APT40 Advaesori

PRC MSS tredkraf long aksen

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**

Tebol blong konten

Ovaviu:

Bakgraon

Advaesori ia, we Australian Signals Directorate's Australian Cyber Security Centre (ACSC blong ASD), United States Cybersecurity mo Infrastructure Security Agency (CISA), the United States National Security Agency (NSA), the United States Federal Bureau of Investigation (FBI), the United Kingdom National Cyber Security Centre (NCSC-UK), the Canadian Centre blong Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), the German Federal Intelligence Service (BND) mo Federal Office blong Protection of the Constitution (BfV), the Republic of Korea's National Intelligence Service (NIS) mo NIS' National Cyber Security Center, mo Japan's National Center of Incident Readiness mo Strategy for Cybersecurity (NISC) mo National Police Agency (NPA) – afta oli lukluk hem olsem "otoring ejensi" – aotlaenem wan People's Republic of China (PRC) stet sponsa saeba grup mo karen tret long ol Australian netwok. Advaesori ya i kamaot long ol otoring ejensi we oli serem save long tret mo tu olsem ACSC blong ASD insiden rispons investigesen.

PRC stet-sponsa saeba grup i bin tagetem finis ol oganaesesen long fulap kantri, iven Australia mo United States, mo ol teknik we oli haelaetem andanit ya ol PRC stet-sponsa akta raonwol nao oli stap yusum oltaem. Mekem se, ol otoring ejensi oli bilivim grup, mo sem teknik i stap olsem wan tret long ol netwok blong ol kantri blong olgeta tu.

Otoring ejensi i asesem se grup ya i kondaktem rabis saeba operesen blong PRC Ministry of State Security (MSS). Aktiviti mo teknik i joen wetem ol grup we oli trakem olsem Advanced Persistent Threat (APT) 40 (we oli save olsem Kryptonite Panda, GINGHAM TYPHOON, Leviathan mo Bronze Mohawk long indastri ripoting). Grup ya oli bin ripotem se hemi bes long Haikou Hainan Provins, PRC mo i kasem wok long PRC MSS, Hainan State Security Department.[2] Advaesori ya i givim wan eksampol blong wan impoten keis stadi blong rabis teknik long aksen agensem tu viktim netwok. Ol keis stadi oli impoten blong saeba sekiuriti praktisona blong faenemaot, priventem mo stretem APT40 intrusen agensem netwok blong olgetawan. Ol keis we oli selektem ya oli blong stret wok blong ripea we oli bin tekem finis blong katemdaon risk blong fasin blong spolem samting bakegen tru long tret akta ya, o ol narawan. Olsem ya, ol keis stadi oli olfala long oda, blong mekem sua se ol oganaesesen oli gat inaf taem blong oli ripea.

Aktiviti samari

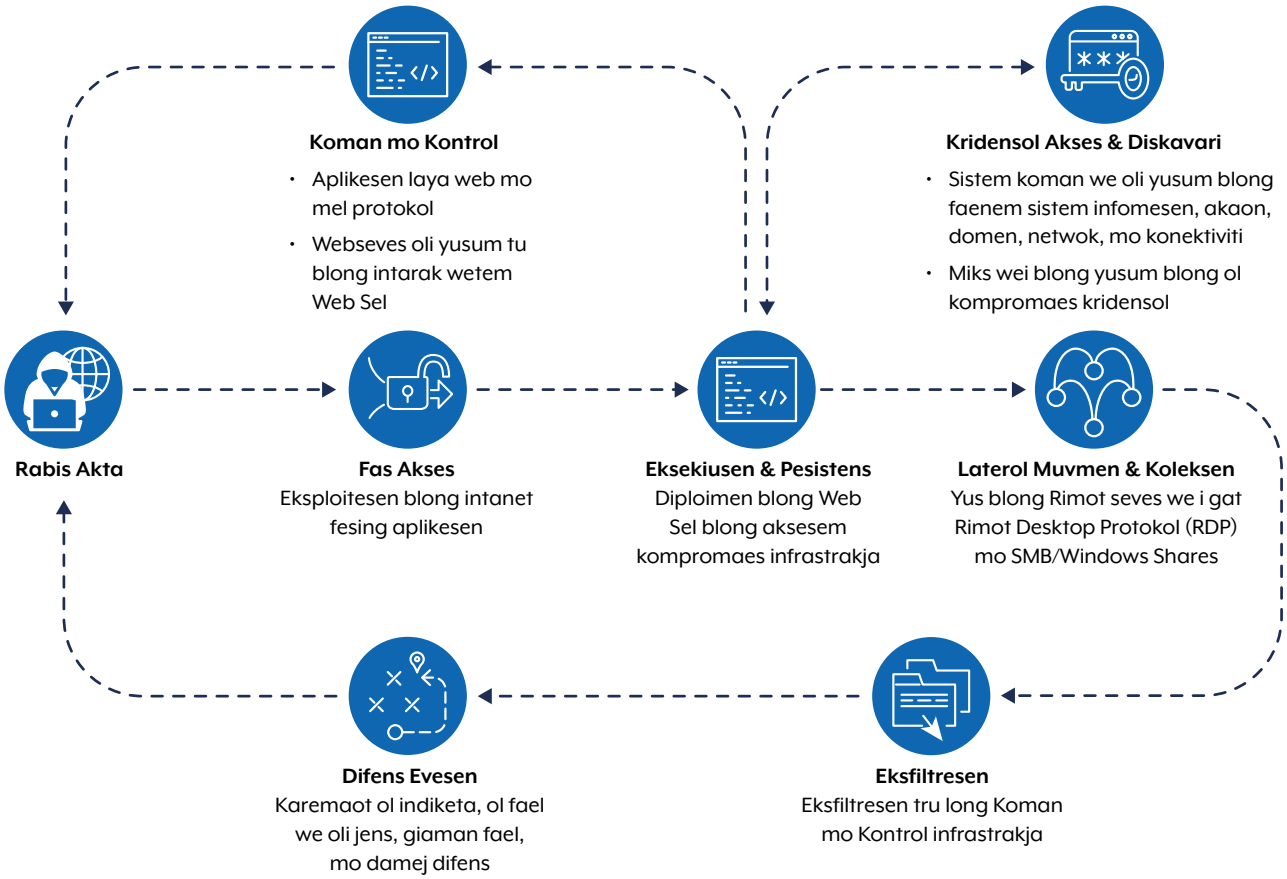
APT40 i bin ripitim ol taget netwok blong Australia tu wetem gavman mo praevet sekta netwok long rijin, mo tret we oli kosem long ol netwok ya oli stap gohed. Tredkraf i tokbaot advaesori ya oltaem oli stap faenem agensem ol netwok blong Australia.

Mas save se, APT40 i gat paoa blong jenis kwik mo yusum atak blong proof-of-concept (s) (POCs) blong ol niu jans blong atak mo yusum kwik olgeta agensem ol taget netwok we oli gat infrastrakja blong sem atak ya. APT40 i kondaktem oltaem rekonesons(save) agensem ol netwok blong intres, we i gat tu netwok long ol otoring ejensi kantri, we oli stap lukaotem ol janis blong atakem ol taget blong hem. Nomol rekonesons ya i putum grup blong faenemaot wik, en blong laef o no gat mentenes divaes long ol netwok blong intres, mo blong stopem kwik spred blong atak. APT40 i gohed blong faenem sakses blong stopem ol atak ya eli stat long 2017.

APT40 i stopem kwik ol niu pablik atak lonng ol bigfala sofwea we oli bin yusum olsem Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) mo Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473). ACSC blong ASD mo otoring ejensi oli ekspektem grup blong kontinu blong yusum POCs blong ol niu hae-profael atak long haoa o dei blong pablik rilis nomo.

2 U.S. Dipatmen blong Jastis. 2021. Fo Chinese Nasonal we oli wok wetem Ministry of State Security oli bin jajem olgeta wetem Global Computer Intrusion Campaign Targeting Intellectual Property mo Confidential Business Information, we hemi ingkludum Infectious Disease Research.

Pikja 1: TTP flojat blong aktiviti blong APT40



Grup ya i kam blong laekem spolem wik, pablik fesing infrastrakja long ol teknik we i nidim yusa intaraksen, olsem fishing kampen, mo putum wan hae praeoriti blong kasem wan tru kridensol blong jenisim wan renj blong ol foloap aktiviti. APT40 i stap yusum nomol web sel (T1505.003) blong kontinu oltaem, speseli long eli laef sekol blong wan intrusen. I nomol, afta long wan saksesful fes akses APT40 i fokas blong statem wan longfala kontinu blong kipim akses long envaeronmen blong viktim. Be, olsem kontinu longtaem i kamaot eli long wan intrusen, janis se bae oli stadi long hem long evri intrusen-nomata long taem blong atak o ol aksen we oli bin tekem.

Notabol tredkraf

Nomata we APT40 oli bin yusum ol kompromaes websaet blong Australia olsem command mo control (C2) host from ol operesen blong olgeta, grup i bin tekem teknik ya (T1594).

APT40 i bin grapem stael ya wolwaet taem hemi yusum ol kompromaes divaes, ingkludum smol-ofis/hom-ofis (SOHO) divaes, olsem operesenol infrastrakja mo las hop ridaerekta (T1584.008) blong ol operesen blong hem long Australia. Hemia i letem ol otoring ejensi blong faenemaot gud mo trakem muvmen blong grup ya.

Plante long ol divaes blong SOHO oli en blong laef o i no fit mo oli givim wan sopsop taget blong N-dei yus. Taem oli agri, SOHO divaes oli givim wan poen blong enta blong ol atak we oli disaenem blong joen gud wetem stret trafik mo jalenjem ol netwok difenda (T1001.003).

Teknik ya ol nara PRC stet-sponsa akta raonwol oli stap yusum oltaem, mo ol otoring ejensi we oli lukaotem hemia blong kam wan tret we oli bin serem. Blong moa infomesen, luk ol joen advaesori People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers mo Devices mo PRC State-Sponsored Actors Compromise mo Maintain Persistent Access long U.S. Critical Infrastructure.

APT40 samtaem i yusum infrastrakja we oli no lisim olsem wan viktim fesing C2 infrastrakja long ol operesen blong hem; be, tredkraf ya lukluk se i stap go daon.

Tuling

ACSC blong ASD i stap serem sam rabis fael we oli faenemaot long taem blong investigesen we i kamaot daon ya. Ol fael ya oli aplodem long VirusTotal blong yusum bigfala netwok difens mo saeba sekiuriti komuniti blong save gud ol tret blong difendem agensem olgeta.

Keis stadi

ACSC blong ASD i serem tu investigesen ripot we oli no save blong provaedem aweanes long hao ol akta oli yusum tul mo tredkraf blong olgeta.

MD5	Faelnem	Moa infomesen
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

Keis stadi 1

Ripot ya oli bin haedem blong yusum blong spredem bigwan. Oganaesesen we i kil ya afta long hemia oli singaotem hem 'oganaesesen'. Sam stret ditel oli bin tekemaot blong protektem aedentiti blong viktim mo insiden rispons wei blong ACSC blong ASD.

Eksekiutif Samari

Ripot ya i talemaot ol faending blong ACSC blong ASD investigesen long saksesful kompromaes blong netwok blong oganaesesen bitwin Julae mo Septemba 2022. Ripot ya oli provaedem long oganaesesen blong samaraesem rabis aktiviti we oli bin faenem mo holem olgeta blong rekomendem ol ripea. Ol risal oli soemaot se agrimen ya APT40 nao i bin tekem.

Long medel Ogis, ACSC blong ASD i bin notifaem oganaesesen blong ol rabis intaraksen wetem netwok blong olgeta long wan kompromaes divaes we grup oli bin yusum long let Ogis mo, wetem konsen blong oganaesesen, ACSC blong ASD i spredem host beis sensa blong spolem ol host long netwok blong oganaesesen. Ol sensa ya oli letem ACSC blong ASD insiden rispons analis blong tekem wan gudfala digitol forensik investigesen. Wetem sensa data we oli gat, ol analis blong ACSC tru long ASD oli mapem gud aktiviti blong grup mo krietem wan taemlaen wetem ol ditel long ol iven we oli bin mekem investigesen ya.

Stat long Julae kasem Ogis, ki akta aktiviti we oli faenem tru long ACSC blong ASD hemi ingkludum:

- host namba, we i letem wan akta blong bildim wanwan map blong netwok blong olgeta;
- yus blong web sel, we i givim long akta wan fes futhol long netwok mo wan paoa blong givimaot koman; mo
- priperesen blong ol nara tul we ol akta oli yusum blong ol rabis pepos.

Investigesen i soemaot evidens blong wan bigfala amaon blong pesenol data we oli aksesem mo evidens se ol akta oli stap muv insaed long netwok (T1021.002). Plante blong ol kompromaes ya oli helpem grup blong statem ol maltipol akses vekta long netwok, mekem se netwok i gat wan flat strakja, mo oli yusum ol intenol sofwea we oli developem we oli no sef blong oli save aplodem ol fael. Witdro data hemi ingkludum ol impoten autentikesen kridensol we i helpem grup blong log in, mo tu netwok infomesen we bae i letem ol akta blong kasembak akses we oli no otoraesem sapos originol akses vekta i bin blok. Nogat moa rabis tul we oli faenem bitim hemia ya long ol fas masin blong spolem; be, wan grup akses long tru mo impoten kridensol nao bae i save karemaot nid blong moa tul. Ol risal blong investigesen oli soemaot se APT40 nao i tagetem oganaesesen, long narasaed olsem wan viktim we oli foldaon komperem long wan pablik tret we oli save long hem.

Investigesen faending

Long medel blong Ogis 2022, ACSC blong ASD i bin notifaem oganaesesen se wan konfem rabis IP we oli bilif se i bin joen wetem wan stet-sponsa saeba grup i bin wok wetem kompiuta netwok blong oganaesesen bitwin Julae mo Ogis. Kompromaes divaes ya ating hemi blong wan smol bisnes o hom yusa nomo.

Long let Ogis, ACSD blong ASD oli bin spredem wan host beis ejen blong hostem long netwok blong oganaesesen we i soem evidens se oli bin gat kil blong wan atak.

Sam atifak we i save sapotem ol wok blong investigesen oli no bin avelebol from konfigaresen blong login o netwok disaen. Nomata long hemia, redines blong oganaesesen blong provaedem evri avelebol data i helpem ACSC blong ASD insiden ripota blong kondaktem wan bigfala investigesen mo blong fomem wan save long aktiviti blong APT40 long netwok.

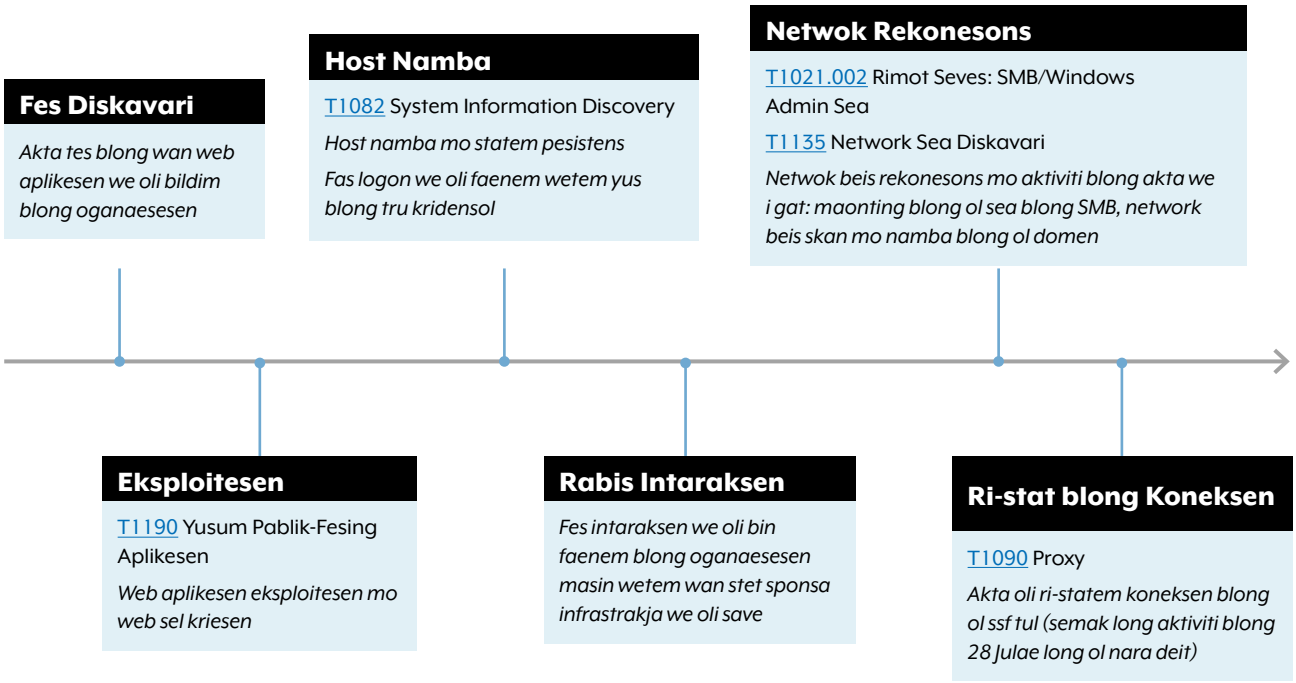
Long Septemba, afta konsaltesen wetem ACSC blong ASD, oganaesesen i disaed blong karemaot IP we oli faenem long fes notis. Long Oktoba, oganaesesen i statem ripea.

Ditel

Stat long Julae, ol akta oli save testem mo spolem wan nomol web aplikesen (T1190) we i ron long `<webapp>2-ext`, we i helpem wan grup blong statem wan futhol long network long wan niu zon (DMZ). Hemia i tekem tu blong nemem tugeta netwok wetem ol nara domen we yu save luk. Kompromaes kridensol (T1078.002) we oli yusum blong ansarem Active Directory (T1018) mo witdroem data tru long ol fael sering (T1039) long ol maltipol masin long DMZ. Akta i karemaot wan Kerberoasting atak blong kasem wan stret netwok kridensol long wan seva (T1558.003). Grup oli no bin faenem eni moa samting blong poen blong presens long tugeta DMZ o intenol netwok.

Visuol taemlaen

Taemlaen andanit ya i givim wan bigfala pikja long ol ki stej blong ol rabis akta aktiviti we oli bin faenem long netwok blong oganaesesen.



Ditel taemlaen

Julae: Ol akta we oli statem wan fes koneksen long fes pej blong wan kastom web aplikesen (T1190) we oli bildim blong oganaesesen (afta oli singaotem hem olsem 'web aplikesen' o '*webapp*') tru long wan transpot leya sekiuriti (TLS) koneksen (T1102). Oli nomo faenem wan nara impoten aktiviti.

Julae: Ol akta oli stat blong nambarem ol web aplikesen websaet mo lukaot long ol enpoen[2] blong go moa long investigesen.

Julae: Ol akta oli fokas long ol tes blong yusum wan stret enpoen.

Julae: Ol akta oli save `POS` gud long web seva, ating tru long wan web sel we oli putum long wan nara pej. Nambatu IP, maet i wok blong ol sem akta, bae i save stat post long sem URL. Ol akta oli krietem mo testem wan namba blong ol web sel.

Stret wei blong yusum oli no save, be hemi klia se stret enpoen oli bin tagetem blong krietem ol fael long `<webapp>2-ext`.

ACSC blong ASD i bilif se tu IP adres koneksen tufala i pat blong sem intrusen from sea intres blong olgeta mo fas koneksen we i hapen bitwin sam minit apat nomo.

Julae: Grup i gohed blong hostem namba, lukaotem ol impoten inkris blong ol jans, mo yusum wan difren web sel blong spred. Ol akta oli login long web aplikesen wetem ol kompromaes kridensol blong `<firstname.surname>@<organisation domain>`

Aktiviti blong ol akta oli no luk olsem se oli kasem impoten inkris long `<webapp>2-ext`. Be, ol akta oli tanem go long ol netwok beis aktiviti.

Julae: Ol akta oli testem ol kompromaes kridensol blong wan seves akaon[3] we maet oli faenem long ol had kod long ol intenol sistem we oli save aksesem.

Julae: Ol akta oli jusum wan open sos tul Secure Socket Funnelling, we oli bin yusum blong konek aot long ol rabis infrastrakja. Koneksen ya oli yusum blong mekem hol long trafik long ol akta atak masin insaed long intenol netwok blong oganaesesen, we nem blong masin ya oli yusum long ol iven blong ol log taem oli stap traem blong yusum ol kridensol blong ol seves akaon.

Ogis: Oli bin luk ol akta oli kondaktem wan sot aktiviti, we ingkludum fel blong statem koneksen we i gat seves akaon.

Ogis: Ol akta oli pefomem impoten netwok mo Aktif Daerektori namba. Wan difren kompromaes akaon hemi wok inaf blong joenem ol sea[4] long ol masin blong Windows insaed long DMZ, blong helpem saksesful data eksfiltresen.

Hemia i wan janis blong yusum wan kridensol we oli stilim long ol masin we oli joenem ya long DMZ. Ol faeawol oli blokem ol akta blong no tagetem intenol netwok wetem semfala aktiviti olsem ya.

Ogis – **Septemba:** SSF tul i statem bakegen wan koneksen long wan rabis IP. Grup ya oli no faenem yet se oli stap mekem moa aktiviti olsem ya kasem taem akses blong olgeta i blok.

Septemba: Oganaesesen i blokem rabis IP taem oli putum olgeta long denaelis long faeawol blong olgeta.

2 Long konteks ya, wan enpoen hemi wan fangsen blong web aplikesen

3 Ol seves akaon oli no joen wetem ol wanwan yusa, be moa long ol seves nomo. Long wan Microsoft koperet domen, i gat fulap kaen akaon.

4 Maonting sea hemi wan proses blong mekem ol fael long wan fael sistem strakja we wan yusa o yusa grup oli save aksesem.

Ol akta taktik mo teknik

MITRE ATT&CK fremwok hemi wan koleksen blong dokumen blong ol taktik mo teknik we oli tret akta oli wokem long saebaspes. Fremwok ya oli krietem tru long US not-for-profit we hemi MITRE Koperesen mo i wok olsem wan globol lanwis araon long ol fasin blong tret akta.

ACSC blong ASD i aksesem ol teknik mo taktik ya blong hemi impoten long ol rabis aktiviti blong ol akta:

Rekonesons

T1594 – Sej Viktim-Onem Websaet

Akta i kaontem kastom web aplikesen websaet blong faenemaot ol janis blong aksesem netwok.

Fas Akses

T1190 – Yusum Pablik-Fesing Aplikesen (long saed blong yusum kastom web aplikesen)

T1078.002 – Tru Akaon: Domen akaon (long saed blong log in wetem stret kridensol)

Yusum intanet ekspos kastom web aplikesen i givim wan fas poen blong akses long akta. Akta bihaen bae i save yusum ol kridensol we oli bin agri long hem blong seftem akses blong olgeta long netwok.

Eksekiusen

T1059 – Koman mo Skrip Intapreta (long saed blong givimaot koman tru long web sel)

T1072 – Sofwea Diploimen Tul (long saed blong akta oli yusum open sos tul Sekiua Soket Fanel (SSF) blong konek long wan IP)

Pesistens

T1505.003 – Seva Sofwea Komponen: Web Sel (long saed blong yus blong wan web sel mo SSF blong statem akses)

Kridensol Akses

T1552.001 – Kridensol long ol Paswod Stoa (long saed blong ol paswod fael we i go wetem bilding manejmen sistem (BMS))

T1558.003 – Stil o Foj Kerberos Tiket: Kerberoasting (long saed blong atak blong kasem netwok kridensol)

Laterol Muvmen

T1021.002 – Rimot Seves: SMB Sea (long saed blong ol akta oli resemap ol SMB sea long ol maltipol divaes)

Koleksen

T1213 – Data we i kam long Information Repositories (long saed blong manuol/ dokumentesen we oli faenem long BMS seva)

Eksfiltresen

T1041 – Eksfiltresen Ova C2 Janel (long saed blong ol akta data we oli karemaot long Active Directory mo maonting sea)

Keis stadi 2

Ripot ya oli bin haedem blong yusum blong spredem bigwan. Oganaesesen we i kil ya afta long hemia oli singaotem hem 'oganaesesen'. Sam stret ditel oli bin tekemaot blong protektem aedentiti blong viktim mo insiden rispons wei blong ACSC blong ASD.

Eksekiutif Samari

Ripot ya i soemaot risal blong ACSC blong ASD investigesen i kam long saksesful kompromaes blong oganaesesen netwok long Eprel 2022. Investigesen ripot ya oli givim long oganaesesen blong samaraesem rabis aktiviti we oli faenem mo putum ol rekomendesen blong ripea. Ol risal oli soemaot se agrimen ya APT40 nao i bin tekem.

Long Mei 2022, ACSC blong ASD i bin notifaem oganaesesen long ol rabis aktiviti we oli luk i stap spolem netwok blong oganaesesen long Eprel 2022 finis i kam. Afta long hemia, oganaesesen i letem ACSC blong ASD i save se oli bin faenem rabis sofwea long wan intanet-fesing seva we i provaedem login potol blong solusen blong oganaesesen koperet rimot akses. Seva ya i yusum wan rimot akses login mo aedentiti manejmen prodak mo bae oli lukluk long hem long ripot ya olsem 'kompromaes aplaens'. Ripot ya i tokbaot risal blong investigesen mo ripea advaes we oli developem blong oganaesesen long rispons long investigesen we ACSC blong ASD i bin kondaktem.

Evidens i soemaot se pat blong netwok blong oganaesesen i bin kompromaes from ol rabis saeba akta tru long rimot akses login potol blong oganaesesen stat long Eprel 2022. Seva ya ating oli bin kompromaes tru long plante akta, mo maet i gat kil tru long wan rimot kod eksekiusen (RCE) atak we oli bin pablisim olbaot raon long sem taem blong kompromaes ya.

Ki akta aktiviti we oli bin faenem tru long ACSC blong ASD hemi gat:

- host namba, we i letem wan akta blong bildim wanwan map blong netwok blong olgeta;
- eksploitesen blong intanet-fesing aplikesen mo yus blong web sel, we i givim fas futhol long netwok mo wan paoa blong karemaot koman;
- developmen blong sofwea atak blong inkrisim ol janis; mo
- koleksen blong kridensol blong letem laterol muvmen

ACSC blong ASD i bin faenemaot se wan rabis akta i bin tekemaot sam handred difren yusanem mo paswod pea long kompromaes aplaens long Eprel 2022, mo tu olsem wan namba blong ol malti-fakta autentikesen kod mo ol atifaks wei i joen long rimot akses sesen. Long wan riviu we i kam long oganaesesen, ol paswod oli bin faenem oli tru. ACSC blong ASD i bin aksesem se akta maet i bin kolektem ol teknikol atifaks ya blong haejakem o krietem wan rimot login sesen olsem wan tru yusa, mo aksesem intenol koperet netwok blong oganaesesen tru long wan tru yusa akaon.

Investigesen faending

Investigesen samari

ACSC blong ASD oli save se ol aplaens blong ol kompromaes akta we i provaedem rimot login sesen blong ol staff blong oganaesesen mo oli bin yusum blong traem blong kondaktem moa aktiviti. Ol aplaens ya i gat tri lod-balens host we fas evidens blong kompromaes oli bin faenemaot eli. Oganaesesen i bin satem daon tu long trifala lod-balens hosts smoltaem nomo afta long fas kompromaes. Olsem wan risal, evri fiuja aktiviti oli hapen long wan singgel host. Ol nara seva we oli joen wetem kompromaes aplaens olgeta tu oli bin lod-balens long wan sem fasin. Long stret toktok, evri kompromaes aplaens we oli tokbaot long plante long ol ripot ya olsem wan 'singgel aplaens'.

Akta i bilif se hemi bin yusum ol atak ya oltaem finis blong spredem web sel i go long kompromaes aplaens stat long Eprel 2022 i go fored. Ol tret akta blong grup nao oli stadi long hem blong kasem hae inkris blong ol janis long aplaens ya. ACSC blong ASD i no save faenem ful digri blong aktiviti from oli nogat inaf login avelebiliti. Be, evidens long divaes i soemaot se wan akta i save kasem olgeta ya:

- Koleksen blong plante handred tru yusanem mo paswod pea; mo
- Koleksen blong ol teknikol atifaks we maet i save letem wan rabis akta blong aksesem wan vituol desktop infrastrakja (VDI) sesen olsem wan tru yusa.

ACSC blong ASD i faenem se akta ating i save lukaot moa kompromaes blong netwok blong oganaesesen. Atifaks we akta i karemaot ya maet i save letem olgeta blong haejakem o statem wan vituol desktop sesen olsem wan tru yusa, ating olsem wan yusa blong jus blong olgeta; iven ol administreta. Akta bae i save yusum vekta akses ya blong go mekem moa kompromaes oganaesesen seves blong kasem pesistens mo ol nara gol.

Ol nara oganaesesen aplaens insaed long hosting provaeda oli manejem envaeronmen we oli no soem evidens blong kompromaes ya.

Akses

Host insaed long kompromaes aplaens ya i provaedem autentikesen tru long Aktif Daerektori mo wan webseva, blong ol yusa we oli konek i go long ol sesen blong VDI (T1021.001).

Lokesen	Kompromaes aplaens hostnem (lod-balens)
Datasenta 1	HOST1, HOST2, HOST3

Aplaens infrastrakja i gat tu akses getawei host we i mekem wan hol i go long VDI blong yusa, taem oli kasem wan autentikesen token we oli krietem mo daonlodem long aplaens.

I nogat evidens blong kompromaes blong eni long ol host ya. Be, akses getawei host log i soemaot evidens blong impoten intaraksen wetem rabis IP adres we oli save long hem. Maet se gud aktiviti ya we bin hapen long host ya, o netwok koneksen wetem tret akta infrastrakja i bin kasem host ya. Fasin blong aktiviti ya oli no save faenemaot wetem ol avelebol evidens be i soemaot se grup i aftarem blong muvum long saed i go insaed long netwok blong oganaesesen (TA0008).

Intenol host

ACSC blong ASD i bin investigetem limit data we i kam long intenol pat blong netwok blong oganaesesen. No sakses o saksesful rabis aktiviti we oli save long hem i bin givim kil long pat blong intenol netwok blong oganaesesen we i gat akses long VDI joen atifaks, wan pat blong wan intenol SQL seva (T1505.001), mo trafik we oli no save eksplenem we oli faenem taem oli go tru long ol rabis IP adres we oli save long hem tru long akses getawei aplaens (TA0011).

Wetem akses blong olgeta long kompromaes aplaens, grup i kolektem ol tru yusanem, paswod (T1003), mo ol MFA token valiu (T1111). Grup i kolektem tu ol JSON Web Token (JWTs) (T1528), we hemi wan autentikesen atifak we oli yusum blong krietem vituol desktop login sesen. Akta maet oli save yusum hemia ya blong krietem o haejakem vituol desktop sesen (T1563.002) mo aksesem

intenol pat blong oganaesesen netwok olsem wan tru yusa (T1078).

Akta tu i save yusum akses blong kompromaes aplaens blong skrasem wan SQL seva (T1505.001), we i stap insaed long intenol netwok blong oganaesesen. Ating akta i gat akses long data ya.

Evidens i avelebol long akses getawei aplaens we i soem se netwok trafik i bin hapen tru o long divaes ya we i kam long ol rabis IP adres we oli save long hem. Olsem we oli talem antap ya, hemia maet i soemaot se ol rabis saeba akta oli givim kil o yusum divaes ya, blong tantanem insaed long intenol netwok.

Investigesen taemlaen

Lis andanit ya i provaedem wan taemlaen blong ol ki aktiviti we oli faenem long taem blong investigesen.

Taem	Iven
Eprel 2022	Rabis IP adres we oli save long hem i intarak wetem akses getawei host HOST7. Kos blong intaraksen oli no save faenem.
Eprel 2022	Evri host, HOST1, HOST2 mo HOST3, oli bin kompromaes tru long wan rabis o ol rabis akta, mo oli putum ol web sel long ol host. Wan log fael oli bin krietem o jenisim smol long HOST2. Fael ya i gat tul blong kridensol we maet wan rabis akta nao i bin kasem. Olgeta ya /etc/security/opasswd mo ol fael /etc/shadow we oli jenisim long HOST1 mo HOST3, we oli soemaot se ol paswd oli bin jenisim. Evidens we i avelebol i stap long HOST1 i talem se paswd blong yusa 'sshuser' oli bin jenisim.
Eprel 2022	HOST2, oganaesesen i bin sadem daon hem. Moa web sel (T1505.003) oli bin krietem long HOST1 mo HOST3. HOST1 i bin eksperiensem SSH nogud fos tes long HOST3. Wan log fael oli bin jenisim (T1070) on HOST3. Fael ya i gat tul blong kridensol (T1078) we maet wan rabis akta nao i bin kasem. Oli bin kasem ol JWT (T1528) mo sendemaot long wan fael long HOST3. Oganaesesen nao i satem daon HOST3. Evri aktiviti afta long taem ya oli bin hapen long HOST1.
Eprel 2022	Moa web sel oli bin krietem long HOST1 (T1505.003). Ol bin kasem ol JWT mo oli sendemaot long wan fael long HOST1.
Eprel 2022	Moa web sel oli bin krietem long HOST1 (T1505.003), mo wan rabis IP adres we oli save long hem wetem host (TA0011). Wan rabis IP adres we oli save hemi intarak wetem akses getawei host HOST7.
Mei 2022	Wan rabis IP adres we oli save hemi intarak wetem akses getawei host HOST7 (TA0011). Wan autentikesen iven blong wan yusa i bin joen wetem wan rabis IP adres we oli save insaed long ol log long HOST1. Wan moa web sel oli bin krietem long host ya (T1505.003).
Mei 2022	Wan skrip long HOST1 wan akta i jenisim smol (T1543). Skrip ya i gat fangsen we i save skrapemaot data long wan intenol SQL seva.
Mei 2022	Wan moa log fael long HOST1 oli jenisim laswan (T1070). Fael ya i gat yusanem mo paswod pea blong netwok oganaesesen, we oli bilif se oli tru (T1078).
Mei 2022	Wan moa log fael oli jes jenisim (T1070). Fael ya i gat ol JWT we oli kolektem long HOST1.
Mei 2022	Moa web sel oli bin krietem long HOST1 (T1505.003). Long deit ya, oganaesesen i bin ripotem diskavari blong wan web sel wetem wan kriesen deit long Eprel 2022 long ACSC blong ASD
Mei 2022	Wan namba blong ol skrip oli bin krietem long HOST1, ingkludum wan we nem blong hem Log4jHotPatch.jar.
Mei 2022	Ol iptebol-sev koman oli bin yusum blong adem tu open pot long akses getawei host. Ol pot hemi 9998 mo 9999 (T1572).

Ol akta taktik mo teknik

Haelaet andanit ya oli sam taktik mo teknik we oli faenemaot long taem blong investigesen.

Fas Akses

T1190 Eksploit Pablik Fesing Aplikesen

Grup ya maet i bin mekyus long RCE, stret inkris, mo autentikesen we i go raon long ol wik long rimot akses login mo aedentifaem manejmen prodak blong kasem fas akses long netwok.

Fas akses wei hemi stret from olgeta samting ya:

- Seva hemi wik long ol CVE long taem ya;
- Oli bin traem blong yusum ol wiknes ya long ol akta infrastrakja we oli save; mo
- Fas intenol rabis aktiviti we oli save i bin hapen sot taem nomo afta long tes we oli bin traem blong mekem.

Eksekiusen

T1059.004 Koman mo Skrip Intapreta: Uniks Sel

Grup i saksesfuli yusum gud ol wiknes antap ya bae i maet save ranem ol koman long wan Uniks sel we i avelebol long aplaens we i kil ya. Komplit ditel blong ol koman we ol akta oli ranem oli no save provaedem from oli no bin login tru long aplaens.

Pesistens

T1505.003 Seva Sofwea Komponen: Web Sel

Ol akta oli spredem sam web sel long ol aplaens we oli kil. Hemi posibol se plante difren akta oli spredem web sel, be wan smol namba blong ol akta nomo oli kondaktem aktiviti wetem ol web sel ya. Ol web sel maet oli letem difren koman eksekiusen tru long akta long ol kompromaes aplaens.

Janis inkris

T1068 Eksploitesen blong Inkris Janis

Avelebol evidens i no diskraebem level blong janis we ol akta oli save kasem. Be, sapos oli yusum web sel, ol akta oli save kasem wan level blong janis we i semak long hemia blong web seva long ol kompromaes aplaens. Ol wiknes oli bilif se oli bin stap long ol kompromaes aplaens we maet i save letem ol akta oli kasem ol stamba janis.

Kridensol Akses

T1056.003 Input Kapja: Web Potol Kapja

Evidens long ol kompromaes aplaens oli soemaot se akta i bin kapjarem sam handred yusanem, paswod pea, long klia teks, we oli bilif se oli tru. Ating se oli bin kapjarem olgeta ya wetem sam jenis long stret autentikesen proses we oli karemaot long ol kridensol blong wan fael.

T1111 Malti-Fakta Autentikesen Intasepsen

Akta i kapjarem tu valiu blong ol token blong MFA we i joen gud wetem ol login ya. Hemia maet se oli kapjarem tru long ol sam jenis long tru autentikesen proses blong karemaot ol valiu ya long wan fael. I nogat evidens long kompromaes blong 'sikret seva' we i storem ol tru valiu we i provaedem blong sekiuriti blong ol token blong MFA.

T1040 Netwok Snifing

Oli bilif se akta i kapjarem ol JWT taem hemi stap kapjarem HTTP trafik long kompromaes aplaens. I gat evidens se program tcpdump oli bin karemaot long kompromaes aplaens, maet hemia nao hao akta i bin kapjarem ol JWT ya.

T1539 Stil Web Sesen Kuki

Olsem oli tokbaot antap ia, akta i tekem JWT, we i semak long web sesen kuki. Olgeta ia akta i sapos blong yusum bakegen blong kasem moa akses.

Diskavari

T1046 Netwok Seves Diskavari

I gat pruv se netwok skaning program map oli bin stopem long kompromaes aplaeans blong skanem ol nara aplaeans long semak pat blong netwok. Hemia oli yusum tru long akta blong faenemaot ol nara netwok seves we oli save kasem we maet i soem ol janis blong laterol muvmen.

Koleksen

Pruv we i stap i no soem olsem wanem ol akta oli kolektem data o wanem stret oli kolektem aot long kompromaes aplaeans o aot long ol sistem. Be, hemi olsem se ol akta oli gat akses long evri fael long kompromaes aplaeans, wetem ol kridensol we oli kapjarem (T1003), ol valiu token blong MFA (T1111), mo ol JWT we oli tokabot antap ia.

Koman mo kontrol

T1071.001 Aplaeans Leia Protokol: Web Protokol

Ol akta oli yusum web sel blong givim koman mo kontrol. Web sel koman i save pas ova long HTTPS tru long web seva we i stap long aplaeans (T1572).

T1001.003 Data Obfuskesen: Protokol Imitesen

Akta i yusum ol divaes olsem wan lonjing poen blong ol atak we oli disaenem blong joenem wetem tru tafik.

Diteksen mo mitigesen rekomendesen

ACSC blong ASD i rekomendem strong blong implementem ASD Essential Eight blong Kontrol mo konek wetem Strategies blong Mitigate Cyber Security Incidents. Andanit hemi ol rekomendesen blong netwok sekiuriti aksen we i mas tekem aksen blong ditektem mo protektem ol indastri tru long APT40, folem stret mitigesen blong fo ki TTP we oli samaraesem long Tebol 1.

Diteksen

Sam long ol fael we oli soem antap ia oli dropem long sam ples olsem C:\Users\Public* and C:\Windows\Temp*. Ol ples ia oli ol gud ples blong raetem data from oli wol raetabol, we i stap, evri akaon yusa oli rejista long windo, gat sakses long ol daerektori mo sabdaerektori blong olgeta. Plante taem, eni yusa oli gat akses long fael smol taem afta, we i letem ol janis blong saed muvmen, difens evasen, smol janis blong eksekiusen mo mekem eksfiltrasen.

Ol Sigma rul we oli stap ia oli stap lukaot long eksekiusen aot long ol saspes ples olsem wan saen blong abnomol aktiviti. Long ol taem ya, ol fiuja investigesen i nidim blong konfomem rabis aktiviti mo klasifikesen.

Taetol: Wol Raetabol Eksekiusen-Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Diskripsen: Ditektem proses eksekiusen we i kam long C:\Windows\Temp.

Bakgraon:

Ol rul ia oli mekem i stret blong eksekiutum aot long C:\Windows\Temp*. Benign aplikesen i yusum bigwan Temp mo hemia i wan rabis saen bitim eksikusen blong eksekiusen aot long ol nara wol raetebol sabdaerektori long C:\Windows.

Blong karemaot ol aplikesen tru long SISTEM o NETWOK SEVES yusa, hemi save katemdaon kwantiti blong benign aktiviti we oli selektem tru long rul ia.

Hemia i minim se rul i save mestem ol rabis eksekiusen long wan hae level be oli rekomendem blong yusum ol nara rul blong faenemaot sapos wan yusa i stap traem blong leftemap ol janis blong SISTEM.

Investigesen:

1. Jekem infomesen we i joen daerek wetem fael eksekiusen, olsem yusa konteks, eksekiusen level we i tru, foloap semtaem long aktiviti mo ol imej we oli lodem tru long fael.
2. Investigetem long proses ya, netwok, fael mo ol nara sapot data long host blong help blong mekem wan asesmen long weta sapos aktiviti ya i nogud.
3. Sapos i gat nid blong kolektem wan kopi blong fael blong rives enjiniaring blong faenemaot sapos hemi tru.

Refrens:

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

Man we i raetem: ACSC blong ASD

Deit: 2024/06/19

Taetol: tes

Tag:

- tlp.grin
- classification.au.official
- atak.eksekiusen

Log Sos:

```
kategori: proses_kriesen
prodak: windo
```

Diteksen:

```
temp:
    Pikja|istatwetem: '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}\}\\'
sistem_yusa:
    Yusa:
    - 'SISTEM'
    - 'NETWOK SEVES'
```

dismhost:

Image|endswith: 'dismhost.exe'

save_parent:

ParentImage|endswith:

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

kondisen: temp mo no (semmak_temp_wei or sistem_yusa o dismhost o known_parent)

Fols positif:

- Alaolis oditing aplikesen oli bin stap lukluk long eksekiutif we i stap ron aot long ol daerektori ya.
- Folem loa, Temp bae holem wan koleksen blong setemap ol aplikesen mo lonja, bae i gat praes blong tingting long olsem wanem fasin ia oli stap lukluk gud netwok blong hem (mo sapos oli save alaoemlist o no) bifo oli yusum rul ia.

Level: lo

Taetol: Wol Raetabol Eksekiusen - No-Temp Sistem Sabdaerektori

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

Diskripsen: Ditektem proses eksekiutif aot long wan wol raetabol long wan sabdaerektori blong Windows OS instol lokesen.

Bakgraon:

Rul ia hemi speseli blong wol raetabol daerektori we i stap insaed long C:\ mo speseli C:\Windows*, wetem eksepsen blong C:\Windows\Temp (we oli yusum fulap tru long benign aplikesen mo olsem ia nao i sloem konfidens blong ol rabis saen).

Appdata folda oli no adem sapos wan fael i bin ran tru olsem SISTEM–hemia i wan wei blong benign we plante temporari fael oli spolem.

Afta we wan inisol netwok beslaen i finis mo soem benign eksekiusen we yumi save aot long ol ples ia, wanwan taem rul ia i mas karemaot.

Investigesen:

1. Jekem infomesen we i joen daerek wetem fael eksekiusen, olsem yusa konteks, eksekiusen level we i tru, foloap semtaem long aktiviti mo ol imej we oli lodem tru long fael.
2. Investigetem long proses ya, netwok, fael mo ol nara sapot data long host blong help blong mekem wan asesmen long weta sapos aktiviti ya i nogud.
3. Sapos i gat nid blong kolektem wan kopi blong fael blong rives enjiniaring blong faenemaot sapos hemi tru.

Refrens:

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

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

Man we i raetem: ACSC blong ASD

Deit: 2024/06/19
Taetol: tes

Tag:

- tlp.grin
- classification.au.official
- atak.eksekiusen

Log sos:

Kategori: proses_kriesen

prodak: windo

Diteksen:

writable_path:

Imej|konden:

- ':\\$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:

Imej|konden: '\\AppData\\'
Yusa: 'SISTEM'

kondisen: raetebol, we imo i no apdeta

Fols positif:

Alaolis oditing aplikesen oli bin stap lukluk long eksekiutif we i stap ron aot long ol daerektori ya.

Samtaem i posibol blong skrip mo administretif tul oli yusum long ples we oli stap jekem samtaem long wan long ol daerektori mo oli sud adresem long wan keis tu keis sistem.

Level: hae

Taetol: Wol Raetabol Eksekiusen - Yusa

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

Diskripsen: Ditektem proses eksekiusen long C:\Users\Public* mo nara wol raetabol folda insaed long ol Yusa.

Bakgraon:

Appdata folda oli no adem sapos wan fael i bin ran tru olsem SISTEM–hemia i wan wei blong benign we plante temporari fael oli spolem.

Investigesen:

1. Jekem infomesen we i joen daerek wetem fael eksekiusen, olsem yusa konteks, eksekiusen level we i tru, foloap semtaem long aktiviti mo ol imej we oli lodem tru long fael.
2. Investigetem long proses ya, netwok, fael mo ol nara sapot data long host blong help blong mekem wan asesmen long weta sapos aktiviti ya i nogud.
3. Sapos i gat nid blong kolektem wan kopi blong fael blong rives enjiniaring blong faenemaot sapos hemi tru.

Refrens:

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

Man we i raetem: ACSC blong ASD

Deit: 2024/06/19

Taetol: tes

Tag:

- tlp.grin
- classification.au.official
- atak.eksekiusen

Log sos:

kategori: proses_kriesen

```
    prodak: windo
```

Diteksen:

```
    ol yusa:
        Imej|konden:
        - ':\\Users\\All Users\\'
        - ':\\Users\\Contacts\\'
        - ':\\Users\\Default\\'
        - ':\\Users\\Public\\'
        - ':\\Users\\Searches\\'
    Appdata:
        Imej|konden: '\\AppData\\'
        Yusa: 'SISTEM'
    Kondisen: yusa mo i no appdata
```

Fols positif:

- Maet i tru se ol skrip mo administretif tul we oli yusum long ol monita ples maet i stap long Pablik o wan sabdaerektori mo oli sud adresem long wan keis tu keis fasin.

Level:midium

Mitigesen

Loging

Long taem blong ACSC blong ASD, wan komon isu i save katemdaon paoa mo spid blong wan wok blong investigesen olsem wan sot blong save mo historikol loging infomesen akros long wan namba blong eria we i gat web seva rikwes log, Window iven log mo intanet proksi log.

ACSC blong ASD i rekomendem riviu mo implementem gaedens blong olgeta long Windows Events Logging and Forwarding we hemi ingkludum konfigeresen blong ol fael mo skrip long Windows Event Logging Repository mo Information Security Manual's Guidelines blong System Monitoring, blong ingkludum sentrol log mo riten log blong wan stret taem.

Paj manejmen

Pajem kwik evri intanet ekspos divaes mo seves, we hemi gat tu web seva, web aplikesen, mo rimot akses getawei. Lukluk blong statem wan sentrolaes paj manejmen sistem blong jenisim mo spidim proses. ACSC blong ASD hemi rekomendem implimentesen blong ISM Gaedlaen blong System Management, speseli, System Patching kontrol we oli avelebol.

Plante kil we akta oli yusum pablik i save long hem mo oli gat paj o mitigesen avelebol. Ol oganaesesen oli sud mekem sua se sekiuriti paj o mitigesen oli aplae long intanet fesing infrastrakja long wan 48 haoa taem, mo taem i posibol, yusum letes vesen blong sofwea mo opereting sistem.

Netwok segmentesen

Netwok segmentesen hemi save mekem hemi moa had blong ol rabis man blong loketem mo kasem akses long wan oganaesesen blong ol pesenol data. Segmen netwok blong limit o blokem laterol muvmen hemi taem oli dinaem trafik bitwin ol kompiuta sapos oli nidim nomo. Impoten seva olsem Active Directory mo ol nara autentikesen seva oli sud save aplaem long wan limit namba blong ol medel seva o 'jam seva'. Oli sud stap monitarem gud ol seva ya, oli sekiua gud mo limitim wij yusa mo divaes nao oli save konek long olgeta.

Nomata long ol taem we oli talem we laterol muvmen oli priventem, moa netwok segmentesen oli save seftem limit namba blong data we oli akta nao oli save aksesem mo tekemaot.

Moa mitigesen

Otoring ejensi i rekomendem tu olgeta mitigesen ya blong faetem APT40 mo ol nara yus blong TTP andanit.

- Jenisim netwok seves, pot mo ol protokol we oli no yusum o no nidim.
- Yusum ol gudfala Web application firewallsl (WAF) blong protektem web seva mo aplikesen.
- Fosem ol smol janis blong limitim akses long ol seva, fael sea, mo ol nara risos.
- Yusum maltae-fakta autentikesen (MFA) mo manejem seves akaon blong mekem ol kridensol oli had blong krakem mo yusum bakegen. MFA oli sud aplaem long evri intanet aksesebol rimot akses seves, we i gat tu:
    - Web mo klaod beis imel
    - Kolaboresen platfom
    - Vituol praevet netwok koneksen
    - Rimot desktop seves
- Riplesem en blong laef tul

Tebol 1. Mitigesen Plan/Teknik

TTP	Essential Eight Mitigation Strategies	ISM Kontrol
Fas Akses T1190 Eksploitesen blong Pablik-Fesing Aplikesen	Paj Aplikesen Paj opereting sistem Maltae-Fakta-Autentikesen Aplikesen kontrol	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Eksekiusen T1059 Koman mo Skrip Intapreta	Aplikesen kontrol Ristrik Microsoft Office makro Ristrik administretif janis	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Pesistens T1505.003 Seva Sofwea Komponen: Web Sel	Aplikesen Kontrol Ristrik administretif janis	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Fas Akses/Janis Inkris/ Pesistens T1078 Tru Akaon	Paj opereting sistem Maltae-Fakta-Autentikesen Ristrik administretif janis Aplikesen kontrol Yusa aplikesen set	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

Blong moa jenerol dideksen mo mitigesen advaes, plis konsaltem Mitigesen mo Diteksen seksen blong MITRE ATT&CK teknik web pej blong wanwan teknik we oli faenemaot ya long MITRE ATT&CK samari long en blong advaesori ya.

Disklema

Infomesen insaed long ripot ia mifala i givim “olsem we i stap” blong infomesenal pepes nomo. Ol otoring ejensi oli no endosem eni komesol entiti, prodak, kampani, o seves, ingkludum eni entiti, prodak, o seves we i go joen wetem dokumen ya. Eni refrens long sam spesel komesol bisnes, prodak, proses, o seves tru long seves mak, tredmak, manufaktara, o no, hemi no mekem o soemaot, rekomendesen, o konfem tru long ol raet ejensi.

Dokumen ya oli makem TLP:CLEAR. Disklosa hemi nogat limit long hem. Ol sos oli save yusum TLP:CLEAR taem infomesen hemi karem smol o no luk ris blong misyus, we hemi go wetem ol rul we oli aplae mo ol proses blong pablik rilis. Oli open long ol standet copyright rul, TLP:CLEAR infomesen maet oli distributem witaot ristriksen. Blong moa infomesen long Traffic Light Protocol, luk cisa.gov/tlp

MITRE ATT&CK – Historikol APT40 tredkraf blong interes

Rekonesons (TA0043)	
Sej Viktim-On Websaet (T1594)	Kasem Viktim Aedentiti Infomesen: Kridensol (T1589.001)
Aktif Skaning: Wik Skaning (T1595.002)	Kasem Viktim Host Infomesen (T1592)
Sej Open Websaet/Domen: Sej Enjin (T1593.002)	Kasem Viktim Netwok Infomesen: Domen Propeti (T1590.001)
Kasem Viktim Aedentiti Infomesen: Imel Adres (T1589.002)	

Risos Developmen (TA0042)	
Kasem Infrastrakja: Domen (T1583.001)	Kasem Infrastrakja (T1583)
Kasem Infrastrakja: DNS Seva (T1583.002)	Kompromaes Akaon (T1586)
Developem ol Paoa: Kod Saening Setifiket (T1587.002)	Kompromaes Infrastrakja (T1584)
Developem ol Paoa: Digitol Setifiket (T1587.003)	Developem ol Paoa: Malwea (T1587.001)
Kasem ol Paoa: Kod Saening Setifiket (T1588.003)	Openem Akaon: Klaod Akaon (T1585.003)
Kompromaes Infrastrakja: Netwok Divaes (T1584.008)	Kasem ol Paoa: Digitol Setifiket (T1588.004)

Fas Akses (TA0001)	
Tru Akaon (T1078)	Fising (T1566)
Tru Akaon: Difol Akaon (T1078.001)	Fising: Spiafising Atajmen (T1566.001)
Tru Akaon: Domen Akaon (T1078.002)	Fising: Spiafising Link (T1566.002)
Ekstenol Rimot Seves (T1133)	Eksploit Pablik-Fesing Aplikesen (T1190)
Draev-bae Kompromaes (T1189)	

Eksekiusen (TA0002)	
Windows Management Instrumentation (T1047)	Koman mo Skrip Intapreta: Python (T1059.006)
Skeduol Wok: Long (T1053.002)	Koman mo Skrip Intapreta: JavaScript (T1059.007)
Skeduol Wok: Skeduol Wok (T1053.005)	Netif API (T1106)
Koman mo Skrip Intapreta (T1059)	Inta-Proses Komunikesen (T1559)
Koman mo Skrip Intapreta: Windows Koman Sel (T1059.003)	Sistem Seves: Seves Eksekiusen (T1569.002)
Koman mo Skrip Intapreta: PaoaSel (T1059.001)	Eksploitesen blong Klaen Eksekiusen (T1203)
Koman mo Skrip Intapreta: Visuol Besik (T1059.005)	Yusa Eksekiusen: Rabis Fael (T1204.002)
Koman mo Skrip Intapreta: Uniks Sel (T1059.004)	Koman mo Skrip Intapreta: Apple Skrip (T1059.002)
Skeduol Wok: Kron (T1053.003)	Sofwea Diploimen Tul (T1072)

Pesistens (TA0003)	
Tru Akaon (T1078)	Seva Sofwea Komponen: Web Sel (T1505.003)
Ofis Aplikesen Setap: Ofis Templet Makros (T1137.001)	Kriet o Modifae Sistem Proses: Windows Seves (T1543.003)
Skeduol Wok: Long (T1053.002)	But o Login Otostat Eksekiusen: Rejistri Ran Ki/Statap Folda (T1547.001)
Skeduol Wok: Skeduol Wok (T1053.005)	But o Login Otostat Eksekiusen: Sotkat Modifikesen (T1547.009)
Ekstenol Rimot Seves (T1133)	Haejak Eksekiusen Flo: DLL Sej Oda Haejak (T1574.001)
Skeduol Wok: Kron (T1053.003)	Haejak Eksekiusen Flo: DLL Saed-Loding (T1574.002)
Akaon Manipulesen (T1098)	Tru Akaon: Klaod Akaon (T1078.004)
Tru Akaon: Domen Akaon (T1078.002)	

Janis Eskelesen (TA0004)	
Skeduol Wok: Long (T1053.002)	Kriet o Modifae Sistem Proses: Windows Seves (T1543.003)
Skeduol Wok: Skeduol Wok (T1053.005)	But o Login Otostat Eksekiusen: Rejistri Ran Ki/Statap Folda (T1547.001)
Proses Injeksen: Tred Eksekiusen Haejak (T1055.003)	But o Login Otostat Eksekiusen: Sotkat Modifikesen (T1547.009)
Proses Injeksen: Proses Halo (T1055.012)	Haejak Eksekiusen Flo: DLL Sej Oda Haejak (T1574.001)

Janis Eskelesen (TA0004)	
Tru Akaon: Domen Akaon (T1078.002)	Eksploitesen blong Janis Eskelesen (T1068)
Akses Token Manipulesen: Token Impesonesen/Stil (T1134.001)	Iven Triga Eksekiusen: Uniks Sel Konfigeresen Modifikesen (T1546.004)
Proses Injeksen: Dynamik-link Laebrari Injeksen (T1055.001)	Tru Akaon: Domen Akaon (T1078.002)
Tru Akaon: Lokol Akaon (T1078.003)	

Difens Evesen (TA0005)	
Rutkit (T1014)	Indaerek Koman Eksekiusen (T1202)
Obfusketed Fael o Infomesen (T1027)	Sistem Baeneri Proksi Eksekiusen: Mshta (T1218.005)
Obfusketed Fael o Infomesen: Sofwea Paking (T1027.002)	Sistem Baeneri Proksi Eksekiusen: Regsvr32 (T1218.010)
Obfusketed Fael o Infomesen: Steganografi (T1027.003)	Korap Tras Kontrol: Kod Saening (T1553.002)
Obfusketed Fael o Infomesen: Kompael Afta Diliveri (T1027.004)	Fael mo Daerektori Pemisen Modifikesen: Linux mo Mac Fael mo Daerektori Pemisen Modifikesen (T1222.002)
Maskared: Maj Tru Nem mo Lokesen (T1036.005)	Vituolaesesen/Sanbokis Evesen: Sistem Jek (T1497.001)
Proses Injeksen: Tred Eksekiusen Haejak (T1055.003)	Maskared (T1036)
Riflektif Kod Loding (T1620)	Impea Difens: Disebol o Modifae Sistem Faeawol (T1562.004)
Proses Injeksen: Proses Halo (T1055.012)	Haed Atifaks: Haed Fael mo Daerektori (T1564.001)
Indiketa Rimuvol: Fael Dilitsen (T1070.004)	Haed Atifaks: Haed Window (T1564.003)
Indiketa Rimuvol: Taemstomp (T1070.006)	Haejak Eksekiusen Flo: DLL Sej Oda Haejak (T1574.001)
Indiketa Rimuvol: Klia Windows Iven Log (T1070.001)	Haejak Eksekiusen Flo: DLL Saed-Loding (T1574.002)
Modifae Rejistri (T1112)	Web Seves (T1102)
Deobfusket/Dikod Fael o Infomesen (T1140)	Maskared: Maskared Wok o Seves (T1036.004)
Impea Difens (T1562)	

Kridensol Akses (TA0006)	
OS Kridensol Damping: LSASS Memori (T1003.001)	Ansekiua Kridensol: Kridensol long Fael (T1552.001)
OS Kridensol Damping: NTDS (T1003.003)	Rabis Fos: Paswod Gesing (T1110.001)
Netwok Snifing (T1040)	Fos Autentikesen (T1187)

Kridensol Akses (TA0006)	
Kridensol long ol Paswod Stoa: Kijen (T1555.001)	Stil o Foj Kerberos Tiket: Kerberroasting (T1558.003)
Input Kapja: Kilogin (T1056.001)	Maltae-Fakta Autentikesen Intasepsen (T1111)
Stil Web Sesen Kuki (T1539)	Stil Aplikesen Akses Token (T1528)
Eksploitesen blong Kridensol Akses (T1212)	Rabis Fos: Paswod Kraka (T1110.002)
Input Kapja: Web Potol Kapja (T1056.003)	OS Kridensol Damping: DCSik (T1003.006)
Kridensol long ol Paswod Stoa (T1555)	Kridensol long ol Paswod Stoa: Kridensol long ol Web Braosa (T1555.003)

Diskavari (TA0007)	
Sistem Seves Diskavari (T1007)	Sistem Infomesen Diskavari (T1082)
Aplikesen Window Diskavari (T1010)	Akaon Diskavari: Lokol Akaon (T1087.001)
Kwestin Rejistri (T1012)	Sistem Infomesen Diskavari, Teknik T1082-Entapraes | MITRE ATT&CK®
Fael mo Daerektori Diskavari (T1083)	Sistem Taem Diskavari (T1124)
Netwok Seves Diskavari (T1046)	Sistem Ona/Yusa Diskavari (T1033)
Rimot Sistem Diskavari (T1018)	Domen Tras Diskavari (T1482)
Akaon Diskavari: Imel Akaon (T1087.003)	Akaon Diskavari: Domen Akaon (T1087.002)
Sistem Netwok Koneksen Diskavari (T1049)	Vituolaesesen/Sanbokis Evesen: Sistem Jek (T1497.001)
Proses Diskavari (T1057)	Sofwea Diskavari (T1518)
Pemisen Grup Diskavari: Domen Grup (T1069.002)	Netwok Sea Diskavari, Teknik T1135 - Entapraes | MITRE ATT&CK®
Sistem Netwok Konfigaresen Diskavari: Intanet Koneksen Diskavari (T1016.001)	

Laterol Muvmen (TA0008)	
Rimot Seves: Rimot Desktop Protokol (T1021.001)	Rimot Seves (T1021)
Rimot Seves: SMB/Windows Admin Sea (T1021.002)	Yusum Nara Autentikesen Tul: Pasem Tiket (T1550.003)
Rimot Seves: Windows Rimot Manejmen (T1021.006)	Laterol Tul Tranfea (T1570)

Koleksen (TA0009)	
Data long Lokol Sistem (T1005)	Akaef Data Koleksen: Akaef tru long Laebrari (T1560.002)
Data long Netwok Sea Draev (T1039)	Imel Koleksen: Rimot Imel Koleksen (T1114.002)

Koleksen (TA0009)	
Input Kapja: Kilogin (T1056.001)	Klipbod Data (T1115)
Otomatik Koleksen (T1119)	Data long Infomesen Fasiliti (T1213)
Input Kapja: Web Potol Kapja (T1056.003)	Data Stej: Rimot Data Stejing (T1074.002)
Data Stej: Lokol Data Stejing (T1074.001)	Akaef Koleksen Data (T1560)
Imel Koleksen (T1114)	

Eksfiltresen (TA0010)	
Eksfiltresen Ova C2 Janel (T1041)	Eksfiltresen Ova Nara Protokol: Eksfiltresen Ova Asimetrik Enkrip No-C2 Protokol (T1048.002)
Eksfiltresen Ova Nara Protokol (T1048)	Eksfiltresen Ova Web Seves: Eksfiltresen long Klaod Storej (T1567.002)

Koman mo Kontrol (TA0011)	
Data Obfuskesen: Protokol Impesonesen (T1001.003)	Web Seves: Ded Drop Risolva (T1102.001)
Komon Yus Pot (T1043)	Web Seves: Wan-wei Komunikesen (T1102.003)
Aplikesen Leya Protokol: Web Protokol (T1071.001)	Ingres Tul Transfea (T1105)
Aplikesen Leya Protokol: Fael Transfea Protokol (T1071.002)	Proksi: Intenol Proksi (T1090.001)
Proksi: Ekstenol Proksi (T1090.002)	Non-Standet Pot (T1571)
Proksi: Maltae-hop Proksi (T1090.003)	Protokol Tanel (T1572)
Web Seves: Baedaereksonal Komunikesen (T1102.002)	Enkrip Janel (T1573)
Enkrip Janel: Asimetrik Kriptografi (T1573.002)	Ingres Tul Transfea (T1105)
Proksi, Teknik T1090-Entapraes | MITRE ATT&CK®	

Impak (TA0040)	
Seves Stop (T1489)	Disk Waep (T1561)
Sistem Satdaon/Ribut (T1529)	Risos Haejak (T1496)

Not (ol)

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.

Yus blong Coat of Arms

Ditel blong ol kondisen we man i mas folem blong yusum Coat of Arms hem i stap long Department of the Prime Minister and Cabinet websaet Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

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