Avizu APT40

Artesanatu MSS RPC iha asaun

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

Índise

Vizaun Jerál:

Fundu

Avizu ida ne'e, autoria husi Sentru Seguransa Sibernétika Australianu ninia Diresaun Sinal Australianu (ACSC nia ASD), Ajénsia Seguransa Sibernétika no Infraestrutura Estadus Unidus (CISA), Ajénsia Seguransa Nasional Estadus Unidus (NSA), Federal Bureau of Investigation (FBI) Estadus Unidus, Sentru Nasional Seguransa Sibernétika Reinu Unidu (NCSC-UK), Sentru Seguransa Sibernétika Kanadá (CCCS), Sentru Nasional Seguransa Sibernétika Nova Zelândia (NCSC-NZ), Servisu Federal Intelijénsia Alemanha (BND) no Gabinete Federal ba Protesaun Konstituisaun (BfV), Servisu Nasional Intelijénsia República Koreia (NIS) no NIS nia Sentru Nasional Seguransa Sibernétika, no Japaun-nia Sentru Nasional Preparasaun Insidenti no Estratéjia ba Seguransa Sibernétika (NISC) no Ajénsia Polisia Nasional (NPA) – depois husi ne'e refere nu'udar "Ajénsia autoria sira" – esplika grupu sibernétiku ne'ebé patrosinadu ho Estadu República Popular China (RPC) no sira-nia ameasa atuál ba rede Australianu sira. Avizu ne'e bazeia ba ajénsia autór sira-nia komprensaun ne'ebé partilla kona-ba ameasa no mós ASD nia ACSC investigasaun resposta ba insidente sira.

Grupu sibernétiku ne'ebé patrosinadu hosi estadu PRC nian uluk alvu ona organizasaun sira iha nasaun oioin, inklui Austrália no Estadus Unidus, no téknika sira ne'ebé destaka iha kraik ne'e regularmente uza ho atór sira seluk ne'ebé patrosinadu husi estadu PRC nian iha nivel mundiál. Tanba ne'e, ajénsia autór sira fiar katak grupu, no téknika sira ne'ebé hanesan nafatin sai ameasa ida ba sira nia nasaun nia rede sira hotu.

Ajénsia autór sira avalia katak grupu ida-ne'e kondutu operasaun sibernétiku malisiozu sira ba Ministériu Seguransa Estadu (MSS) PRC nian. Atividade no téknika sira sobrepassa ho grupu sira ne'ebé rastreiu nu'udar Amease Persisténsi Avansadu (APT) 40 (koñesidu mós nu'udar Kryptonite Panda, GINGHAM TYPHOON, Leviathan no Bronze Mohawk iha relatóriu indústria nian). Grupu ida-ne'e uluk relata ona katak nia bazeia iha Haikou, Provínsia Hainan, PRC no simu knaar hosi PRC MSS, Departamentu Seguransa Estadu Hainan.[2] Avizu tuirmai fornese amostra ida hosi estudu kazu signifikativu sira kona-ba adversáriu nia téknika sira iha asaun kontra rede vítima rua. Estudu kazu ne'e konsekuensial ba pratikante seguransa siber sira atu identifika, prevene no remedia intrusaun APT40 sira kontra sira-nia rede rasik. Estudu kazu nomeiadu ne'e mak sira ne'ebé remediasaun apropriu realiza ona atu redus risku ba re-esplorasaun ho atór ameasa ida ne'e ka sira seluk. Nune'e, estudu kazu sira naturalmente tuan liu iha natureza, atu asegura katak organizasaun sira hetan tempu nesesáriu atu hadi'a.

Rezumu atividade

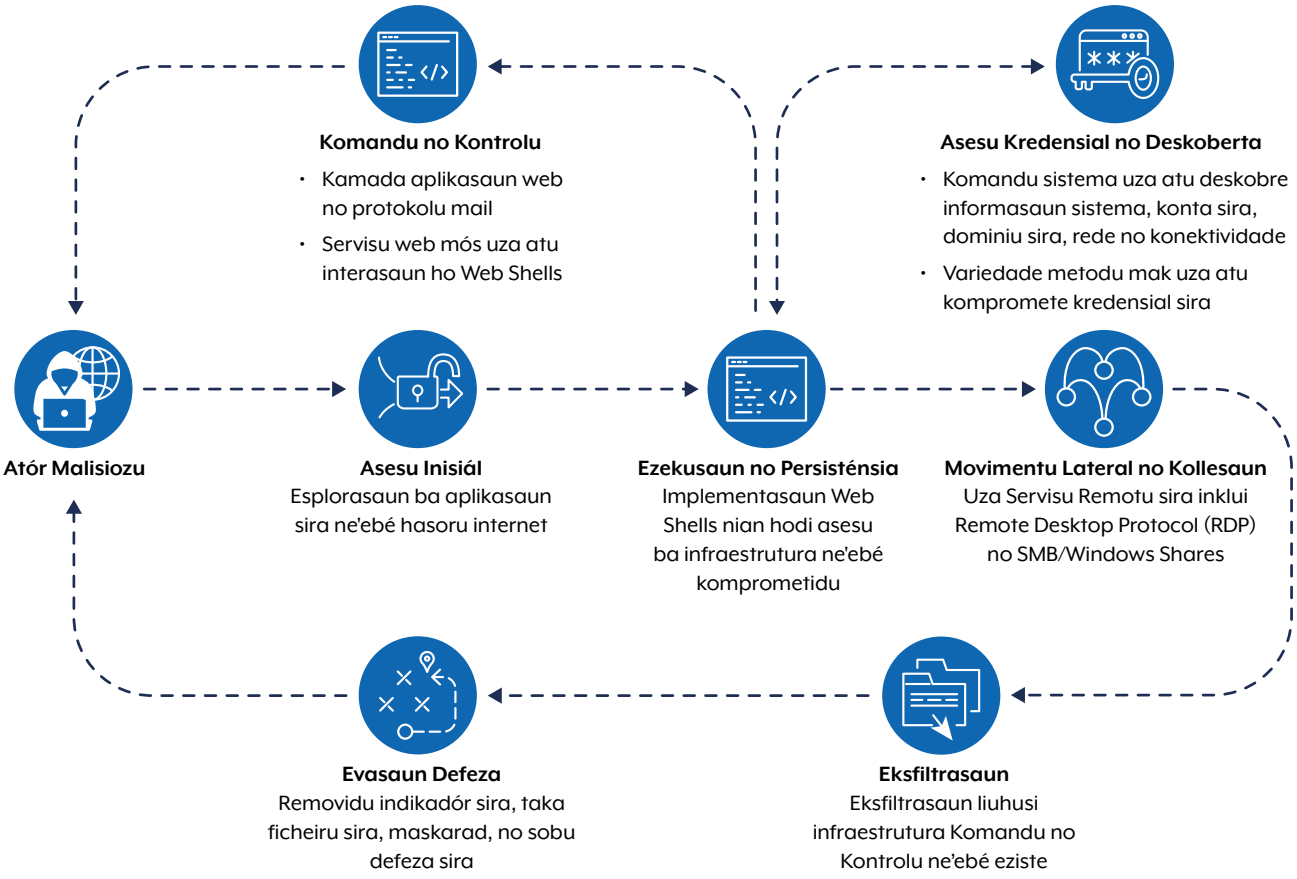
APT40 alvu beibeik ba rede Austrálianu sira no mós rede governu no setór privadu sira iha rejiaun laran, no ameasa ne'ebé sira aprezenta ba ami nia rede ne'e kontinua hela. Artesanatu ne'ebé deskreve iha avizu ida-ne'e observa regularmente kontra rede Australianu sira.

Notavelmente, APT40 iha kapasidade atu transforma lalais no adapta esplora prova-konseitu (sira) husi vulnerabilidade foun sira no utiliza kedas sira kontra rede alvu sira ne'ebé iha infraestrutura husi vulnerabilidade asosiadu. APT40 hala'o rekoñesimentu regularmente kontra rede interese sira, inklui rede iha nasaun ajénsia autór sira, hodi buka oportunidade sira atu kompromete ninia alvu sira. Rekoñesimentu regulár ida-ne'e postura grupu atu identifika dispozitivu sira ne'ebé vulneravel, iha finál vida ka la mantein ona iha rede sira ne'ebé iha interese, no atu koloka lalais esplorasaun sira. APT40 kontinua hetan susesu ba esplora vulnerabilidade sira hahú kedas husi 2017.

APT40 esplora lalais vulnerabilidade públiku foun sira iha software ne'ebé uza boot liutan hanesan Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) no Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473). ASD nia ACSC no ajénsia autor sira hein katak grupu ne'e sei kontinua uza POC ba vulnerabilidade sira ho perfillu foun aas iha oras ka loron balun nia laran hafoin fó sai públiku.

2 Departementu Justisa EUA 2021 Sidadaun Xinés na'in haat ne'ebé servisu ho Ministériu Seguransa Estadu nian akuzadu tanba Kampaña Intrusaun Komputadór Globál ne'ebé Alvu Propriedade Intelektuál no Informasaun Negósiu Konfidensiál, Inklui Peskiza Moras Infesiozu.

Figura 1: Fluxugrama TTP ba atividade APT40



Grupu ida-ne'e parese prefere ba esplora infraestrutura vulneravel, ne'ebé hasoru públiku duké tékniku sira ne'ebé presiza interasaun uzuáriu nian, hanesan kampaña phishing, no tau prioridade aas atu hetan kredensial válidu sira hodi permite atividade akompañamentu variedade. APT40 uza web shell regularmente (T1505.003) ba persisténsia, partikularmente iha inísiu siklu moris intrusaun ida nian. Normalmente, hafoin asesu inisiál ne'ebé susesu APT40 foka ba estabelesimentu persisténsia hodi mantein asesu ba vítima nia ambiente. Maibé, tanba persisténsia akontese iha inísiu intrusaun ida, ida-ne'e iha posibilidade boot liu atu observa iha intrusaun hotu-hotu – la haree ba estensaun kompromisu nian ka asaun sira seluk ne'ebé foti ona.

Artesanatu ne'ebé notável

Maske APT40 uluk uza ona website australianu sira ne'ebé kompometidu hanesan host komandu no kontrolu (C2) ba nia operasaun sira, grupu ne'e evolui ona téknika ida-ne'e (T1594).

APT40 adota ona tendénsia globál hodi uza dispositivu sira ne'ebé kompometidu, inklui dispositivu eskritóriu ki'ik/eskritóriu uma nian (SOHO), hanesan infraestrutura operasionál no rediresionadór ikus nian (T1584.008) ba nia operasaun iha Austrália. Ida-ne'e permite ona ajénsia autor sira ba karakteriza no rastreiu di'ak liután movimentu grupu ida-ne'e nia.

Dispositivu SOHO sira ne'e barak mak besik mate oa ka ladauk patch no oferese alvu ne'ebé kmaan ba esplorasaun N-day. Bainhira kompometidu, dispositivu SOHO sira oferta pontu lansamentu ida ba atake sira ne'ebé dezeña atu kahur ho tráfiku lejítimu no dezafia defensór rede sira (T1001.003).

Tékniku ida-ne'e mós uza regularmente ho atór sira seluk ne'ebé patrosinadu husi estadu RPC nian iha mundu tomak, no ajénsia autor sia konsidera ida-ne'e hanesan ameasa ida ne'ebé partilla. Ba informasaun adisionál, haree avizu konjuntu sira Atór Sibernétiku sira ne'ebé Patrosinadu hosi Estadu República Populár Xina nian Esplora Fornesedór no Dispozitivu sira Rede nian no Atór sira ne'ebé Patrosinadu hosi Estadu PRC nian Kompromete no Mantein Asesu Persistente ba Infraestrutura Krítiku EUA nian.

APT40 dalaruma uza infraestrutura ne'ebé sosa ka aluga hanesan infraestrutura C2 ne'ebé hasoru vítima iha nia operasaun sira; maske nune'e, artesanatu ida-ne'e parese iha diminuisaun relativu.

Feramenta

ASD nia ACSC partilla ficheiru malisiozu balun ne'ebé identifika ona durante investigasaun sira ne'ebé esplika iha kraik. Ficheiru sira-ne'e deskarga ona ba VirusTotal hodi permite komunidade defeza rede no seguransa sibernétika nian atu komprende di'ak liután kona-ba ameasa sira ne'ebé sira tenke kombate.

Estudu kazu

ASD-nia ACSC ne'e partilla relatóriu investigasaun anonimizadu rua atu fornese konsientementu kona-ba hanusa atór sira funsiona sira-nia feramenta no artesanatu.

MD5	Naran ficheiru	Informasaun adisionál
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java Source
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Java Bytecode
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Java Bytecode
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Java Source
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Java Bytecode
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Java Bytecode
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Java Bytecode
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Java Bytecode
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | Java Bytecode
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Java Source

Estudu kazu 1

Relatóriu ida-ne'e sai anonimizadu atu permite divulgasaun ne'ebé luan liután. Organizasaun ne'ebé hetan impaktu sei hanaran 'organizasaun'. Detallu espesífiku balun hasai tiha ona atu proteje identidade hosi vítima no métodu sira resposta ba insidente hosi ASD nia ACSC.

Rezumu ezekutivu

Relatóriu ida-ne'e esplika detallu kona-ba deskobrimentu sira husi investigasaun ACSC ASD nian kona-ba kompromisu susesu husi rede organizasaun nian entre Jullu no Setembru 2022. Relatóriu investigativu ida-ne'e fornese ba organizasaun hodi halo rezumu ba atividade malisiozu ne'ebé observa no enkuadra rekomendasaun sira ba remedisaun. Deskobrimentu sira indika katak kompromisu ne'e realiza ho APT40.

Iha fulan Agostu nia klaran, ASD nia ACSC notifika organizasaun kona-ba interasaun malisiozu ho sira nia rede husi dispositivu ida ne'ebé provavelmente kompometidu ne'ebé uza ho grupu iha fulan Agostu nia rohan no, ho organizasaun nia konsentimentu, ASD nia ACSC koloka sensor bazeia ba host ba host sira ne'ebé provavelmente afetadu iha organizasaun nia rede. Sensor sira-ne'e permite analista ASD nia ACSC nian resposta ba insiden atu hala'o investigasaun forense dijitál tomak. Uza dadus sensor ne'ebé disponivel, analista ACSC ASD nian halo mapa ho susesu ba grupu nia atividade no kria liña tempu detallu ida kona-ba eventu sira ne'ebé observa ona.

Desde Jullu to'o Agostu, atividade atór xave sira ne'ebé observa husi ASD nia ACSC inklui:

- enumerasaun host, ne'ebé permite atór ida ba harii sira nia mapa rasik husi rede;
- uza web shell, fó ba atór fatin inisiál iha rede no kapasidade atu ezekuta komandu sira; no
- implementasaun husi ferramenta sira seluk ne'ebé aproveita husi atór ba objetivu malisiozu sira.

Investigasaun ne'e deskobre evidénsia dadus sensivel ho kuantidade boot husi sira ne'ebé asesu no evidénsia katak atór sira-nia movimentu lateralmente liuhosi rede (T1021.002). Kompromisu barak maka fasilita husi grupu nia estabelesimentu husi vetor asesu oioin ba rede, rede ne'ebé iha estrutura ne'ebé latan, no uza software mak dezenvolve internamente ne'ebé la seguru ne'ebé bele uza hodi hatama ficheiru sira ho arbiru. Dadus ne'ebé filtradu inklui kredensial autentikasaun privilejiadu ne'ebé permite grupu atu tama, no mós informasaun rede ne'ebé sei permite atór sira atu hetan fali asesu la autorizadu se vetor asesu orijinál hetan blokeia. Laiha ferramenta adisionál ne'ebé maka deskobre duke sira ne'ebé maka iha mákina esploradu inisialmente; maske nune'e, grupu ida nia asesu ba kredensial lejítimu no privilejiadu sira sei nega nesesidade ba ferramenta adisionál sira. Deskobrimentu sira hosi investigasaun indika katak organizasaun ne'e provavelmente sai alvu deliberadamente husi APT40, envezde sai vítima oportunista ba vulnerabilidade ne'ebé koñesidu hosi públiku.

Rezultadu investigasaun

Iha fulan-Agostu nia klaran tinan 2022, ASD nia ACSC notifika organizasaun katak IP malisiozu ida ne'ebé konfirmadu ne'e fiar katak iha afiliasaun ho grupu sibernétiku ida mak patrosinadu hosi estadu, halo ona interasaun ho rede informátika sira organizasaun nian entre pelumenus fulan Jullu no Agostu. Dispositivu ne'ebé hetan kompromete provavelmente pertense ba negósiu ki'ik ka uzuáriu iha uma.

Iha fulan Agostu nia rohan, ASD nia ACSC koloka ajente ida ne'ebé bazeia host ba host iha organizasaun nia rede ne'ebé hatudu evidénsia katak hetan impaktu husi kompromisu.

Artefaktu balun ne'ebé bele suporta esforsu investigasaun nian la disponivel tanba konfigurasaun hosi rejistu ka dezeñu rede nian. Maski nune'e, organizasaun nia prontidaun atu fornese dadus hotu-hotu ne'ebé disponivel. permite respondente insidente ACSC ASD nian atu hala'o análize kompreensivu no atu forma komprensaun ida kona-ba atividade APT40 ne'ebé provável iha rede.

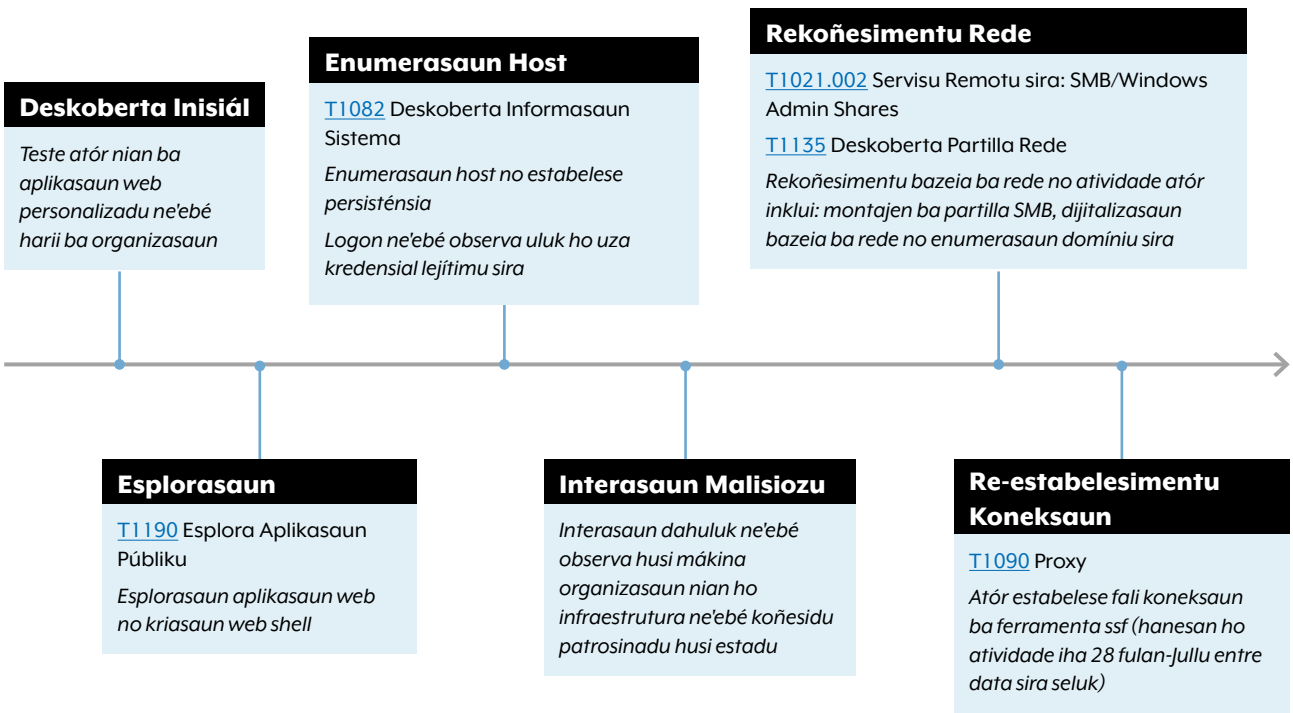
Iha Setembru laran, hafoin konsulta ho ASD nia ACSC, organizasaun deside atu nega lista IP ne'ebé identifika iha notifikasaun inisiál. Iha Outubru, organizasaun hahú remedisaun.

Detallu

Hahú iha fulan-Jullu, atór sira bele koko no esplora aplikasaun web personalizadu ida (T1190) ne'ebé realiza iha `<webapp>2-ext`, permite grupu atu estabelese pontu apoiu iha zona demilitarizada rede nian (DMZ). Ida-ne'e aproveita hodi enumera rede no mós domíniu vizivel sira hotu. Kredensiál kompometidu sira (T1078.002) uza hodi halo konsulta ba Active Directory (T1018) no eksfiltra dadus ho monta partilla ficheiru sira (T1039) iha mákina DMZ oioin. Atór hala'o atake Kerberoasting ida atu hetan kredensial rede válidu sira husi servidór ida (T1558.003). Observadu grupu ne'e parese la hetan pontu prezensa adisionál ruma iha DMZ ka iha rede internu.

Liña tempu vizuál

Liña tempu iha kraik fornese vizaun jerál luan ida kona-ba faze xave sira hosi atividade atór malisiozu nian ne'ebé observa iha rede organizasaun nian.



Liña tempu detallu

Jullu: Atór sira estabelese ligasaun inisiál ida ba pájina oin husi aplikasaun web personalizadu (T1190) ne'ebé harii ba organizasaun (iha ne'e refere hanesan 'aplikasaun web' ka '*webapp*') liuhusi ligasaun seguransa kamada transporte (TLS) (T1102). Laiha atividade notavel seluk ne'ebé maka observa.

Jullu: Atór sira hahú enumera aplikasaun web nia website hodi buka pontu finál sira[2] atu investiga liután.

Jullu: Atór sira konsentra iha tentativa hirak atu esplora pontu finál espesífiku ida.

Jullu: Atór sira bele ho susesu `POST` ba servidór web, provavelmente liuhusi web shell ne'ebé tau iha pájina seluk. IP segundu, ne'ebé provavelmente uza ho atór sira mak hanesan, mós hahú publika ba URL ne'ebé hanesan. Atór sira kria no koko númeru ida husi web shell ne'ebé provável.

Métodu esplorasaun loloos ne'e mak deskoñesidu, maibé klaru katak pontu finál espesífiku ne'e alvu atu kria ficheiru sira iha `<webapp>2-ext`.

ASD nia ACSC fiar katak koneksaun enderesu IP rua ne'e halo parte iha intrusaun ne'ebé hanesan tanba sira nia interese ne'e partilla no koneksaun inisiál sira ne'ebé akontese iha minutu balun nia laran.

Jullu: Grupu kontinua hala'o enumerasaun host nian, buka oportunidade sira ba eskalasaun priviléjiu nian, no implementa web shell ida ne'ebé diferente. Atór sira tama iha aplikasaun web uza kredensial sira ne'ebé kompometidu ba `<naranprimeiru.naran>@<domíniu organizasaun>`.

Atór sira-nia atividade la parese atu atinji ho susesu eskalasaun priviléjiu iha `<webapp>2-ext`. Envezde, atór sira muda ba atividade bazeia ba rede.

Jullu: Atór koko kredensial sira ne'ebé kompometidu ba konta servisu ida[3] ne'ebé provavelmente hetan kódigu metin iha bináriu sira mak asesivel internamente.

Jullu: Atór sira koloka ferramenta open-source Secure Socket Funnelling, ne'ebé mak uza hodi liga ba infraestrutura malisiozu nian. Koneksaun ida-ne'e uza atu halo túnel ba tráfiku husi mákina atake atór nian tama ba rede internu organizasaun nian, ne'ebé naran mákina sira espozitu iha rejistu eventu nian bainhira sira tenta atu uza kredensial ba konta servisu nian.

Agostu: Atór sira haree hala'o atividade limitadu, inklui la konsege estabelese koneksaun sira ne'ebé envolve konta servisu nian.

Agostu: Atór sira hala'o enumerasaun rede no Active Directory ne'ebé signifikativu. Konta kompometidu ida ne'ebé diferente ne'e subsekuentemente uza hodi monta partilla sira[4] iha mákina Windows iha DMZ nia laran, hodi permite eksfiltrasaun dadus ne'ebé susesu.

Ida-ne'e parese hanesan utilizasaun oportunista husi kredensiál ne'ebé nauk iha mákina sira mak bele monta iha DMZ. Firewall sira blokeia atór atu labele alvu ba rede internu ho atividade ne'ebé hanesan.

Agostu – **Setembru:** Instrumentu SSF estabelese fali koneksaun ida ba IP malisiozu ida. Grupu ne'e la hetan observasaun hala'o atividade adisionál ruma to'o sira nia asesu hetan blokeia.

Setembru: Organizasaun blokeia IP ne'ebé malisiozu hodi nega ida-ne'e iha sira nia firewall.

2 Iha kontestu ida-ne'e, pontu finál ne'e mak funsaun ida husi aplikasaun web

3 Konta servisu sira la'ós liga ba uzuáriu individuál sira, maibé liuliu ba servisu sira. Iha domíniu korporativu Microsoft nian, iha konta oioin.

4 Monta partilla sira ne'e mak prosesu atu halo ficheiru sira iha estrutura sistema ficheiru nian ne'ebé asesivel ba uzuáriu ida ka grupu uzuáriu nian.

Tátika atór nian no téknika sira

Enkuadramentu MITRE ATT&CK ne'e mak kolesaun dokumentadu ida kona-ba tátika no téknika sira ne'ebé uza ho atór ameasa sira iha espasu siber. Enkuadramentu ne'e kria husi organizasaun naun lukrativu EUA nian The MITRE Corporation no funsiona hanesan linguajen globál komún ida kona-ba hahalok atór ameasa nian.

ASD nia ACSC avalia tékniku no tátika sira tuirmai atu sai relevante ba atividade atór malisiozu:

Rekoñesimentu

T1594 – Peskiza Website sira ne'ebé maka Vítima sira mak na'in

Atór ne'e enumera aplikasaun web personalizadu nia website hodi identifika oportunidade sira atu asesu ba rede.

Asesu Inisiál

T1190 – Esplora Aplikasaun ne'ebé hasoru Públiku (kona-ba esplora aplikasaun web personalizadu)

T1078.002 – Konta sira ne'ebé válidu: Konta Domíniu sira (kona-ba tama ho kredensial sira ne'ebé kompremete)

Esplora aplikasaun web personalizadu sira ne'ebé hetan espozisaun ba internet fornese pontu asesu inisiál ida ba atór. Atór ne'e depois bele uza kredensial sira ne'ebé kompromete ona hodi aumenta sira nia asesu ba rede.

Ezekusaun

T1059 – Intérprete Komandu no Scripting (kona-ba ezekusaun komandu liuhusi web shell)

T1072 – Feramenta Implementasaun Software (kona-ba atór ne'ebé uza feramenta open-source Secure Socket Funneling (SSF) hodi konekta ba IP)

Persisténsia

T1505.003 – Servidór Komponente Software: Web Shell (kona-ba uza web shell no SSF hodi estabelese asesu)

Asesu Kredensial

T1552.001 – Kredensiál sira husi Loja Senha nian (kona-ba ficheiru senha nian ne'ebé relasiona ho sistema jestaun edifísiu nian (BMS))

T1558.003 – Nauk ka falsifika Billeti Kerberos nian: Kerberoasting (kona-ba atake atu hetan kredensial rede nian)

Movimentu Lateral

T1021.002 – Servisu Remotu: SMB Shares (kona-ba atór ne'ebé monta SMB shares husi dispositivu oioin)

Kollesaun

T1213 – Dadus husi Repositóriu Informasaun sira (kona-ba manuál/dokumentasaun ne'ebé hetan iha servidór BMS)

Eksfiltrasaun

T1041 – Eksfiltrasaun Liuhosi Kanál C2 (kona-ba eksfiltrasaun dadus atór nian hosi Active Directory no partilla montante)

Estudu kazu 2

Relatóriu ida-ne'e sai anonimizadu atu permite divulgasaun ne'ebé luan liután. Organizasaun ne'ebé hetan impaktu sei hanaran 'organizasaun'. Detallu espesífiku balun hasai tiha ona atu proteje identidade hosi vítima no métodu sira resposta ba insidente hosi ASD nia ACSC.

Rezumu ezekutivu

Relatóriu ida-ne'e fó sai detallu kona-ba deskobrimentu sira husi investigasaun ACSC ASD nian kona-ba kompromisu susesu husi rede organizasaun nian iha Abril 2022. Relatóriu investigasaun ida-ne'e fornese ba organizasaun hodi halo rezumu ba atividade malisiozu ne'ebé observa no enkuadra rekomendasaun sira ba remedisaun. Deskobrimentu sira indika katak kompromisu ne'e realiza ho APT40.

Iha Maiu 2022, ASD nia ACSC notifika organizasaun ida kona-ba atividade malisiozu ne'ebé deskonfia fó impaktu ba organizasaun nia rede dezde Abril 2022. Tuir mai, organizasaun informa ba ASD nia ACSC katak sira deskobre ona software malisioso iha servidór ida ne'ebé hasoru internet ne'ebé fornese portál login ba organizasaun nia solusaun asesu remotu korporativu. Servidór ida-ne'e uza asesu remotu ba login no produtu jestaun identidade no sei refere iha relatóriu ida-ne'e hanesan 'dispositivu ne'ebé kompromet idu'. Relatóriu ida-ne'e esplika detallu kona-ba deskobrimentu investigasaun nian no konsellu remedisaun nian ne'ebé dezenvolve ba organizasaun hodi hatán ba investigasaun ne'ebé hala'o hosi ASD nia ACSC.

Evidénsia indika katak parte ida husi rede organizasaun hetan kompromete husi atór malisiozu sibernétiku liuhosi portál asesu remotu organizasaun nian dezde pelumenus fulan-Abril 2022. Servidór ida-ne'e bele hetan kompromisu husi atór oioin, no provavelmente hetan afetadu husi vulnerabilidade ezekusaun kódigu remotu (RCE) ne'ebé maka hetan publisidade luan iha tempu kompromisu nian.

Atividade atór xave sira ne'ebé observa husi ASD nia ACSC inklui:

- enumerasaun host, ne'ebé permite atór ida ba harii sira nia mapa rasik husi rede;
- esplorasaun ba aplikasaun sira ne'ebé hasoru internet no uza web shell, fó ba atór pontu apoiu inisiál iha rede no kapasidade atu ezekuta komandu sira;
- esplorasaun ba vulnerabilidade software nian hodi aumenta priviléjiu sira; no
- halibur kredensial sira hodi permite movimentu laterál

ASD nia ACSC deskobre katak atór malisiozu ida eksfiltra ona par naran uzuáriu no senha úniku atus balun iha aparellu ne'ebé kompromet idu iha Abril 2022, no mós kódigu autentikasaun multi-fatór lubuk ida no artefaktu tékniku sira ne'ebé relasiona ho sesaun asesu remotu. Bainhira organizasaun halo revizaun, senha mak hetan sai lejítimu. ASD nia ACSC avalia katak atór ne'e halibur artefaktu tékniku sira-ne'e hodi nauk ka kria sesaun login remotu hanesan uzuáriu lejítimu, no asesu ba rede korporativa internu organizasaun nian uza konta uzuáriu lejítimu.

Rezultadu investigasaun

Rezumu investigasaun

ASD nia ACSC determina katak atór kompromete aparellu ne'ebé fornese sesaun login remotu ba pesoál organizasaun nian no uza kompromisu ida-ne'e hodi tenta hala'o atividade liutan. Aparellu sira-ne'e kompostu hosi host na'in tolu ne'ebé iha ekilíbriu karga nian iha ne'ebé mak detekta evidénsia dahuluk kona-ba kompromisu. Organizasaun taka host rua hosi host tolu ne'ebé iha ekilíbriu karga nian lakleur hafoin kompromisu inisiál. Nu'udar rezultadu, atividade subsekuente hotu akontese iha host ida de'it. Servidór sira seluk ne'ebé asosiadu ho aparellu ne'ebé kometidu mós hetan ekilíbriu karga nian iha maneira ne'ebé hanesan. Ba lejibilidade, aparellu kometidu hotu-hotu refere iha maioria relatóriu ida-ne'e hanesan 'aparellu ida de'it'.

Atór ne'e fiar katak uza ona vulnerabilidade sira ne'ebé públiku koñese hodi koloka web shell sira ba aparellu ne'ebé kometidu hahú iha fulan-Abril 2022 ba oin. Atór ameasa sira husi grupu ne'e avaliadu ona katak hetan ona priviléjiu sira ne'ebé aumenta iha aparellu. ASD nia ACSC labele determina atividade nia estensaun tomak tanba falta disponibilidade rejistu. Maibé, evidénsia iha dispositivu indika katak atór ida atinji buat sira tuirmai:

- Kolesaun husi par naran uzuáriu no senha jenuínu atus balun; no
- Kolesaun artefaktu tékniku sira ne'ebé bele permite atór malisiozu ida ba asesu sesaun infraestrutura desktop virtuál (VDI) hanesan uzuáriu lejítimu.

ASD nia ACSC avalia katak atór sei buka atu hasa'e liután kompromisu husi rede organizasaun nian. Artefaktu sira ne'ebé mak atór hasai bele permite sira atu nauk ka hahú sesaun desktop virtuál sira hanesan uzuáriu lejítimu, karik hanesan uzuáriu ne'ebé sira hili, inklui administradór sira Atór bele uza ona vetor asesu ida ne'e hodi kompromete liután servisu organizasaun nian hodi atinji persisténsia no objetivu sira seluk.

Aparellu organizasaun sira seluk iha ambiente jeridu fornesedór hosting nian la hatudu evidénsia kompromisu nian.

Asesu

Host ho aparellu ne'ebé kometidu fornese autentikasaun liuhusi Active Directory no webserver ida, ba uzuáriu sira ne'ebé konekta ba sesaun VDI (T1021.001).

Lokasaun	Naran host sira ba aparellu ne'ebé kometidu (ekilibradu ho karga)
Sentru dadus 1	HOST1, HOST2, HOST3

Infraestrutura aparellu nian inklui mós host portaun asesu nian ne'ebé fornese túnel ida ba VDI ba uzuáriu, bainhira sira iha token autentikasaun ne'ebé maka hamosu no deskarga husi aparellu.

Laiha evidénsia kona-ba kompromisu hosi host sira-ne'e. Maibé, rejistu sira husi host gateway asesu nian hatudu evidénsia interasaun signifikativu ho enderesu IP ne'ebé koñesidu malisiozu. Iha posibilidade katak ida-ne'e reflete atividade ne'ebé akontese iha host ida-ne'e, ka koneksaun rede nian ho infraestrutura atór ameasa \ ne'ebé alkanse host ida-ne'e. Natureza husi atividade ida-ne'e labele determina uza evidénsia ne'ebé disponivel maibé indika katak grupu ne'e buka atu muda lateralmente iha organizasaun nia rede (TA0008).

Host internu

ASD nia ACSC investiga dadus limitadu sira husi segmentu rede organizasaun internu nian. Atividade malisiozu tentativa ka susesu ne'e koñese katak fó impaktu ba segmentu rede organizasaun internu nian inklui asesu atór nian ba artefaktu sira ne'ebé relasiona ho VDI, hamoos servidór SQL internu ida (T1505.001), no tráfiku ne'ebé labele esplika mak observadu sai husi enderesu IP malisiozu ne'ebé koñesidu liuhusi portaun asesu ba aparellu (TA0011).

Uza sira nia asesu ba aparellu ne'ebé kometidu, grupu halibur naran uzuáriu jenuínu sira, senha sira (T1003), no valór token MFA nian (T1111). Grupu ne'e mós halibur JSON Web Tokens (JWTs) (T1528), ne'ebé artefaktu autentikasaun ida mak uza hodi kria sesaun login desktop virtuál. Atór bele uza sira-ne'e atu kria ka hijack sesaun desktop virtuál sira (T1563.002) no asesu ba segmentu rede organizasaun internu nian hanesan uzuáriu lejítimu (T1078).

Atór ne'e mós uza asesu ba aparellu ne'ebé komprometidu hodi hasai servidór SQL (T1505.001), ne'ebé hela iha rede internu organizasaun nian. Iha posibilidade katak atór ne'e iha asesu ba dadus ida-ne'e.

Evidénsia ne'ebé disponivel husi aparellu portaun asesu hatudu katak tráfiku rede nian akontese liuhusi ka ba dispositivu ida-ne'e husi enderesu IP malisiozu ne'ebé koñesidu. Hanesan deskreve ona iha leten, ida-ne'e bele indika katak atór sibernétiku malisiozu sira fó impaktu ka utiliza dispositivu ida-ne'e, ho potensiál atu muda ba rede internu.

Liña tempu investigasaun

Lista iha kraik fornese liña tempu ida kona-ba atividade xave sira ne'ebé deskobre durante investigasaun.

Oras	Eventu
Abril 2022	Enderesu IP malisiozu ne'ebé koñesidu halo interasaun ho host gateway asesu HOST7. Natureza husi interasaun ne'e labele determina.
Abril 2022	Host hotu-hotu, HOST1, HOST2 no HOST3, hetan kompromisu husi atór malisiozu ida ka atór sira, no web shell aloka iha host sira. Ficheiru rejistu ida kria ka modifika ona iha HOST2. Ficheiru ida-ne'e kontein materiál kredensiál ne'ebé provavelmente kaptura husi atór malisiozu ida. Ficheiru /etc/security/opasswd no /etc/shadow hetan modifikasaun iha HOST1 no HOST3, indika katak senha sira altera ona. Evidénsia ne'ebé disponivel iha HOST1 sujere katak senha ba uzuáriu 'sshuser' altera ona.
Abril 2022	HOST2 taka ona husi organizasaun. Web shell adisionál (T1505.003) kria ona iha HOST1 no HOST3. HOST1 esperiénsia tentativa forsa brutu SSH husi HOST3. Ficheiru rejistu ida hetan modifikasaun (T1070) iha HOST3. Ficheiru ida-ne'e kontein materiál kredensiál (T1078) ne'ebé provavelmente kaptura husi atór malisiozu ida. JWT sira hetan kaptura (T1528) no hasai ba ficheiru ida iha HOST3. HOST3 taka ona husi organizasaun. Atividade hotu-hotu hafoin tempu ida-ne'e akontese iha HOST1.
Abril 2022	Web shell adisionál kria ona iha HOST1 (T1505.003). JWT sira hetan kaptura no hasai ba ficheiru ida iha HOST1.
Abril 2022	Web shell adisionál sira kria iha HOST1 (T1505.003), no enderesu IP malisiozu ne'ebé koñesidu halo interasaun ho host (TA0011). Enderesu IP malisiozu ida ne'ebé koñesidu ona halo interasaun ho host gateway asesu HOST7.
Maiu 2022	Enderesu IP malisiozu ne'ebé koñesidu halo interasaun ho host gateway asesu HOST7 (TA0011). Eventu autentikasaun ida ba uzuáriu ida liga ba enderesu IP malisiozu ne'ebé koñesidu iha rejistu iha HOST1. Web shell adisionál ida mak kria iha host ida-ne'e (T1505.003).
Maiu 2022	Skript ida iha HOST1 hetan modifikasaun husi atór ida (T1543). Script ida ne'e kontein funsionalidade ne'ebé maka sei hasai dadus husi servidór SQL internu.
Maiu 2022	Ficheiru rejistu adisionál ida iha HOST1 hetan modifikasaun ikus liu (T1070). Ficheiru ida-ne'e kontein par sira naran uzuáriu no senha ba rede organizasaun nian, ne'ebé mak fiar katak lejítimu (T1078).
Maiu 2022	Ficheiru rejistu adisionál ida hetan modifikasaun ikus liu (T1070). Ficheiru ida-ne'e kontein JWT sira ne'ebé halibur husi HOST1.
Maiu 2022	Web shell adisionál kria ona iha HOST1 (T1505.003). Iha data ne'e, organizasaun ne'e relata deskoberta web shell ida ho data kriasaun iha Abril 2022 ba ASD nia ACSC
Maiu 2022	Skript lubuk ida maka kria ona iha HOST1, inklui ida ho naran Log4jHotPatch.jar.
Maiu 2022	Komandu iptables-save uza hodi aumenta porta rua ne'ebé nakloke ba host gateway asesu nian. Porta sira ne'e mak 9998 no 9999 (T1572).

Tátika atór nian no téknika sira

Destaka iha kraik ne'e mak tátika no téknika oioin ne'ebé identifika durante investigasaun.

Asesu Inisiál

T1190 Esplora Aplikasaun Konekta Públiku

Grupu ne'e provavelmente esplora RCE, eskalasaun priviléjiu, no vulnerabilidade bypass autentikasaun nian iha produtu jestaun asesu remotu no jestaun identidade nian hodi hetan asesu inisiál ba rede.

Métodu asesu inisiál ida-ne'e konsidera hanesan provável liu tanba tuirmai:

- Servidór ne'e vulnerável ba CVE sira-ne'e iha tempu ne'ebá;
- Tentativa atu esplora vulnerabilidade sira-ne'e husi infraestrutura atór koñesidu; no
- Atividade malisiozu internu dahuluk ne'ebé koñesidu akontese lakleur hafoin tentativa esplorasaun sira ne'ebé halo ona.

Ezekusaun

T1059.004 Intérprete Komandu no Scripting: Unix Shell

Grupu ne'ebé esplora ho susesu vulnerabilidade sira iha leten karik bele hala'o komandu sira iha Unix shell mak disponivel iha aparellu ne'ebé afetadu. Detallu kompletu sira kona-ba komandu ne'ebé realiza ho atór sira labele fornese tanba sira la rejistu husi aparellu.

Persisténsia

T1505.003 Komponente Software Servidór: Web Shell

Atór sira koloka web shell hirak iha aparellu ne'ebé afetadu. Iha posibilidade katak atór distintu oioin koloka web shell, maibé ladun barak atór mak kondutu atividade uza web shell ne'e. Web shell sira sei permite ezekusaun komandu arbitráriu husi atór iha aparellu ne'ebé komprometidu.

Eskalasaun Priviléjiu

T1068 Esplorasaun ba Eskalasaun Priviléjiu

Evidénsia ne'ebé disponivel la deskreve nivel priviléjiu mak hetan husi atór sira. Maibé, uza web shells, atór sira sei atinji ona nivel priviléjiu ida ne'ebé komparavel ho servidór web iha aparellu komprometidu. Vulnerabilidade sira ne'e fiar katak prezente iha aparellu ne'ebé komprometidu sei permite atór sira atu hetan priviléjiu abut nian.

Asesu Kredensial

T1056.003 Kaptura Entrada: Kaptura Portál Web

Evidénsia kona-ba aparellu ne'ebé komprometidu hatudu katak atór ne'e kaptura ona par senha naran uzuáriu atus resin, iha tekstu klaru, ne'ebé fiar katak lejítimu. Iha posibilidade katak sira-ne'e kaptura uza modifikasaun ruma ba prosesu autentikasaun jenuínu ne'ebé hasai kredensial sira ba ficheiru ida.

T1111 Intersepsaun Autentikasaun Multi-Fatór

Atór ne'e mós kaptura valór husi token MFA sira ne'ebé koresponde ba login lejítimu sira. Sira ne'e provavelmente kaptura liuhusi modifikasaun prosesu autentikasaun jenuínu hodi hasai valór sira-ne'e ba ficheiru ida. Laiha evidénsia kona-ba kompromisu husi 'servidór segredu' ne'ebé rai valór úniku sira ne'ebé fornese ba seguransa husi token MFA sira.

T1040 Sniffing Rede

Atór ne'e fiar katak kaptura ona JWT sira ho kaptura tráfiku HTTP iha aparellu ne'ebé komprometidu. Iha evidénsia katak tcpdump utilidade nian ezekuta ona iha aparellu ne'ebé komprometidu, ne'ebé bele sai hanesan oinsá atór kaptura JWT sira-ne'e.

T1539 Nauk Web Session Cookie

Hanesan deskreve ona iha leten, atór kaptura JWT sira, ne'ebé maka análogu ho cookies sesaun web nian. Sira ne'e bele uza fali ho atór hodi estabelese asesu liután.

Deskobre

T1046 Deskobre Servisu Rede

Iha evidénsia katak utilidade dijitalizasaun rede nmap ezekuta ona iha aparellu ne'ebé komprometidu hodi dijitaliza aparellu sira seluk iha segmentu rede hanesan. Ida-ne'e provavelmente uza ho atór hodi deskobre servisu rede asesível seluk ne'ebé bele aprezenta oportunidade sira ba movimentu laterál.

Kollesaun

Evidénsia ne'ebé disponivel la revela oinsá atór sira halibur dadus ka saida loos maka halibur husi aparellu ne'ebé komprometidu ka hosi sistema sira seluk. Maibé, iha posibilidade katak atór sira iha asesu ba ficheiru hotu-hotu iha aparellu ne'ebé komprometidu, inklui kredensial sira ne'ebé kaptura (T1003), valór token MFA (T1111), no JWT sira ne'ebé deskreve iha leten.

Komandu no Kontrolu

T1071.001 Protokolu Kamada Aplikasaun: Protokolu Web

Atór sira uza web shell ba komandu no kontrolu. Komandu web shell nian sei pasa liuhusi HTTPS uza servidór web ne'ebé eziste iha aparellu (T1572).

T1001.003 Obfuskasaun Dadus: Imitasaun Protokolu

Atór sira uza dispositivu sira ne'ebé komprometidu hanesan pontu lansamentu ba atake sira ne'ebé dezeña atu kahur ho tráfiku lejítimu.

Rekomendasaun sira ba deteksaun no mitigasaun

ASD nia ACSC rekomenda maka'as atu implementa ASD Essential Eight Kontrolu sira no asosiadu Estratéjia sira atu Mitiga Insidente sira Seguransa Sibernétiku nian. Iha kraik ne'e rekomendasaun sira ba asaun seguransa rede nian ne'ebé tenke foti atu detekta no prevene intrusaun sira husi APT40, tuir fali ho mitigasaun espesífiku sira ba TTP xave haat ne'ebé rezumu iha Tabela 1.

Deteksaun

Ficheiru balun ne'ebé identifika iha leten tama ba lokasaun sira hanesan C:\Users\Public* no C:\Windows\Temp*. Lokasaun sira-ne'e bele sai fatin konveniente atu hakerek dadus tanba sira normalmente bele hakerek iha mundu tomak, katak, konta uzuáriu hotu-hotu ne'ebé rejista iha Windows iha asesu ba diretóriu sira-ne'e no sira-nia subdiretóriu sira. Dala barak, kualkér uzuáriu bele asesu ba ficheiru sira-ne'e, hodi permite oportunidade sira ba movimentu laterál, evazaun defeza nian, ezekusaun ho priviléjiu minimu no preparasaun ba eksfiltrasaun.

Regra Sigma sira tuirmai buka ezekusaun husi lokasaun sira ne'ebé suspeitu hanesan indikadór ida husi atividade anómalu. Iha kazu hotu-hotu, presiza investigasaun tuirmai atu konfirma atividade no atribuisaun malisiozu.

Titulu: Ezekusaun Mundiál ne'ebé bele hakerek - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Deskrisaun Detekta ezekusaun prosesu husi C:\Windows\Temp.

Fundu:

Regra ida-ne'e buka espesifikamente ba ezekusaun husi C:\Windows\Temp*. Temp uza luan liutan husi aplikasaun benigna sira no nune'e indikadór malisiozu ida ho konfiansa minimu duké ezekusaun hosi subdiretóriu sira seluk ne'ebé bele hakerek iha C:\Windows.

Hasai aplikasaun sira ne'ebé ezekuta hosi uzuáriu sira nia SYSTEM ka NETWORK SERVICE nian hamenus substansialmente kuantidade atividade benigna ne'ebé hili husi regra ida-ne'e.

Ida-ne'e signifika katak regra bele liu deit ezekusaun malisiozu sira iha nivel priviléjiu ne'ebé aas liu maibé rekomenda atu uza regra sira seluk hodi determina se uzuáriu ida tenta atu levanta priviléjiu sira ba SISTEMA.

Investigasaun:

1. Ezamina informasaun ne'ebé asosiadu diretamente ho ezekusaun ficheiru ida-ne'e, hanesan kontestu uzuáriu nian, nivel integridade ezekusaun nian, atividade akompañamentu imediatu no imajen sira ne'ebé karrega husi ficheiru.
2. Investiga prosesu kontestuál, rede, ficheiru no dadus apoiu sira seluk iha host hodi ajuda halo avaliasaun ida kona-ba karik atividade ne'e malisiozu.
3. Karik nesesáriu tenta atu halibur kópia ida hosi ficheiru ba enjeñaria reversa hodi determina karik ida-ne'e lejítimu.

Referénsia:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Autor: ASD nia ACSC

Data: 2024/06/19

Estatutu: esperimentál

Tags:

- tlp.green
- classification.au.official
- attack.execution

Rekursu rejistu:

kategoria: prosesu_kriasaun
produtu: windows

Deteksaun:

```
temp:
    Image|startswith: 'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase: 'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
system_user:
    Uzuáriu:
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

kondisaun: temp no la'e (common_temp_path ka system_user ka dismhost ka known_parent)

Pozitivu falsu sira:

- Aplikasaun auditoria Allowlist nian hetan ona observasaun hala'o ezekutável sira husi Temp
- Temp sei lejítimu kontein array ida husi aplikasaun konfigurasaun no lansadór sira, nune'e sei vale atu konsidera oinsá prevalente hahalok ida-ne'e iha rede ida ne'ebé monitoriza (no karik ida-ne'e bele tama iha allowlisted ka lae) molok implementa regra ida-ne'e.

Nivel: ki'ik

Titulu: Ezekusaun Mundiál ne'ebé bele hakerek - La'ós-Subdiretóriu Sistema Temporáriu

ID 5b187157-e892-4fc9-84fc-aa48aff9f997

Deskrisaun Detekta ezekusaun prosesu husi lokasaun bele hakerek iha mundu iha subdiretóriu husi lokasaun instalasaun Windows OS.

Fundu:

Regra ida-ne'e espesifikamente haree ba ezekusaun husi diretóriu sira ne'ebé bele hakerek iha C:\ no partikularmente C:\Windows*, ho eksesaun ba C:\Windows\Temp (ne'ebé maka uza barak liu ho aplikasaun benigna sira no nune'e indikadór malisiozu ho konfiansa minimu liu).

Pasta AppData sira sei esklui karik ficheiru ida hala'o hanesan SYSTEM - ida-ne'e maka maneira benignu ida iha ne'ebé ficheiru aplikasaun temporáriu barak maka ezekuta.

Hafoin kompleta liña baze rede inisiál no identifika ezekusaun benignu sira ne'ebé koñesidu husi fatin sira-ne'e, regra ida-ne'e ladún funsiona.

Investigasaun:

1. Ezamina informasaun ne'ebé asosiadu diretamente ho ezekusaun ficheiru ida-ne'e, hanesan kontestu uzuáriu nian, nivel integridade ezekusaun nian, atividade akompañamentu imediatu no imajen sira ne'ebé karrega husi ficheiru.
2. Investiga prosesu kontestuál, rede, ficheiru no dadus apoiu sira seluk iha host hodi ajuda halo avaliasaun ida kona-ba karik atividade ne'e malisiozu.
3. Karik nesesáriu tenta atu halibur kópia ida hosi ficheiru ba enjeñaria reversa hodi determina karik ida-ne'e lejítimu.

Referénsia:

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Autor: ASD nia ACSC

Data: 2024/06/19

Estatutu: esperimentál

Tags:

- tlp.green
- classification.au.official
- attack.execution

Rekursu rejistu:

kategoria: prosesu_kriasaun

produtu: windows

Deteksaun:

writable_path:

Imajen|kontein:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'

- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Imajen|kontein: '\\AppData\\'
Uzuáriu: 'SYSTEM'

kondisaun: writable_path no la'ós appdata

Pozitivu falsu sira:

Aplikasaun auditoria Allowlist nian hetan ona observasaun hala'o ezekutável sira hosi diretóriu sira-ne'e

Ida-ne'e plausivel katak script sira no ferramenta administrativu sira ne'ebé uza iha ambiente ne'ebé monitorizadu bele aloka iha diretóriu sira-ne'e ida no tenke aborda iha baze kazu-ba-kazu.

Nivel: aas

Titulu: Ezekusaun Mundiál ne'ebé bele hakerek - Uzuáriu sira

ID 6dda3843-182a-4214-9263-925a80b4c634

Deskrisaun Detekta ezekusaun prosesu husi C:\Users\Public* no pasta sira seluk ne'ebé bele hakerek iha mundu iha Uzuáriu nia laran.

Fundu:

Pasta AppData sira sei esklui karik ficheiru ida hala'o hanesan SYSTEM - ida-ne'e maka maneira benignu ida iha ne'ebé ficheiru aplikasaun temporáriu barak maka ezekuta.

Investigasaun:

1. Ezamina informasaun ne'ebé asosiadu diretamente ho ezekusaun ficheiru ida-ne'e, hanesan kontestu uzuáriu nian, nivel integridade ezekusaun nian, atividade akompañamentu imediatu no imajen sira ne'ebé karrega husi ficheiru.
2. Investiga prosesu kontestuál, rede, ficheiru no dadus apoiu sira seluk iha host hodi ajuda halo avaliasaun ida kona-ba karik atividade ne'e malisiozu.
3. Karik nesesáriu tenta atu halibur kópia ida hosi ficheiru ba enjeñaria reversa hodi determina karik ida-ne'e lejítimu.

Referénsia:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Autor: ASD nia ACSC

Data: 2024/06/19

Estatutu: esperimentál

Tags:

- tlp.green
- classification.au.official
- attack.execution

Rekursu rejistu:

kategoria: prosesu_kriasaun
produtu: windows

Deteksaun:

uzuáriu sira

Imajen|kontein:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:

Imajen|kontein: '\\AppData\\'
Uzuáriu: 'SYSTEM'

kondisaun: uzuáriu sira no la'ós appdata

Pozitivu falsu sira:

- Ida-ne'e plausivel katak script sira no ferramenta administrativu sira mak uza iha ambiente ne'ebé monitorizadu bele aloka iha Públiku ka subdiretóriu ida no tenke aborda tuir kazu ida-idak.

Nivel: médiu

Mitigasaun sira

Logging

Durante investigasaun ACSC ASD nian, kestaun komún ida ne'ebé hamenus efikásia no velosidade esforsu investigasaun nian maka falta informasaun rejistu komprensivu no istóriku iha área lubuk ida inklui rejistu pedidu servidór web nian, rejistu eventu Windows nian no rejistu proxy internet nian.

ASD nia ACSC rekomenda halo revizaun no implementa sira nia orientasaun kona-ba Windows Event Logging and Forwarding inklui ficheiru konfigurasaun no skript sira iha Windows Event Logging Repository no Information Security Manual nia Orientasaun ba Sistema Monitoring atu inklui rejistu sentralizadu a sira no retein rejistu sira ba períodu ida ne'ebé adekuadu.

Jestaun patch

Patch lalais dispositivu no servisu sira hotu ne'ebé maka iha internet, inklui servidór web sira, aplikasaun web sira, no portaun asesu remotu sira. Konsidera implementa sistema jestaun patch sentralizadu ida hodi automatiza no aselera prosesu. ASD nia ACSC rekomenda implementasaun husi ISM nia Orientasaun ba Jestaun Sistema, espesifikamente, kontrolu Sistema Patching nian bainhira aplikavel.

Maioria esplorasaun sira ne'ebé uza ho atór ne'e koñesidu ba públiku no iha patch ka mitigasaun sira ne'ebé disponivel. Organizasaun sira tenke asegura katak patch seguransa ka mitigasaun sira ne'e aplika ba infraestrutura ne'ebé hasoru internet iha oras 48 nia laran, no bainhira posivel, uza versaun atualizadu husi software no sistema operasaun sira.

Segmentasaun rede

Segmentasaun rede nian bele halo difisil liu ba adversáriu sira atu lokaliza no hetan asesu ba dadus sensitivu organizasaun nian. Segmenta rede sira hodi limita ka blokeia movimentu laterál ho nega tráfiku entre komputadór sira só deit bainhira presija. Servidór importante sira hanesan Active Directory no Servidór autentikasaun sira seluk tenke bele administra de'it husi númeru limitadu servidór intermediáriu sira ka 'servidór jump'. Servidór sira ne'e tenke monitoriza ho metin, asegura ho di'ak no limita uzuáriu no dispozitivu ida ne'ebé maka bele konekta ba sira.

La haree ba instánsia sira ne'ebé identifika ona iha ne'ebé movimentu laterál hetan prevensaun, segmentasaun rede adisionál bele limita liután kuantidade dadus ne'ebé atór sira bele asesu no ekstrai.

Mitigasaun adisionál sira

Ajénsia autoria mós rekomenda mitigasaun sira tuirmai atu kombate APT40 no ema seluk mak uza TTP sira iha kraik.

- Dezativa servisu rede, porta no protokolu sira ne'ebé la uza ka la nesesáriu.
- Uza firewall aplikasaun Web (WAF) ne'ebé sintonizadu ho di'ak atu proteje servidór web no aplikasaun sira.
- Haforsa priviléjiu minimu liu hodi limita asesu ba servidór sira, partilla ficheiru sira, no rekursu sira seluk.
- Uza autentikasaun multi-fatór (MFA) no konta servisu jeride sira hodi halo kredensial sira sai araska liutan atu sobu no uza fali. MFA tenke aplika ba servisu asesu remotu hotu-hotu ne'ebé asesivel ba internet, inklui:
  - Email bazeia ba web no cloud
  - Plataforma kolaborasaun
  - Ligasaun rede privadu virtuál
  - Servisu desktop remotu
- Substitui ekipamentu sira ne'ebé maka laiha ona vida.

Tabela 1. Estratéjia/Tékniku Mitigasaun

TTP	Estratéjia Mitigasaun Ualu ne'ebé Esensiál	Kontrolu ISM
Asesu Inisiál T1190 Esplorasaun ba Aplikasaun ne'ebé Hasoru ba Públiku	Patch aplikasaun sira Patch sistema operasaun sira Autentikasaun Multi-Fatór Kontrolu Aplikasaun	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Ezekusaun T1059 Komandu no Intérprete Scripting	Kontrolu Aplikasaun Restrinje makro Microsoft Office nian Restrinje priviléjiu administrativu sira	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Persisténsia T1505.003 Komponente Software Servidór: Web Shell	Kontrolu Aplikasaun Restrinje priviléjiu administrativu sira	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Asesu Inisiál / Eskalasaun Priviléjiu / Persisténsia T1078 Konta sira ne'ebé válidu	Patch sistema operasaun sira Autentikasaun Multi-Fatór Restrinje priviléjiu administrativu sira Kontrolu Aplikasaun Protesuan ba Aplikasaun Uzuáriu	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

Ba konsellu deteksaun no mitigasaun jerál adisionál, favór konsulta seksaun sira Mitigasaun no Deteksaun iha pájina web téknika MITRE ATT&CK nian ba téknika ida-idak ne'ebé identifika iha rezumu MITRE ATT&CK nian iha avizu ida-ne'e nia rohan.

Desaprovadór

Informasaun iha relatóriu ida ne'e fornese hela "loloos" ba objetivu informasional deit. Ajénsia sira ne'ebé halo dokumentu ida ne'e la fó apoiu ba entidádé komersiál, produtu, kompañia, ka servisu sira, inklui entidádé, produtu, ka servisu sira ne'ebé iha link iha dokumentu laran ida ne'e. Referénsia ruma ba entidade komersiál espesífiku sira, produtu sira, prosesu sira, ka servisu sira ho marka servisu, marka komersiál, fabrikante, ka seluk tan, la konstitui ka implika endosu, rekomendasaun, ka favoresementu hosi ajénsia autória sira.

Dokumentu ida-ne'e markadu ho TLP:CLEAR. Divulgasaun la limitadu. Rekursu sira bele uza TLP:CLEAR kuandu informasaun iha risku mínimu ka laiha risku previzível ba utilizasaun sala, tuir regra no prosedimentu sira ne'ebé aplikavel ba divulgasaun públika. Sujeitu ba regra padraun direitu autór nian, informasaun TLP:CLEAR bele partilla sein restrisaun. Atu hetan informasaun liután kona-ba Protokolu Trafiku, haree ba cisa.gov/tlp

MITRE ATT&CK – Komérsiu istóriku ne'ebé interesse APT40

Rekoñesimentu (TA0043)	
Peskiza Website Vitima nian (T1594)	Halibur Informasaun Identidade Vítima nian: Kredensial (T1589.001)
Varimentu Ativu: Varimentu Vulnerabilidade (T1595.002)	Halibur Informasaun Host Vítima nian (T1592)
Buka Peskiza Website/Domíniu: Motora Peskiza sira (T1593.002)	Halibur Informasaun Rede Vítima nian: Propriedade Domíniu nian (T1590.001)
Halibur Informasaun Identidade Vítima nian: Enderesu Email (T1589.002)	

Dezenvolvimentu Rekursu (TA0042)	
Adkuiri infraestrutura: Domíniu (T1583.001)	Adkuiri Infraestruturas (T1583)
Adkuiri infraestrutura: Servidór DNS (T1583.002)	Konta Komprometidu (T1586)
Dezenvolve Kapasidade: Sertifikadu Asinatura Kódigu (T1587.002)	Infraestrutura Komprometidu (T1584)
Dezenvolve Kapasidade: Sertifikadu Dijitál (T1587.003)	Dezenvolve Kapasidade: Malware (T1587.001)
Obten Kapasidade sira: Sertifikadu Asinatura Kódigu (T1588.003)	Estabelese Konta sira: Konta Cloud (T1585.003)
Infraestrutura Komprometidu: Dispositivu Rede sira (T1584.008)	Obten Kapasidade sira: Sertifikadu Dijitál (T1588.004)

Asesu Inisiál (TA0001)	
Konta sira ne'ebé válidu (T1078)	Phishing (T1566)
Konta sira ne'ebé válidu: Konta Padraun sira (T1078.001)	Phishing: Aneksu Spearphishing (T1566.001)
Konta sira ne'ebé válidu: Konta Domíniu sira (T1078.002)	Phishing: Ligasaun Spearphishing (T1566.002)
Servisu Remotu Esternu (T1133)	Esplora Aplikasaun ne'ebé Hasoru Públiku (T1190)
Kompromisu Drive-by (T1189)	

Ezekusaun (TA0002)	
Instrumentasaun Jestaun Window (T1047)	Intérprete Komandu no Scripting: Python (T1059.006)
Tarefa/Serbisu ne'ebé Ajendadu: At (T1053.002)	Intérprete Komandu no Scripting: JavaScript (T1059.007)
Tarefa/Serbisu ne'ebé Ajendadu: Tarefa Ajendadu (T1053.005)	API Nativa (T1106)
Intérprete Komandu no Scripting (T1059)	Komunikasaun Inter-Prosesu (T1559)
Intérprete Komandu no Scripting: Shell Komandu Windows (T1059.003)	Servisu Sistema: Ezekusaun Servisu (T1569.002)
Intérprete Komandu no Scripting: PowerShell (T1059.001)	Esplorasaun ba Ezekusaun Kliente (T1203)
Intérprete Komandu no Scripting: Visual Basic (T1059.005)	Ezekusaun Uzadór: Ficheiru Malisiozu (T1204.002)
Intérprete Komandu no Scripting: Unix Shell (T1059.004)	Intérprete Komandu no Scripting: Apple Script (T1059.002)
Tarefa/Serbisu ne'ebé Ajendadu: Cron (T1053.003)	Ferramenta sira ba Implementasaun Software nian (T1072)

Persisténsia (TA0003)	
Konta sira ne'ebé válidu (T1078)	Komponente Software Servidór: Web Shell (T1505.003)
Hahú Aplikasaun Eskritóriu: Makro Modelu Eskritóriu nian (T1137.001)	Kria ka Modifika Prosesu Sistema: Servisu Windows (T1543.003)
Tarefa/Serbisu ne'ebé Ajendadu: At (T1053.002)	Ezekusaun Autostart Boot ka Logon: Rejistu Run Keys / Startup Folder (T1547.001)
Tarefa/Serbisu ne'ebé Ajendadu: Tarefa Ajendadu (T1053.005)	Ezekusaun Autostart Boot ka Logon: Modifikasaun Shortcut (T1547.009)
Servisu Remotu Esternu (T1133)	Fluxu Ezekusaun Hijack: Sekuestru Ordem Peskiza DLL (T1574.001)
Tarefa/Serbisu ne'ebé Ajendadu: Cron (T1053.003)	Fluxu Ezekusaun Hijack: Karegamentu lateral DLL (T1574.002)
Manipulasaun Konta (T1098)	Konta sira ne'ebé válidu: Konta Cloud (T1078.004)
Konta sira ne'ebé válidu: Konta Domíniu sira (T1078.002)	

Eskalasaun Priviléjiu (TA0004)	
Tarefa/Serbisu ne'ebé Ajendadu: At (T1053.002)	Kria ka Modifika Prosesu Sistema: Servisu Windows (T1543.003)
Tarefa/Serbisu ne'ebé Ajendadu: Tarefa Ajendadu (T1053.005)	Ezekusaun Autostart Boot ka Logon: Rejistu Run Keys / Startup Folder (T1547.001)
Prosesu Injesaun: Hijacking Ezekusaun Thread (T1055.003)	Ezekusaun Autostart Boot ka Logon: Modifikasaun Shortcut (T1547.009)
Prosesu Injesaun: Prosesu Hollowing (T1055.012)	Fluxu Ezekusaun Hijack: Sekuestru Ordem Peskiza DLL (T1574.001)

Eskalasaun Priviléjiu (TA0004)	
Konta sira ne'ebé válidu: Konta Domíniu sira (T1078.002)	Esplorasaun ba Eskalasaun Priviléjiu (T1068)
Manipulasaun Asesu Token: Nauk/Imitasaun ba Token (T1134.001)	Ezekusaun ne'ebé hamosu tanba Eventu: Modifikasaun Konfigurasaun Unix Shell (T1546.004)
Prosesu Injesaun: Injesaun Biblioteka Ligasaun Dinámiku (T1055.001)	Konta sira ne'ebé válidu: Konta Domíniu sira (T1078.002)
Konta sira ne'ebé válidu: Konta Lokál sira (T1078.003)	

Evazaun Defeza (TA0005)	
Rootkit (T1014)	Ezekusaun Komandu Indiretu (T1202)
Arkivu ka Informasaun ne'ebé La Klaru (T1027)	Ezekusaun Proxy Sistema Binário: Mshta (T1218.005)
Ficheiru ka Informasaun ne'ebé disimula Pakote Software (T1027.002)	Ezekusaun Proxy Sistema Binário: Regsvr32 (T1218.010)
Ficheiru ka Informasaun ne'ebé disimula Steganografia (T1027.003)	Subverte Kontrolu Konfiansa: Asinatura Kódigu (T1553.002)
Ficheiru ka Informasaun ne'ebé disimula Kompila Depois Entrega (T1027.004)	Modifikasaun ba Lisensa Ficheiru no Diretóriu: Modifikasaun Lisensa Ficheiru no Diretóriu Linux no Mac (T1222.002)
Disimula: Koresponde ho Naran ka Fatin Lejítimu (T1036.005)	Virtualizasaun/Evasaun Sandbox: Verifika Sistema (T1497.001)
Prosesu Injesaun: Hijacking Ezekusaun Thread (T1055.003)	Disimula (T1036)
Karegamentu Kódigu Refletivu (T1620)	Bronkas Defeza: Dezativa ka Modifika Sistema Firewall (T1562.004)
Prosesu Injesaun: Prosesu Hollowing (T1055.012)	Subar Artefaktu: Ficheiru no Diretóriu sira ne'ebé subar (T1564.001)
Hasai Indikadór: Eliminasaun Ficheiru (T1070.004)	Subar Artefaktu: Window ne'ebé Subar (T1564.003)
Hasai Indikadór: Timestomp (T1070.006)	Fluxu Ezekusaun Hijack: Sekuestru Ordem Peskiza DLL (T1574.001)
Hasai Indikadór: Hamós Rejistu Eventu Windows sira (T1070.001)	Fluxu Ezekusaun Hijack: Karegamentu lateral DLL (T1574.002)
Modifika Rejistu (T1112)	Servisu Web (T1102)
Hasai/Dekodifika Ficheiru ka Informasaun (T1140)	Disimula: Tarefa ka Servisu Disimuladu (T1036.004)
Bronkas Defeza (T1562)	

Asesu Kredensial (TA0006)	
Dumping Kredensial OS: Memória LSASS (T1003.001)	Kredensial La Seguru: Kredensial iha Ficheiru (T1552.001)
Dumping Kredensial OS: NTDS (T1003.003)	Forsa Brutu: Adivinha Senha (T1110.001)
Sniffing Rede (T1040)	Autentikasaun Forsadu (T1187)

Asesu Kredensial (TA0006)	
Kredensial husi Loja Senha: Porta-xave (T1555.001)	Nauk ka falsifika bileti Kerberos nian: Kerberoasting (T1558.003)
Kaptura Entrada: Rejistu Tekladu (T1056.001)	Intersepsaun Autentikasaun Multi-Fatór (T1111)
Nauk Cookie Sesaun Web nian (T1539)	Nauk Token Asesu ba Aplikasaun (T1528)
Esplorasaun ba Asesu Kredensial (T1212)	Forsa Brutu: Bronkas Senha (T1110.002)
Kaptura Entrada: Kaptura Portal Web (T1056.003)	Dumping Kredensial OS: DCSync (T1003.006)
Kredensial husi Loja Senha sira (T1555)	Kredensial husi Loja Senha: Kredensial husi Web Browser sira (T1555.003)

Deskoberta (TA0007)	
Deskoberta Servisu Sistema (T1007)	Deskoberta Informasaun Sistema (T1082)
Deskoberta Window Aplikasaun (T1010)	Deskoberta Konta: Konta Lokal (T1087.001)
Rejistu Pergunta (T1012)	Deskoberta Informasaun Sistema, Téknika T1082 - Empreza | MITRE ATT&CK®
Deskoberta Ficheiru no diretóriu (T1083)	Deskoberta Tempu Sistema (T1124)
Deskoberta Servisu Rede (T1046)	Deskoberta Sistema-nain/Uzuáriu (T1033)
Deskoberta Sistema Remotu (T1018)	Deskoberta Konfiavel Domíniu (T1482)
Deskoberta Konta: Konta Email (T1087.003)	Deskoberta Konta: Konta Domíniu (T1087.002)
Deskoberta Koneksaun Rede Sistema (T1049)	Virtualizasaun/Evasaun Sandbox: Verifika Sistema (T1497.001)
Deskoberta Prosesu (T1057)	Deskoberta Software (T1518)
Deskoberta Grupu Permisaun: Grupu Domíniu (T1069.002)	Deskoberta Partilla Rede, Téknika T1135 - Empreza | MITRE ATT&CK®
Deskoberta Konfigurasaun Rede Sistema: Deskoberta Koneksaun Internet (T1016.001)	

Movimentu Lateral (TA0008)	
Servisu Remotu: Protokolu Desktop Remotu (T1021.001)	Servisu Remotu (T1021)
Servisu Remotu: Partilla Admin SMB/Windows (T1021.002)	Uza Material Autentikasaun Alternadu: Passa Bileti (T1550.003)
Servisu Remotu: Jerensiamentu Remotu Windows (T1021.006)	Tranfere Feramenta Lateral (T1570)

Kollesaun (TA0009)	
Dadus husi Sistema Lokal (T1005)	Dadus Rekollu Arkivu: Arkivu liuhusi Biblioteka (T1560.002)
Dadus husi Drive Partilla Rede (T1039)	Rekolla Email: Rekolla Email Remotu (T1114.002)

Kollesaun (TA0009)	
Kaptura Entrada: Rejistu Tekladu (T1056.001)	Dadus Clipboard (T1115)
Kollesaun Automatiku (T1119)	Dadus husi Repositóriu Informasaun (T1213)
Kaptura Entrada: Kaptura Portal Web (T1056.003)	Dadus Prezente: Dadus Prezente iha Lókasun Remotu (T1074.002)
Dadus Prezente: Dadus Prezente Lokal (T1074.001)	Dadus Rekollu Arkivu (T1560)
Rekolla Email (T1114)	

Eksfiltrasaun (TA0010)	
Eksfiltrasaun Liuhusi Kanal C2 (T1041)	Eksfiltrasaun Liuhis Protokolu Alternativu: Eksfiltrasaun Liuhusi Protokolu Naun-C2 Enkriptadu Asimétriku (T1048.002)
Eksfiltrasaun Liuhusi Protokolu Alternativu (T1048)	Eksfiltrasaun Liuhusi Servisu Web: Eksfiltrasaun ba Armazenamentu Cloud (T1567.002)

Komandu no Kontrolu (TA0011)	
Ofuskazaun Dadus: Imitasaun Protokolu (T1001.003)	Servisu Web: Resolvedór Dead Drop (T1102.001)
Porta Normalmente Utilizada (T1043)	Servisu Web: Comunicação Unidiresional (T1102.003)
Protokolu Kapa Aplikasaun: Protokolu Web (T1071.001)	Transferénsia Ferramenta Ingressu (T1105)
Protokolu Kapa Aplikasaun: Protokolu Transfere Ficheiru (T1071.002)	Proxy: Proxy Interna (T1090.001)
Proxy: Proxy Esterna (T1090.002)	Portu Naun-Padraun (T1571)
Proxy: Proxy Multi-hop (T1090.003)	Túnel Protokolu (T1572)
Servisu Web: Komunikasaun Bidiresional (T1102.002)	Kanal Enkriptadu (T1573)
Kanal Enkriptadu: Encriptasaun Asimétrika (T1573.002)	Transferénsia Ferramenta Ingressu (T1105)
Proxy, Téknika T1090 - Empreza | MITRE ATT&CK®	

Impaktu (TA0040)	
Para Servisu (T1489)	Hamós Disku (T1561)
Desliga/Reinisia Sistema (T1529)	Sequestru Rekursu (T1496)

Nota sira

Desaprovadór

Materiál iha guia ida ne'e hanesan natureza jeral no la bele konsidera nu'udar sujestaun legal ka depende ba asistênsia iha kondisaun partikulár ka situasaun emerjênsia. Iha kualkér asuntu importante, Ita tenke ba buka sujestaun profisional independente apropriadu mak relasiona ho Ita nia kondisaun rasik.

Commonwealth la aseita responsabilidade ka liabilidade ba kualkér defeitu, lakon ka despeza mak mosu nu'udar rezultadu husi konfiansa ba informasaun mak konteudu iha guia nia laran ida ne'e.

Ba informasaun liutan ka atu relata insidente seguransa sibernétika, kontaktu ami:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Númeru ne'e disponivel atu uza deit iha Austrália laran.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre