3663d49d76c69f8693a4565c
- 1e19df21dba272cbf002e11c35cb024c
- 2cda932f5a9dafb0a328d0f9788bd89c
- 431d61e95586c03461552d134ca54d16
- 503f112e243519a1b9e0344499561908

- 51ba8d3aadbbde812934ddd0006b1b80
- 5483da573c6a239f9a5d6e6552b307b0
- 66004c532d292572494de9934fe3910b
- 69434397fe9df4c7533a51db27e35c82
- 7189bd036bbddd4e7d849e442ddb9caa
- 748b043f1602547196fbbada0536a7c3
- 77958f66ade19ace783617531f0d82ac
- 883096cb92446c152da91f805baf256f
- 98cafe7df2d7e332d2602bb5b4c49019
- 9df999f142f137b0794b8afcaaedc588
- a74812faa9245f21516393218545387c
- af95fbcf9da33352655f3c2bab3397e2
- b1e75b6457adecccf00d3f0dd59e4c9e
- b717432e1fb2ce1affcfe4b489c92e6d
- b9e0b3844e46490682902fd7aa55b8d7
- bff3fdbff0a5d4aa1c03f7982c968e54
- c60ac6a6e6e582ab0ecb1fdbd607705b
- c7ae7f5becb7cf94aa107ddc1caf4b03
- d25890a2e967a17ff3dad8a70bfdd832
- d724d178eb09cd8ce2af8b088117b332
- d81135333a0eed3e973107891e996505
- e44eb48c7f72ffac5af3c7a37bf80587
- e72e0069e1fb4328e2704bda97fb4a40
- ed6cb54d34f1cc8c9095c201f3173a06
- f526a8ea744a8c5051deefbf2c6010af
- 0f7b6bb3a239cf7a668a8625e6332639
- 37e172be64b12f3207300d11b74656b8
- 74874922171b67bb181c0ce087744fa7
- 74d5d4e9a556a6170f19893e7ffdeffa
- 7a647af3c112ad805296a22b2a276e7c
- a18d79e94229fdf02ef091cf974ed546
- e2eadf60d8f25cae9b29decab461177b
- e9fda12cfcceffd2e6a19c39dcb01b1e
- 1ce7d5a1566c8c449d0f6772a8c27900
- a655323232f2defb99c4e975ab1edcec
- 2902e12f00a185471b619233ee8631f3
- a9429fa4db9a5fe059896653a5d4d35c
- b75fe8539b7dc28190a501e879a05a9d
- c46070b5e113a7f5d9a58de14a11e430
- 302f76897e4e5c8c98a52a38c4c98443

FileHash-SHA1:

- 8d4f19b221751297b0c3a10f105772d7286c9411
- bf6ba727ff14ca2fddf619f292d56db9d9088066
- ce4758849b53af582d2d8a1bc0db20683e139fcc
- e6b34a589e61b155ab70f11f8f7393316c9a3189
- 003605a4edc028caf03d28edf41104407acee437
- 0ceb5e99b2e1b2dd04cc07d1301c9649ce4cb458
- 262e3fe7631204be404bdbdc2633282072461a61
- 2cde82cf7a1bc88c8fc5865cb57f31f6437f74fc

- 3de04890311bca0785f77e57a49840261b7d83e2
- 3f87d550f0b7c4f2ec8e60e8eed4214d49ddee61
- 5b34aceddba8942c78b202ed30a7bf0250b57841
- 651c70f9d995c52fa48493b2e60904d15cad8821
- 6bd48f5f1d861ad57b9dffd8e4aa7fe3b3c6a110
- 7901d79f118cc659b7b6c09ce77d578de43bcc02
- 8d635ca131d8aa20971744dcb30a9e2e1f8cd1be
- 923161f345ed3566707f9f878cc311bc6a0c5268
- 941d001e2974c9762249b93496b96250211f6e0f
- a420fbd6cb9d10db807251564c1c9e1718c6fbc5
- af0c62beca277b97df1afb4f7b318dc48d742638
- b2643228c07d29f7ee1ead76bb4363351216fd17
- b5f884a10072732d853a42d3860d4f81467dea4e
- ba9de479beb82fd97bbdfbc04ef22e08224724ba
- c28ac747eedad47c36e93960dfa19e87e38b6803
- c2eaca8799d335954ef3d9a1867ec1b629ca4f1a
- c4d6c1fd4c1a702a2302cc62bce7d770e5b7369c
- c5b39dec7922bbfd6f7e0d067eaa7339dab6479b
- d373052c6f7492e0dd5f2c705bac6b5afe7ffc24
- d4f6241abe5f46e6b18f10da95d004924eac4ed3
- d7e073f9355723e2e731ee8b46ecb67863d9b81b
- db9ba4f42942b27e1690c6d8a1bbd5b9d188fe49
- ded8a79542421728be812dd6f340de9bac694b87
- e27521c7158c6af3aa58f78fcbed64b17c946f70
- ec4e4760b04d51e4b6f7acaf5a6e86b8620eb8df
- ef63ea46665db65cfc7479c6f2286424bbc46c38
- f070a115100559dcaf31ce34d9e809a3134b2511
- 1895d7c4f785f92e48b5191fd812822593cbc73f
- 2ea20c54564d2550d08c6f9ff5d0560c627f3718
- 5263a135f09185aa44f6b73d2f8160f56779706d
- 73ee462cb96f4857f9f5bbdc4cada5800f2b8932
- 9cdf137e3f2493c9e141d5ec05f890e32b9b4e87
- ae007dba80a0fc03e44a22db3f4e53ed854b4b38
- cecc54143cc375af1b9aed0021643b179574e592
- f8425e27fb5340b4d50bdee1800dcc428a7d388f
- 60854185f6338e1bfc7497fd41aa44c5c00d8f85
- fe8cd9dce3f82e76f5a5651c60c72e638f826ade
- 7e7f666a6839abe1b2cc76176516f54e46a2d453
- 9874546fea08fee04b3271a6366ff6dd3ad6fae2
- 5007943bec2cf5310cfe8b8c49d6f55f79ad0e4c
- a2f1d03ac8c2c3c33c0f77e8882572cac188b762
- 9180ea8ba0cdfe0a769089977ed8396a68761b40

FileHash-SHA256:

- 9b42decb7ea825b939fc36ab924e0c80324e0a4eccb4c371eac60a8672af9603
- 026e8823b1885c0d58e48bda8b0c4501710d181dcf603970cdbfb5782f18281d
- 1cdafbe519f60aaadb4a92e266fff709129f86f0c9ee595c45499c66092e0499
- 4eba4d465f8f5df529f986f89c80b3ab93f6ab86a6da236d7b129fc0228af29a
- 6f31cf7a11189c683d8455180b4ee6a60781d2e3f3aadf3ecc86f578d480cfa9
- a8a7fdbbc688029c0d97bf836da9ece926a85e78986d0e1ebd9b3467b3a72258

- ec8252a333f68865160e26dc95607f2c49af00f78c657f7f8417ab9d86e90bf7
- 1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc
- 27009c0abd2709cd5cac4c0135b8f3bed3229b0921601638ba9e90713ede91ea
- 2afafaf2823e9918d17cdca28648ec94e4d7eabf95b936342456a75be0a1a658
- 2b28270c1675990a2c78b31faab547fb75948dd1c2b22e892377ee5e40abebc2
- 2e2ad6392e75d5a5155498c2a76cb373d17ca3ad4ba57c6d33c623fca5e29342
- 337d21f964091417f22f35aee35e31d94fc3f35179c36c0304eef6e4ae983292
- 35415d97038e091744e9cab3b88c78c1a7ca87f78d2b4a363f72f2c28d65932b
- 379ef7c4f6dfae8cc0c8556861ff41930b88c7d9b107a5de10ccd194e1bda0cb
- 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c
- 3d13fae5e5febfa2833ce89ea1446607e8282a2699aafd3c8416ed085266e06f
- 3f4ceeada7ff021c30df1646437d2ab0e55997bbb281444501f6d1f4ea8fa209
- 4839fd081e720d7d5091274470679c120378196e1f4faf80c4bac08d8ee7bb8c
- 4d24b359176389301c14a92607b5c26b8490c41e7e3a2abbc87510d1376f4a87
- 6192beb56de670de902193a33380e5eb0f3b4b2e3e848e7eea8950075f00f2e5
- 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33
- 67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4
- 6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360
- 7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488
- 8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50
- 8bfa4c2c1065b105ec80a86f460e0e0221b39610109cc6cd4b441dd86e6b4aef
- 920384692233578a59fc8de2b0205fd9fb20bb0d75c1d5a1534377abf0fc08bc
- 92072945358b605c024b9e3335fb33b82faf33048c56f5529aaf5af4bf0c1b30
- 9bf7692f8da52c3707447deb345b5645050de16acf917ae3ba325ea4e5913b37
- b3f473b0fd752fcd8b0d5983366c4ccccdacdceb8d6ba25fcb02b34c622cca78
- bb6cf834a990f8edf79d87981cfffcb8beb86e82a55ec4afe0a718da795a38da
- c239dadd55b55b817fda5b0c2bb062adf399a5b78a8b3280a473d3ae66f81777
- c9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0
- cfbcea795524c69a6d28fd9e60e07437d8f2abd23812109430ca2efd46606310
- d1aa0ceb01cca76a88f9ee0c5817d24e7a15ad40768430373ae3009a619e2691
- d371ee0aa4fa710c00173d296c999a5497a18b38c80095db68a2dc5e46ed35f7
- f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e
- fb2433beb961839b36198e242d0dedb7fa85ab3e08a1141d02874aa4235ac776
- 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d
- 131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07
- 18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88
- 1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386
- 20739e8fc050187af013e2499718895e4c980699ccaf046b2f96b12497e61959
- 3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75
- 5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32
- 7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4
- 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be
- 892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0
- 9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065
- aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d
- aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9
- bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138
- d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca
- dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e

- ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc
- 36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c
- 73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf
- 8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694
- 1c1ef7736dd95ea9aa2dc5784dc51977a1d890c92159e16315ef15546556bcdf
- 2b02d732c6c46d8cb3758851c9e79a52761956109f55407c1a5d693a8a1af1f3
- 681697c35dbb1beba9886f5c44882ccca32dd7e9e483a381e981e7409a0e35cb
- b711f7617f507053a131a75b0971409f76663b404aa1c51bfbe2cd32f2ac8fb8
- be8257317bea80a1ed670d70eb4f21bba246c266a59724185b366c2dcfb2b8ea
- dfee389e1ffa09ed81adcf0d0f165d859e0c045ad7d90f6edcf3f96dfcceba2b
- 595c869f8ec7eaf71fef44bad331d81bb934c886cdff99e1f013eec7acdaf8c9
- b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9e08687796be30e2093286c
- b64acb7dcc968b9a3a4909e3fddc2e116408c50079bba7678e85fee82995b0f4
- 12a6d61b309171b41347d6795002247c8e2137522a756d35bb8ece5a82fc3774
- 1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296
- e1321a4b2b104f31aceaf4b19c5559e40ba35b73a754d3ae13d8e90c53146c0f
- 74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1
- 3d2b58ef6df743ce58669d7387ff94740ceb0122c4fc1c4ffd81af00e72e60a4
- 0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43
- 0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f
- a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc
- 03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45
- 2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422
- 40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5
- 5ea65e2bb9d245913ad69ce90e3bd9647eb16d992301145372565486c77568a2
- 643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562
- 6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84
- fef09b0aa37cbdb6a8f60a6bd8b473a7e5bffdc7fd2e952444f781574abccf64
- 0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c
- dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198
- 9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c
- 2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83
- 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a

Hostname:

- DESKTOP-3GCJKGQ
- WIN-KFUMVU06ESH
- WIN-OX9CQTDSEIK
- WIN-MV7S8OJTOIK
- DESKTOP-KT76603
- HOST14872171171

IPv4:

- 77.247.126.158
- 13.107.42.12
- 104.200.72.33
- 170.130.165.171
- 185.82.216.56
- 45.227.254.26
- 80.66.88.203
- 152.89.196.111

- 185.11.61.114
- 194.26.29.102
- 91.240.118.29
- 91.132.92.60
- 138.124.184.174
- 148.72.168.13
- 148.72.171.171
- 199.127.60.236

URL:

- https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion

3. RECOMENDACIONES:

- Desconfiar de los adjuntos y enlaces de correo electrónico, y verificar siempre el remitente.
- Ejecutar la estrategia 3-2-1-1-0 de copias de seguridad, que consiste en realizar periódicamente tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube; además una de las copias esté disponible fuera de conexión, y cero copias sin verificar o con errores.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Priorizar la reparación de vulnerabilidades explotadas conocidas.
- Habilitar la autenticación multifactor (MFA) para todos los servicios en la medida de lo posible, especialmente para correo web, VPN y cuentas que acceden a sistemas críticos.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware.
- Aplicar parches y actualizar periódicamente el software y las aplicaciones a su última versión y realizar evaluaciones de vulnerabilidad periódicas.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar ransomware y otro software malicioso antes de que puedan cifrar sus archivos.
- Implementar soluciones de seguridad avanzadas, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), para identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Implementar un plan de recuperación.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°177	Fecha: 01-08-2024
		Página: 12 de 17

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en BIG-IP Next Central Manager		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo agotamiento de los recursos, condición de carrera y omisión de autenticación mediante una ruta o canal alternativo en BIG-IP Next Central Manager. La explotación exitosa de estas vulnerabilidades podría permitir a un usuario local realizar un ataque de denegación de servicio (DoS) y aumentar privilegios en el sistema. Asimismo, un atacante remoto no autenticado podría comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-46747 de tipo omisión de autenticación mediante una ruta o canal alternativo, podría permitir a un atacante remoto comprometer el sistema afectado. La vulnerabilidad existe debido a una autenticación incorrecta en la utilidad de configuración. Un atacante remoto no autenticado puede enviar solicitudes especialmente diseñadas al sistema, eludir la autenticación y ejecutar comandos arbitrarios en el dispositivo. Esta vulnerabilidad está siendo explotada en la naturaleza.

La vulnerabilidad de severidad **baja** denominada "**GhostRace"**, identificada por MITRE como CVE-2024-2193 de tipo condición de carrera, podría permitir a un usuario local aumentar privilegios en el sistema. La vulnerabilidad existe debido a una condición de carrera especulativa. Un usuario local puede explotar la carrera y obtener acceso no autorizado al contenido de la memoria del host arbitrario, incluida la memoria asignada a otros invitados. Esta vulnerabilidad puede explotarse localmente. El atacante debe tener credenciales de autenticación y autenticarse correctamente en el sistema.

La vulnerabilidad de severidad **baja,** identificada por MITRE como CVE-2024-26602 de tipo agotamiento de los recursos, podría permitir a un usuario local realizar un ataque de DoS. La vulnerabilidad existe debido a una gestión inadecuada de los recursos en kernel/sched/membarrier.c. Un usuario local puede provocar el agotamiento de los recursos y realizar un ataque de DoS. Esta vulnerabilidad puede explotarse localmente. El atacante debe tener credenciales de autenticación y autenticarse correctamente en el sistema.

A. Productos afectados:

- BIG-IP Next Central Manager: 20.0.1 - 20.2.0.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://my.f5.com/manage/s/article/K000140297

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°177	Fecha: 01-08-2024 Página: 13 de 17

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el servicio web Exacqvision de Johnson Controls		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo política permisiva entre dominios con dominios no confiables que afecta al servicio web Exacqvision de Johnson Controls. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante enviar una solicitud no autorizada o acceder a datos de un dominio no confiable.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-32862 de tipo política permisiva entre dominios con dominios no confiables, se debe a que, en determinadas circunstancias, el servicio web Exacqvision no proporciona protección suficiente contra dominios que no son de confianza.

A. Productos afectados:

- Exacqvision Web Service: 22.12.1.0.

3. RECOMENDACIÓN:

- Actualizar el servicio web afectado a la versión 24.06 que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-214-02

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°177	Fecha: 01-08-2024
		Página: 14 de 17

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Nueva campaña de phishing dirigida a usuarios de Microsoft OneDrive		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

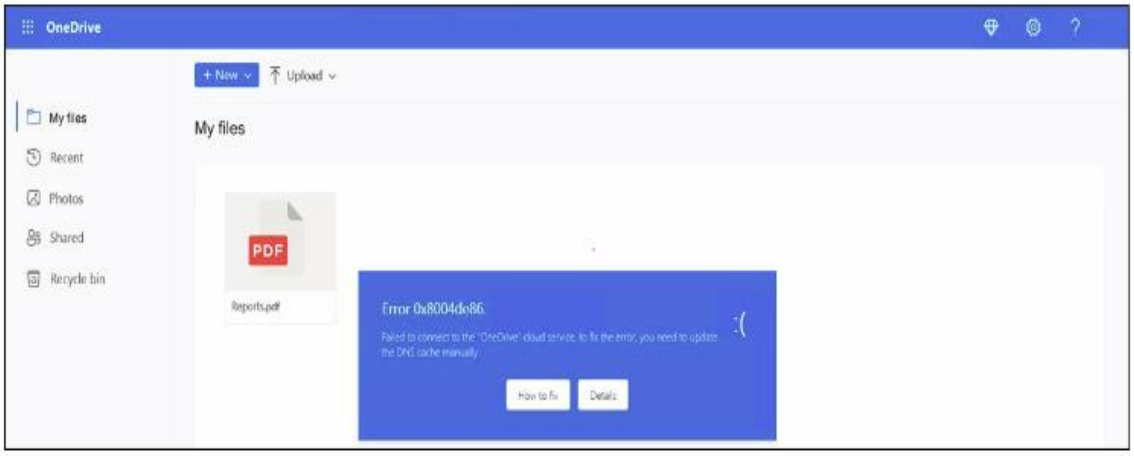
1. ANTECEDENTES:

Los investigadores de seguridad del Centro de investigación avanzada de Trellix han descubierto una sofisticada campaña de phishing/downloader dirigida a los usuarios de Microsoft OneDrive. La campaña emplea tácticas avanzadas de ingeniería social para engañar a los usuarios para que ejecuten un script de PowerShell. Un ataque exitoso podría permitir a un atacante remoto a comprometer sus sistemas.

2. DETALLES:

Los investigadores de seguridad han descubierto una sofisticada campaña de phishing dirigida a los usuarios de Microsoft OneDrive. En esta campaña, los atacantes emplean tácticas avanzadas de ingeniería social para engañar a sus víctimas para que ejecuten un script malicioso de PowerShell. Un ataque exitoso podría permitir a un atacante remoto a comprometer sus sistemas.

El vector del ataque inicial comienza con un correo electrónico que contiene un archivo HTML que insta a sus víctimas a resolver un problema de DNS para acceder a un archivo de Microsoft OneDrive. Al abrir el archivo HTML, se muestra una imagen que simula una página de OneDrive, que muestra un mensaje de error sobre un problema de DNS con dos botones: “Details” y “How to fix”. Al hacer clic en “Details”, los usuarios son dirigidos a una página legítima de Microsoft Learn sobre la resolución de problemas de DNS. Sin embargo, el botón “How to fix” ejecuta una función de JavaScript dentro del archivo HTML, guiando a los usuarios para que abran la terminal de Windows PowerShell y ejecuten un comando específico.



Cuando se ejecuta, el comando vacía la caché de DNS y crea una carpeta llamada “descargas” en la unidad C:. Luego descarga un archivo, extrae su contenido y ejecuta un script.

Los investigadores de Trellix indicaron que esta secuencia de acciones resalta el uso que hacen los atacantes de procesos de apariencia legítima para engañar a los usuarios y hacer que comprometan sus sistemas. Esta combinación de jerga técnica y mensajes de error urgentes es una táctica clásica de ingeniería social, diseñada para manipular las emociones del usuario y provocar una acción apresurada sin una consideración cuidadosa.

Al decodificar cadenas codificadas en Base64 y copiar comandos al portapapeles, los atacantes manipulan eficazmente a los usuarios para que ejecuten el script malicioso.

En esta campaña, mediante ataques de la ingeniería social en el panorama de la ciberseguridad, los atacantes pueden infiltrarse incluso en los entornos más seguros, al aprovecharse de las emociones y la confianza de los usuarios.

A. Productos afectados:

- Usuarios de Microsoft OneDrive.

B. Indicadores de compromiso (IoC):

Archivo adjunto por correo electrónico con el siguiente formato de nombre de archivo (las fechas y los números varían):

- clarify_27-May_202017.html
- clarify_27-May_690357.html
- clarify_15-june_586190.html

Hashes de muestras analizadas para el archivo adjunto .html:

- d6faa6bd1732517f260d94feb3cdbfc2
- 1152103edc64ddee7ea4e07cd5dd78ae
- ef082ddcbf5c94f1da1d2026d36b6b3f
- 55cf60a640fc773a7c38de9c5e44da30
- cf16271bfe826db5ef0c1a67433a619f
- 7f5c82eadbaadec6ba2b004fbafa9a31
- 328110e6c36cd70edac6bea395c40b18
- 363b4f9fdb1e2a5926037b207caecfe5
- b183269587055f35cb23d2d33ff3f5fa
- 2df579460a76631836d108578af4caa5
- 0e36cf2719295596da0c7ef10b11df15
- 7707ef4e03f0b1ab6b6fb96757a6
- d524addd18d8014d72abb9dd172e782d
- ef9d05bb8a24bec1d94123c90b1268bb
- 4341f0372eda93afce82908014f420d9
- 30997b5e63297c58c4f9fe73c8c200ac
- eed2174f5b87d58b1b0baea0e509e141
- sordo955bbf5d66db200e366ae3563eab
- cac3c4005f952293b383021994947 59a
- 08da892161bbf09f1437dade7

Una carpeta llamada c:\downloads que contiene estos archivos:

- Un archivo .zip de 2 caracteres (por ejemplo, st.zip, D7.zip, wi.zip, C9.zip, DJ.zip, Ap.zip, hf.zip)
- Un script de AutoIt llamado script.a3x
- Un ejecutable de AutoIt llamado AutoIt3.exe

Hashes MD5 para muestras conocidas de la carga útil del script AutoIt:

- beb8a50f67424c3b70cb56fc8833d246
- 04cdff477585cb0747ecd20052f03c2e
- 404bd47f17d482e139e64d0106b8888d
- 7a7d09b4bcd75bc7d7badd3c117596f7
- a1846e262d900f56f4a7d5f51100ec44
- dfa96717b69fa69d264a60b9de36f078
- 253cdeabd5e429832f9bbd7f37dd0798

Hash de la versión de AutoIt3.exe utilizada en el ataque:

- c56b5f0201a3b3de53e561fe76912bfd

Hashes MD5 para muestras conocidas de los archivos .zip:

- 763d557c3e4c57f7d6132a444a930386
- d0ad617ed1812822eebc9592d49a575c
- 1ff108f1bfb39b21db5f1d4f7ad56bf2
- 96bb795d111717109fac22f8433c7e27
- 0852c3e7903dd3b1db6a6b232c33a25a
- e0768bce522927eb89f74750e09f2a1c
- 7133ae7dd452aa6469c85e236a59159e

Sitios web:

- hxxps://kostumn1[.]ilabserver[.]com

Cabe indicar que este sitio está marcado como PUP (programas potencialmente no deseados) de alto riesgo por Skyhigh security en hxxps://trustedsource.org/.

Firmas de detecciones de Trellix ENS para los IoC:

- HTML/Phishing.xl
- AUTOIT/Agent.p
- AutoIt/Agent.o
- PS/Agent.jc

3. RECOMENDACIONES:

- No responder a correos electrónicos que soliciten información personal o financiera. Los atacantes suelen simular ser entidades confiables, como bancos, y pueden pedirte que ingreses datos en sitios falsificados;
- Verificar que el nombre y la dirección de correo electrónico del remitente sean conocidos y legítimos. Observar con atención a detalles como errores gramaticales o enlaces que no coinciden con la dirección oficial de la entidad;
- Evitar hacer clic en enlaces o descargar archivos adjuntos de fuentes no verificadas. Estos pueden contener malware que compromete tu dispositivo;
- Implementar MFA puede añadir una capa adicional de seguridad, dificultando el acceso no autorizado incluso si tus credenciales son comprometidas;
- Mantener el sistema operativo, navegadores y software de seguridad siempre actualizados para protegerte contra vulnerabilidades conocidas;
- Capacitar a los empleados para que reconozcan y respondan adecuadamente a intentos de ataques de phishing;
- Mantener un control sobre tus cuentas en línea y cierra aquellas que no utilices. Se debe cambiar las contraseñas con regularidad y verificar si alguna ha sido expuesta en violaciones de datos;
- Considera usar navegadores que bloqueen sitios de phishing conocidos y mantener habilitadas las funciones de seguridad.

Fuente de Información:	• hxxps://www.trellix.com/blogs/research/onedrive-pastejacking/

Índice alfabético