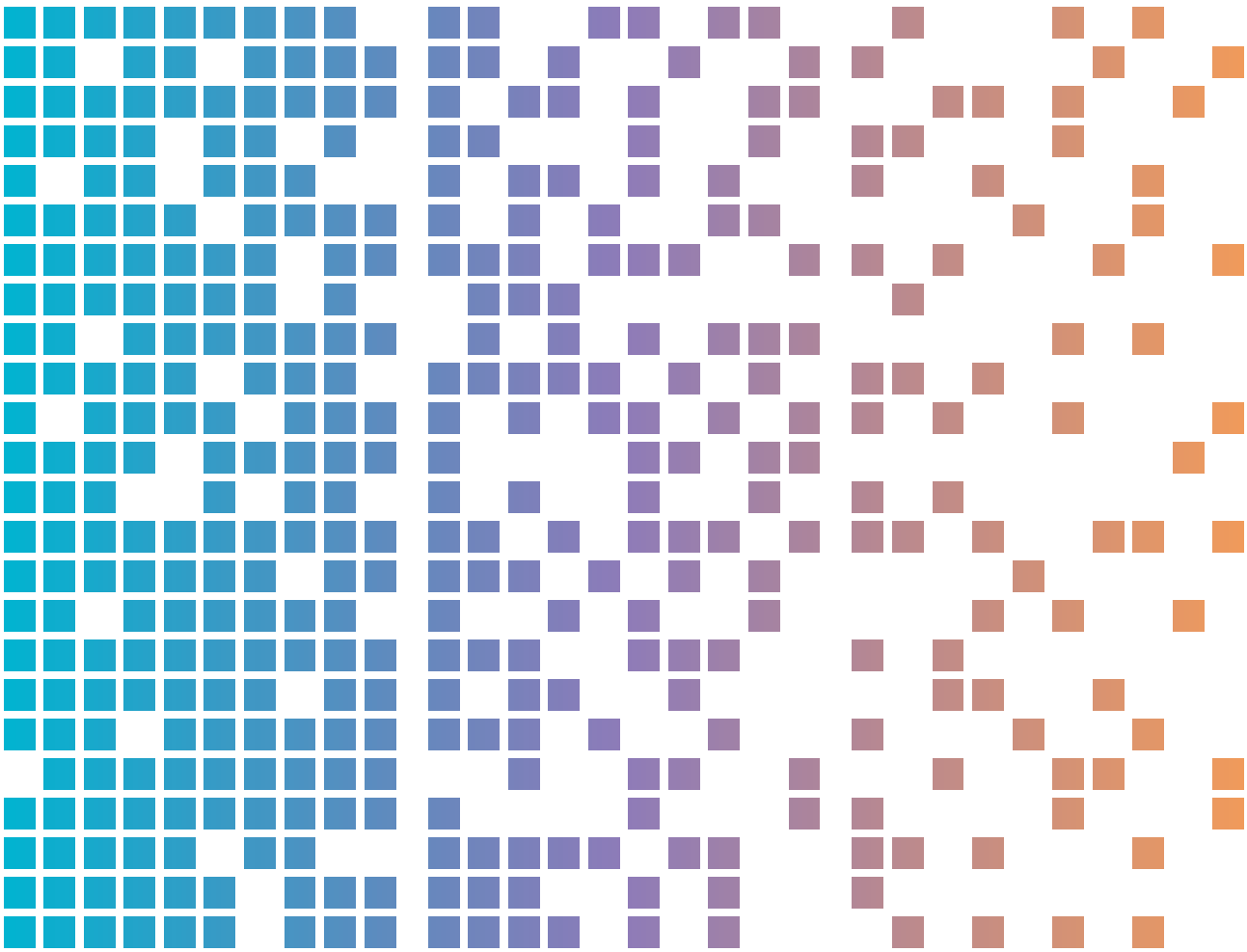
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Fasin blong stil kwaet: saebakriminal i yusum infomesen blong stilim malwea blong atakem ol bisnes netwok



Kompleksiti Konten
MODERET

Tebol blong konten

Konteks

Infomesen stila malwea i stilim ol aedentiti mo sistem infomesen we ol saebakriminal oli kasem, speseli blong kasem mane long hem. Infomsen stila oli bin stap lukluk long ol saebakraem atak we i go agensem sam oganaesesen mo sekta raonwol, we i tekem tu Australia. Pablikesen ia i provaedem ol rida wetem saeba gaedens long infomesen stila malwea, we i gat tret aktiviti mo mitigesen advaes blong ol oganaesesen mo ol employi blong olgeta.

Ki poen

- Infomesen stila malwea, we hemi info stila tu, i wan kaen malwea we oli disaenem blong kolektem infomesen long wan divaes blong viktim. Hemia i save gat yusa nem mo paswod, kredit kad ditel, kriptokarensi walet, lokol fael, mo braosa infomesen wetem ol kuki, yusa histri mo otofil fom ditel.
- Saebakriminal oli save pem mo yusum ol aedentiti we oli stilim we i go wetem ol akaon we oli wok tugeta blong kasem fes akses long ol divaes blong ol viktim bos, wokman blong olgeta mo ol nara entapraes sistem. Risal afta long aksen blong ol oganaesesen ia i save gat ransamwea, ekstosen, bisnis imel koperesen mo stil blong intelektuol propeti.
- Australian Signals Directorate's Australian Cyber Security Centre (ACSC blong ASD) i bin faenemaot koperet netwok brij we hem i stap insaed long ol employi blong aksesem ol wok risos aot long ol divaes koperesen blong yuwan. Long sam eksampol, saebakriminal i kasem impoten akses blong wok wetem ol netwok mo yusum ol aedentiti we oli stilim mo i stret. Investigesen blong yumi i soem se oltaem bigfala koperesen i kamaot afta ol saebabkriminal oli gat janis blong aksesem ol yusa akaon.
- Ol oganaesesen we oli helpem ol wokman, kontrakta, manejem seves provaeda o ol nara pat blong aksesem netwok fulwan, we oli gat Bring Your Own Device (BYOD) hadwea, oli nid blong save denja blong ol info stila mo protektem olgetawan long tret ia. Ol saebakriminal oli oganaesem info stila long ol divaes blong viktim wetem yus blong wan bigfala teknoloji, i gat tu fising imel, paeret sofwea daonlod, sej enjin optimaesesen (SEO) teknik, rabis advataesmen o rabis link we oli postem long sosol media platfom. Long jenerol, ol divaes we oli yusum tugeta long wok mo stamba tingting blong yuwan oli stap long risk blong infeksen tru long ol teknik ia folem fasin blong wan yusa mo ridius sekiuriti kontrol.
- Info stila i givim wan naes model blong ol saebakriminal blong kasem saebakraem aktiviti, speseli long ol saebakriminal entri-level mo olgeta we oli gat smol teknikol skil. Sam saebakriminal bae oli salem prodak blong info stila tru long wan Malware-as-a-Service (MaaS) stael program, mo jajem sabskripsen fi blong evri manis.

Bakgraon

Yus blong info stila tru long saebakriminal i wan tret blong sekiuriti mo gud blong oganaesesen blong ol man Austrelia. Info stila infeksen oltaem i stap olsem aktiviti blong oltaem long mein saeba sekiuriti insiden, olsem ol saebakriminal oli yusum olgeta blong hipimap ol yusa kridensol. Ol yusa kridensol ya, speseli olgeta we oli givim akses long intanet long ol ples blong seves o akaon we i gat janis, oli nao yusum blong save gat akses insaed long koperet sistem mo data.

Not: Fes akses broka i plei wan rol we i spesel insaed long saebakraem ekosistem taem oli pem mo stretem ol yusa kridensol we oli stilim ol yusa kridensol. Afta oli salemaot hae-kwaliti yusa kridensol, blong lukaotem ol popula envaeromen, long ol saebakriminal we bae oli yusum kridensol blong yusa blong kasem spolem netwok blong oganaesesen.

Blong stilim tru yusa kridensol oli hae valiu long ol saebakriminal, from se oli spidimap fes akses blong ol koperet netwok mo entapraes sistem. Wetem tru yusa kridensol we oli stilim, saebakriminal i save stap longwe long sam fasin blong taktik mo teknik, we i gat:

- fasin blong soem mo lukaotem wan taget
- givimaot taget netwok blong oli faenem
- developem wei blong fes akses, olsem:
  - fising materiol
  - no yusum gud sofwea mo eksposem
  - tagetem ol ples blong seves, we i gat RemoteDesktop Protocol (RDP) o virtual privatenetwork (VPN) seves
  - simpol fos atak agensem yusa aedentiti (mekemap paswod long maen)

Ol step ia i nidim wan investmen blong taem mo wan level blong teknikol skil we i soem wan mak long sam saebakriminal. Espeseli, saebakriminal we oli no save go tru long koperet netwok difens, oli save gat benefit stret long info stila infeksen, taem ol infeksen ia oli save givim kwik mo isi akses long yusa kridensol blong ol korperet netwok we oli wantem.

Long ol ples blong wok, sam wokman oli yusum ol pesenol divaes blong, tugeta, wok mo intanet braosing. Taem oli mekem olsem, ol wokman oli save jusum yusa kridensol blong olgeta insaed long web braosa paswod stoa mo ekstensen blong olgeta, o oli save mekem yus long web braosa otofil fija. Info stila oli tagetem paswod stoa, mo wetem ol konfomesen blong kuki mo ol nara data blong yuwan insaed long web braosa.

No olsem ol koperet divaes, pesenol divaes oltaem i nogat enfos entapraes sekiuriti polisi, we i posem wan hae risk long ol oganaesesen. Eksampol, ol wokman oli save joen long ol aktiviti olsem blong daonlodem paeret sofwea mo hae risk onlaen braosa, blong kwiktaem soem long ol saeba tret mo malwea infeksen.

Ol info stila, distributa, fes akses broka mo ransamwea we oli joen mo fomem wan stamba tingting blong wan saebakraem ekosistem we i mekem faenensol profit. Ekosistem i gro i kam gud moa taem ol saebakriminal oli speselaes mo develop skil we i tagetem sam step blong wan atak, mo afta salem skil iaolsem seves i go long ol nara kriminal we oli pat.

Tret aktiviti

ACSC blong ASD i stap trakem mo wajem wan inkris blong info stila aktiviti raonwol, we i soem wan tret we i gro long Australia netwok. Indastri i ripotem se info stila hem i moa popula malwea varian truaot long saebakraem aktiviti long 2023. Inkris volium blong data we oli stilim blong salem long dak web maketples, mo wan inkris long fes akses broka aktiviti we i levelem data ya, hemi soem tren ia we i stap kam antap, we inkris kwiktaem long 2024.

Infomesen stila ekosistem

Stej 1: Kasem malwea

Info stila oltaem oli givim long olgeta, long ol saebkriminal maketples, olsem MaaS o Stealer-as-a-Service, o salem olsem sos kod. MaaS i minim bisnis model we wan malwea developa i salem wan sabskripsen i go long rabis sofwea blong olgeta i go long wanwan tru long web-beis platfom, semak long tru Software-as-a-Service ofring. Maas model i mekem mak blong entri blong ol saebakriminal i kam daon, mo letem wanwan we i nogat teknikol skil blong serem malwea mo karem infomesen we oli stilim blong yusum long ol saeba atak.

Info stila oli givim olsem MaaS olsem jenerol advataes blong wan fi blong evri manis we i no sas, mo givim long saebakriminal akses long wan info stila dasbod. Daspod i help blong krietem info stila malwea, oganaesem data we oli stilim mo trakem namba blong joenem sistem. MaaS opereta i givim ol fija apdeit, tul mo teknikol sapot blong stap longwe long diteksen blong antivaeres sofwea mo blong pulum mo holemtaet ol sabskraeba. Plante info stila oli gat paoa blong dilitim olgetawan aot long divaes blong ol viktim afta we oli mekem data eksfiltresen.

Stej 2: Distribiusen

Saebakriminal we oli serem info stila mo karem infomesen long ol divaes we oli joen oli singaotem ‘Trafas’ (trafik distribiuta). Trafas i lidim ol viktim i go long rabis link, helpem spred blong info stila olsem pat blong bigfala kampen. Plante kampen oli no selektem, oli dipen long ol janis blong infeksen. Be, sam kampen oli mekem blong ol stret indastri mo mekem taget spea-fising agensem ol stret viktim. Trafas i kondaktem moa ol taget kampen ya olsem ansa blong ol kastoma diman; eksampol, ples we ol paya oli stap lukaotem akses long stret hae valiu oganaesesen o sekta.

Trafas bae i arenjem info stila long ol divaes blong viktim mo yusum wan bigfala renj blong teknik, we i gat:

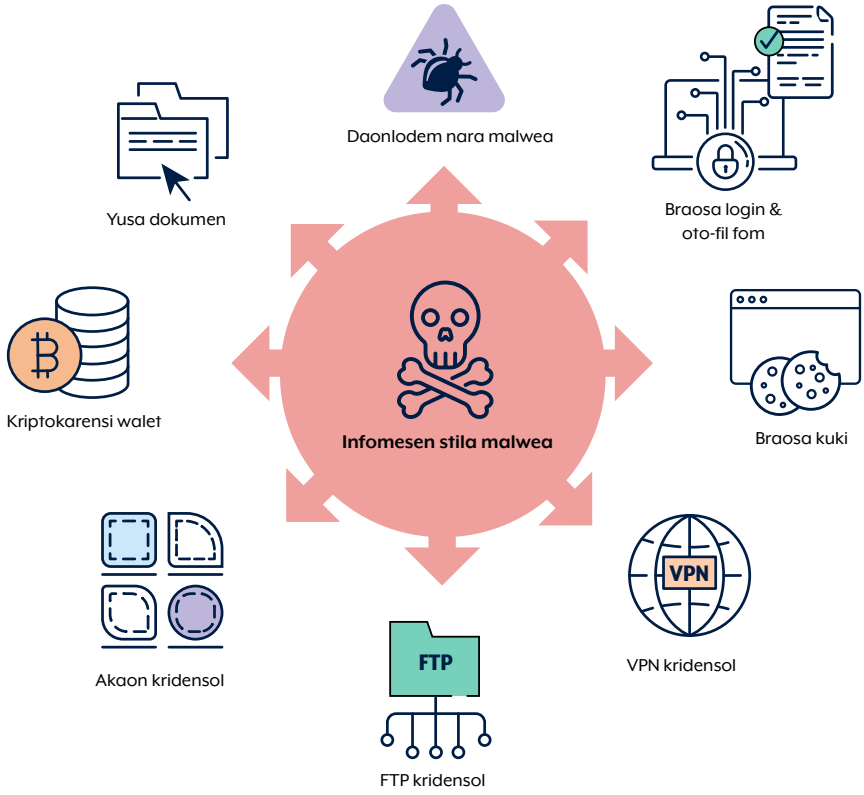
- **botnet**: netwok blong joenem ol kompiuta sistem we saebakriminal i kontrolem blong karem ol rabis aksen olsem givimaot fising mesej o malwea

- **fising**: i traem blong kasem pesenol infomesen tru long trik, we i gat imel o daerek mesej long sosol media, forom mo mesej ap we oli komon distribiusen rod we i mekem mak blong entri blong ol saebakriminal i go daon:
  - Ol mesej ia oltaem oli gat wan rabis link, be oli no go wetem ol rabis fael long imel hemwan.
- **rabis sej risal**: i kam tru long sej enjin optimaesesen (SEO) teknik we i tagetem stret ol websaet we oli sevem malwea we i jenis olsem tru sofwea o ol nara konten
- **malvetaesing**: i yusum denja kod, pinim i go insaed long tru onlaen advataesmen, blong serem malwea
- **krak o paeret sofwea**: daonlod we i gat ol vidio gem, serem ol vidio tru long YouTube, wetem ol rabis link long vidio diskripsen o ol komen, o aot long ol daonlod saet we i no gat tras long hem
- **sosol media advataesmen mo pos**: ol daerek taget blong jenisem ol malwea fael
- **rabis sofwea apdeit**: oltaem i jenis olsem wan web braosa apdeit

Stej 3: Data haves

Taem wan info stila i wok long divaes blong viktim, hem i stat kolektem pesenol data long masin we i joen long hem. Be wan nara wei blong stilim yusa kridensol, long ol taem we info stila oli pat blong wan botnet, saebakriminal i save kontrolem ol divaes we oli joen taem oli sendem konfigaresen koman blong aktivetem sam moa paoa o givimaot nara malwea. Long jeneral, info stila oli save:

- yusa nem mo paswod, speseli olgeta we oli storem long web braosa maltae-fakta autentikesen (MFA) yusa sesen/ token
- ol otentikesen kuki
- web braosa otofil fom infomesen
- imel kridensol, konden mo ol kontak
- web braosing histri
- yusa dokumen
- kredit kad ditel
- jat log blong desktop mesej ap
- sistem infomesen
- kryptokarensi walet
- VPN o Fael Transfea Protokol (FTP) kridensol.



Pikja 1. Info stila paoa

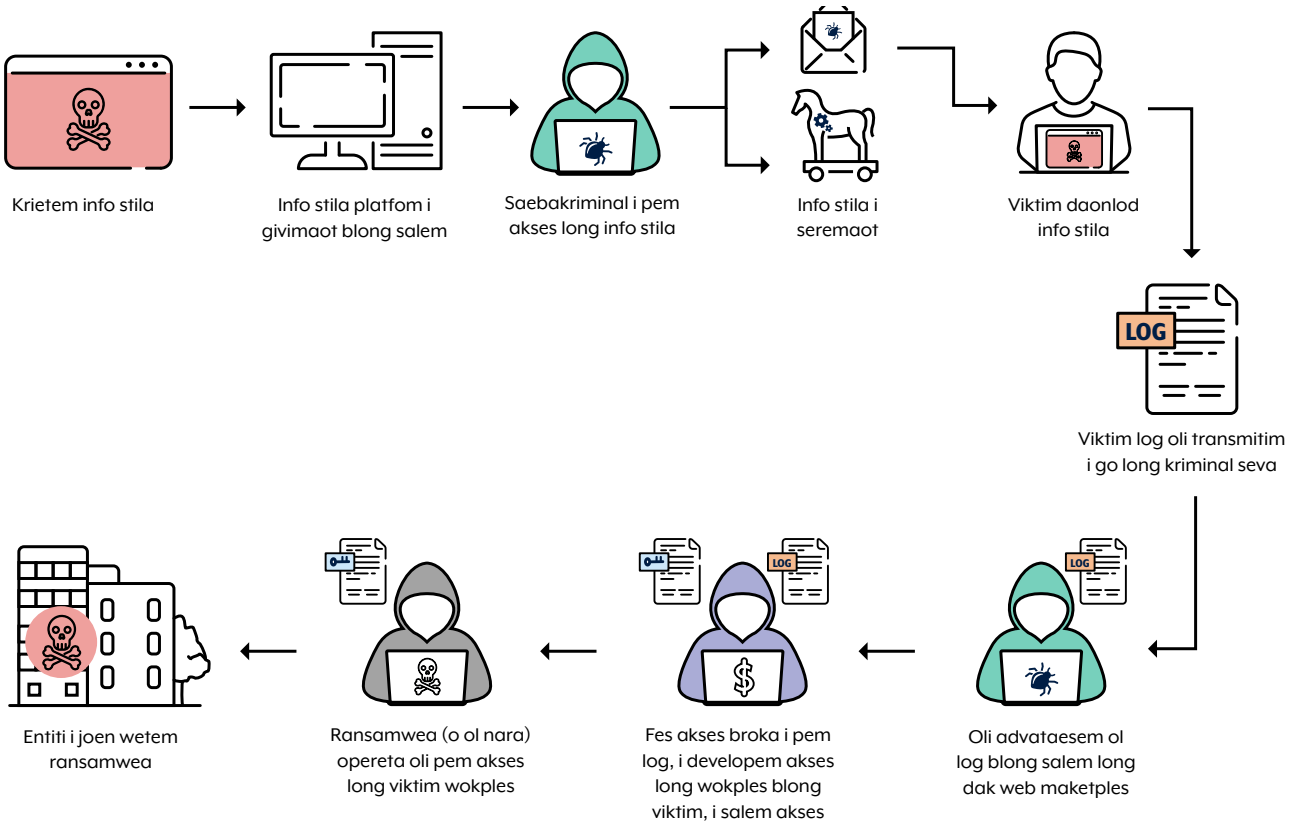
Sam web braosa autentikesen kuki oli kipim wan yusa login insaed long wan akaon o seves blong plante dei long wan taem, blong mekem se ol yusa oli no nid blong konfem bakegen. Sapos oli stilim, ol autentikesen kuki ia oli save stap gud longwe long MFA we i wan mas mo givim saebakriminal akses i go insaed long ol akaon blong ol viktim, netwok kampani mo bisnis sistem.

Stej 4: Data koleksen mo proses blong kasem mane

Info stila oli konfigarem blong karemaot infomesen blong viktim, we oli singaotem 'logs', blong rabis koman-mo-kontrol seva. Long jenerol, info stila i kontrolem ol ap blong mesej, olsem Telegram mo Discord, blong serem wan fid blong log wetem ol saebakriminal.

Ol stret maketples oli stap long Telegram mo truaot long dak web blong salem mo tredem ol log. Saebakriminal i mekem mane long log long plante wei, we i gat:

- fasin blong salem log long kriminal maketples, wetem fes akses broka
- Spolemgud ol viktim daerek, tru long aedentiti stil mo blakmel
- yusum infomesen blong fes akses insaed long kampani netwok blong ransamwea aktiviti.



Pikja 2. Info stila ekosistem mo posibol impak long wan oganaesesen

Ol risal

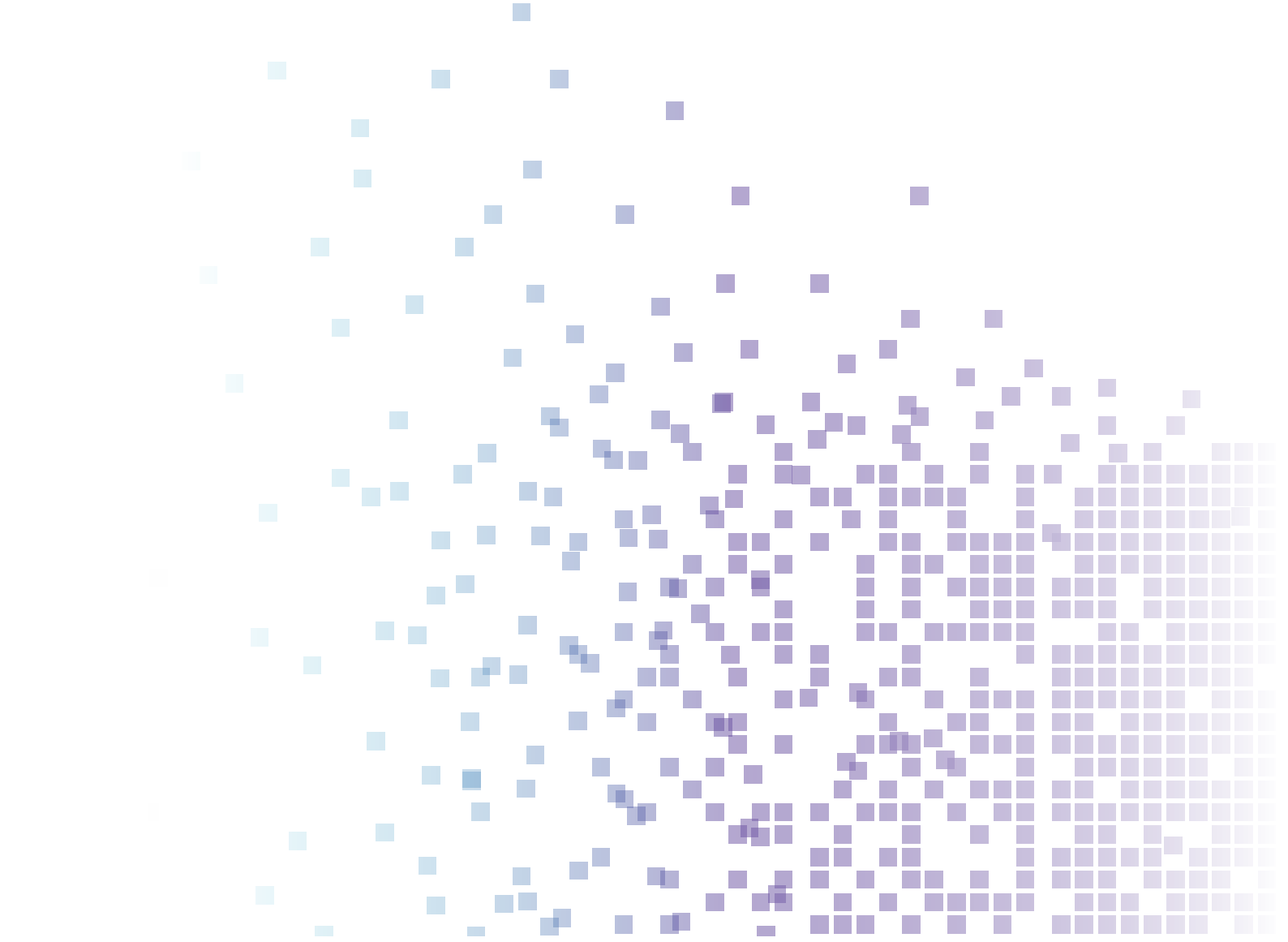
Info stila i save gat sam rabis risal blong tugeta, wanwan mo ol oganaesesen. Long ples we info stila i kolektem yusa kridensol, saebakriminal oli save yusum ol yusa kridensol ya blong aksesem kampani netwok o bisnis sistem wetem wan stret yusa akaon, plante taem sistem ona i let blong faenemaot.

Blong **ol oganaesesen** we info stila oli spolem, bae i save gat ol risal olsem:

- ransamwea
- Data brij
- bisnis imel kompromaes
- stil blong intelektuol propeti
- stil blong pesenol infomesen.

Blong **wanwan man** we info stila oli spolem, bae i save gat ol risal olsem:

- akses we i nogat atoriti long pesenol imel o ol sosol media akaon
- inkris risk blong stil blong aedentiti
- inkris risk blong ol fising atak
- faenensol risk o nogat akses long ol faenensol akaon
- lusum praevesi.



Keis stadi

Long keis stadi ia i haed nomo blong save serem long pabilk. I pulum sam saeba sekiuriti insiden we i muvum sam entiti blong Australia we oli bin ripotem long ACSC blong ASD. Entiti we i kasem impak ia afta, oli singaotem 'organisation'. Ol nem blong ol man long keis stadi ia oli no tru mo oli karemaot ol ditel blong protektem aedentiti blong ol viktim.

Oganaesesen hem i wan bisnis blong Australia we i letem ol staf blong aksesem kampani sistem long ol pesenol divaes blong olgeta. Alice hemi wan wokman blong oganaesesen we i stap wok hemwan.

Taem hem i wok long hom, Alice i aksesem kampani netwok blong oganaesen blong hem wetem pesenol laptop blong hem. Alice **i daonlodem**, long **laptop blong hemwan**, wan vesen blong Notepad++ (we hemi wan kaen sofwea blong tekem not) aot long wan websaet we hem i biliv se i tru. Wan **info stila** i jenis olsem wan instola blong Notepad++ sofwea.

Taem Alice i traem blong instolem sofwea, info stila i kam aktiv mo stat **blong karem yusa kridensol** aot long laptop blong hem. Hemia i gat, yusanem mo paswod blong wok blong hem, we hem i bin sevem long web braosa sef login fija blong hem. Info stila i sendem yusa kridensol ya long wan ples blong koman-mo-kontrol seva, we wan grup blong saebakriminal nao oli kontrolem.

Oli pakejem ol log we oli stilim wetem ol narafala mo afta **salem i go long saebakriminal** tru long wan dak web maketples.

Bob, wan saebakriminal i pem yusa kridensol blong Alice, i faenem yusa kridensol blong ol seves long oganaesesen netwok blong hem. Oganaesesen blong Alice i **no bin stopem MFA** ol seves ia, we i minim se Bob i save yusum yusa kridensol ya we oli stilim ya blong save gat gud **konfem mo aksesem** kampani netwok.

Bob i aksesem kampani netwok blong oganaesesen blong Alice we oli no save, hem i yusum **stret yusa kridensol we oli stilim**. Bob i save muv raon long kampani netwok mo luksave ol pesenol data we i blong oganaesesen mo i stilim blong oli save karemaot olgeta long kampani.

Blong stilim ol pesenol data, Bob **putum long kod** databes blong oganaesesen **mo ol fael sistem** blong mekem se oli no save kasem.

Mitigesen

Ol oganaesesen oli no save gat kontrol long ol divaes we i konek long kampani netwok, speseli long ol pesenol divaes we ol wokman oli yusum taem oli stap wok long hem. ACSC blong ASD i rekomendem ol oganaesen blong lukluk moa blong gat kontrol blong protektem olgetawan long risk blong ol info stila we i stap tagetem ol yusa kridensol. Ol kwalifikesen ia i gat:

Givim aweanes abaot saeba sekiuriti trening long ol staf

- Protektem saksesful taget blong sosol enjiniaring mo daonlod blong ol rabis fael, taem oli givim gudfala trening long ol staf.
- Mekem aweanes blong info stila, wei blong givimaot fising tret blong olgeta i go long oganaesesen blong yu.

Protektem ol akaon blong kampani

- Yusum MFA:
- Yusum MFA truaot long ol seves blong aotsaed mo insaed, sistem mo pesenol data sos, speseli blong webmel, VPN, mo ol akaon we oli laki blong gat yusa akaon we i save aksesem ol kritikol sistem. Bes praktis i blong yusum strong fising risistens MFA long evri akaon.
- Katemaot ol yusa akaon taem oli nomo nidim.
- Limitim ol janis blong administreta:
- Mekem netwok administresen mo ol nara laki wok blong yusum wan tru lok-daon wokstesen nomo (eksampol wan administresen woksatesen we i sef)
- Folem ol smol bes janis blong praktis we i nidim administresen blong yusum ol yusa akaon blong manejem ol sistem mo standad yusa akaon blong ol wok we i no blong administresen.
- Protektem ol janis blong yusa akoan (karemaot olgeta we i gat atoriti blong aksesem ol seves onlaen) blong aksesem intanet, imel mo web seves.
- Tingting blong yusum just-in-time administresen blong ol sistem mo aplikesen.
- Pusum manejmen i strong mo mekem odit blong ol laki yusa akaon.
- Oltaem, apdeitem paswod, speseli ekstenol-fesing blong rimot akses akaon
- Pusum laeftaem, taem aot mo sanset polisi long ol sesen token mo kuki.

Mekem strong bisnis muvmen

- Mekem wan bisnis muvmen risk asesmen mo yusum bisnis muvmen blong mekem strong gaedlaen.
- Yusum wan Bring Your Own Device (BYOD) polisi sapos yu letem ol wokman blong yusum ol pesenol divaes blong wok, from ol joen bisnis divaes oli moa sef bitim blong no manejem ol pesenol divaes.

Luklukbak mo jekem saplae jen risk blong ol venda we i aksesem netwok blong yu, we i gat Software-as-a-Service (Saas) venda mo Managed Service Providers. Hao blong Manejem Sekiuriti blong Yu Taem Yu Pat long wan Managed Service Provider.

Protektem kampani netwok blong yu

- Kipim ol aplikesen mo opereting sistem oli apdeit.
- Yusum lokol sekiuriti polisi blong mekem aplikesen kontrol wetem wan strik alao lis.
- Yusum netwok sistem divisen blong seraotem netwok pat beis long rol mo wok.
- Odit mo jekem yusa aktiviti, speseli blong ol wokman.
- Luklukgud ol laki akaon we oli save soem no raet akses long pesenol data o data transfea aktiviti we i no nomol, olsem bigfala volium blong data we oli sendem i go aotsaed long wan netwok.
- Mekem ol polisi blong lusum data mo ol tul blong protektem deta transfea we i nogat raet.

Blong kam wan ASD Saeba Sekiuriti Netwok Patna mo joenem ASD's Cyber Threat Intelligence Sharing (CTIS) seves

- CTIS i wan tu wei blong serem platfom we i mekem gavman mo ol bisnis patna oli save kasem mo serem infomesen abaot rabis saeba aktiviti.
- ACSC blong ASD i stap trakem aktiviti blong info stila mo serem ditel blong aktiv koman mo kontrol infrastrakja truaot long CTIS platfom.
- Saenap blong kam wan patna mo protektem oganaesesen mo kastoma data blong yu aot long saebakrimina tret.

Rere from wan koperesen

- Developem wan saeba sekiuriti insiden rispons plan blong yusum long wan taem blong info stila koperesen. Mekemsua se ol wokman oli save wanem blong mekem mo hu blong kondaktem sapos oli se oli daonlodem wan fael we oli no sua long hem.

Statem Essential Eight blong ACSC blong ASD

- Antap long ol kwalifikesen we oli tokbaot antap ia, ACSC blong ASD i rekomendem strong blong statem olgeta we oli stap long Essential Eight blong ACSC blong ASD.

Advaes long ol wokman taem oli wok long ples ia

- Protektem infomesen blong yu long ol pesenol divaes
  - Developem klin saeba mo no klik long ol link we i luk difren o kamaot, o daonlodem ol fael o sofwea long ol sos we yu no save o no trastem.
  - Yusum difren paswod blong wok mo ol pesenol akaon. Yusum MFA blong ol pesenol akaon taem i posibol.
  - Yu no mas putum wok kridensol blong yu long pesenol paswod maneja be nomo sapos bos blong yu i apruvum. Hemia i tekem tu web braosa paswod maneja blong yu. **Sapos yu gat tu tingting, rikwestem blong bos blong yu i givim wan kampani sapot paswod maneja.**
  - Yu no mas log in i go long ol wok akaon blong yu blong serem ol wokstesen.
  - Lukaot long wanem oli storem long web braosa otofil fija blong yu. Info stila i tagetem ol data braosa we oli sevem long otofil fom. Taem yu fulumap web fom, tingting blong putum pesenol data long han, olsem kredit kad namba, no sevem long web braosa otofil fija blong yu.
  - Log aot long evri seves onlaen mo kliarem web braosa kuki afta we yu finis long wan braosing sesen blong no givim tumas infomesen long ol info stila.
  - Mekemsua se opereting sistem blong yu we oli bildim long antivaeres solusen i wok. Sapos yu yusum wan antivaeres solusen blong nambatri pati, mekemsua se i apdeit mo hem i blong wan tru venda.

Asistens

Ol oganaesen blong Australia we i gat kil o i nidim asistens long wan info stila koperesen yu save kondaktem ACSC blong ASD tru long **1300 CYBER1 (1300 292 371)** o sabmitim wan ripot long cyber.gov.au/report.

ACSC blong ASD i leftemap tingting blong ol entiti blong ripotem ol wari netwok aktiviti mo poen blong koperesen blong joen wetem ol info stila, iven sapos wan insiden oli jekem finis. Mifala i yusum infomesen we yufala i givim blong impruvum save blong mifala long saeba tret akta taktik, teknik mo proses, we i helpem mifala blong wonem ol nara oganaesesen blong Australia we oli bin kasem kil long sem wei.

Disklema

Tul insaed long gaed ia hem i jenerol mo man i no mas tekem olsem likol advaes o dipen long hem blong helpem hem long eni taem o imejensi situesen. Long eni impoten mata, yu mas lukaotem stret independen profesenol advaes long saed blong ol situesen blong yuwan.

Commonwealth hem i no akseptem responsabiliti o laeabiliti blong eni damej, lus o ekspens we man i kasem olsem wan risal blong dipen long infomesen we i stap insaed long gaed ia.

Blong kasem moa infomesen, o blong ripotem wan saeba sekiuriti insiden, kondaktem mifala:

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

Namba ia hem i avelebol blong yu yusum insaed long Ostrelia nomo.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre