Faufautuaga APT40

PRC MSS auala faapitoa o tomai e fai ai a latou galuega

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**

Fua faatatau o mea o i totonu

Vaaiga Lautele

Mea o i tua atu

O lenei faufautua, na tusia ma faatonuina e le Australian Signal Directorate's Australian Cyber Centre (ASD's ACSC), o le United States Cybersecurity ma le Infrastructure Security Agency (CISA), le United States National Security Agency (NSA), le United States Federal Bureau of Investigation (FBI), le United Kingdom National Cyber Security Centre (NCSC-UK), le Canadian Centre mo Cyber Security (CCCS), le New Zealand Cyber Security Centre (NCSC-NZ), le German Federal Intelligence Service (BND), ma le Federal Office mo le Protection o le Constitution (BfV), le Republic o Korea's National Intelligence Service (NIS), ma le NIS' National Cyber Security Center, Ma le Japan's National Center of Incident Readiness ma Strategy mo le Cybersecurity (NISC), ma le National Police Agency (NPA) - mulimuli ane ua faasinoina faapea o "faalapotopotoga e faavaeina polokalame" - ua 'oto'otoina se People Republic of China (PRC) kulupu initaneti o loo lagolagoina e le setete ma lo latou faamata'u o i ai nei i auala o faasalalauga i Ausetalia. E aumai e le faufautua malamalamaga faasoa a faalapotopotoga e tusia ma faatonutonuina o faamata'u faapea suesuega i le tali atu i mea e tutupu mai a le ASD's ACSC.

O le kulupu initaneti e lagolagoina e le setete o le PRC na taula'i talu ai ni faalapotopotoga i atunuu eseese, e aofia ai Ausetalia ma le Iunaite Setete, ma o auala na fai ai o loo faamatamata tetele i lalo ifo e masani ona fa'aaoga e isi tagata e faatinoina na lagolagoina e le setete PRC i le lalolagi. O le mea lea, o faalapotopotoga faufautua na talitonu o se kulupu, ma auala na fai ai e tali tutusa e tumau pea o se faamata'u foi i isi auala o faasalalauga a le latou atunuu.

Na maua e faalapotopotoga faufautua faapea o lenei kulupu e faatautaia gaioiga matu'ia o initaneti mo le PRC Ministry of State Security (MSS). O gaioiga ma auala e fai ai na ova atu i le tuliloaina e le kulupu faapea o le Advanced Persistent Threat (APT) 40 (faapea foi ona iloa o le Kryptonite Panda, GINGHAM TYPHOON, Leviathan ma Bronze Mohawk i lipoti o falefaigaluega). O lenei kulupu na lipotia talu ai faapea sa faamautu i Haikou, Hainan Province, PRC ma sa maua faatonuga mai le PRC MSS, Hainan State Security Department.[2] O Faufautua nei na tuuina mai se faataitaiga o suesuega o mataupu iloga o lenei auala o faiga leaga e faasaga i auala o faasalalauga e lua ua afaina. O suesuega o mataupu o taunu'uga mo tagata tomai e faavaeina le malu puipuia o initaneti ina ia faailoaina, foia ma faaleleia le osofaia o APT40 e faasaga i a latou lava auala o faasalalauga. O suesuega o mataupu filifilia o i latou faapea e talafeagai le faaleleia sa faia e tuuitiitia ai lamatiaga o le toe mauaina e le tagata e faatinoina faamata'u, po o isi. E pei o lea, o suesuega o mataupu e sili atu le matua i le natura, ina ia mautinoa ua tuuina atu i faalapotopotoga taimi e tatau ai ina ia faaleleia ai.

Tuufaatasiga o Gaioiga

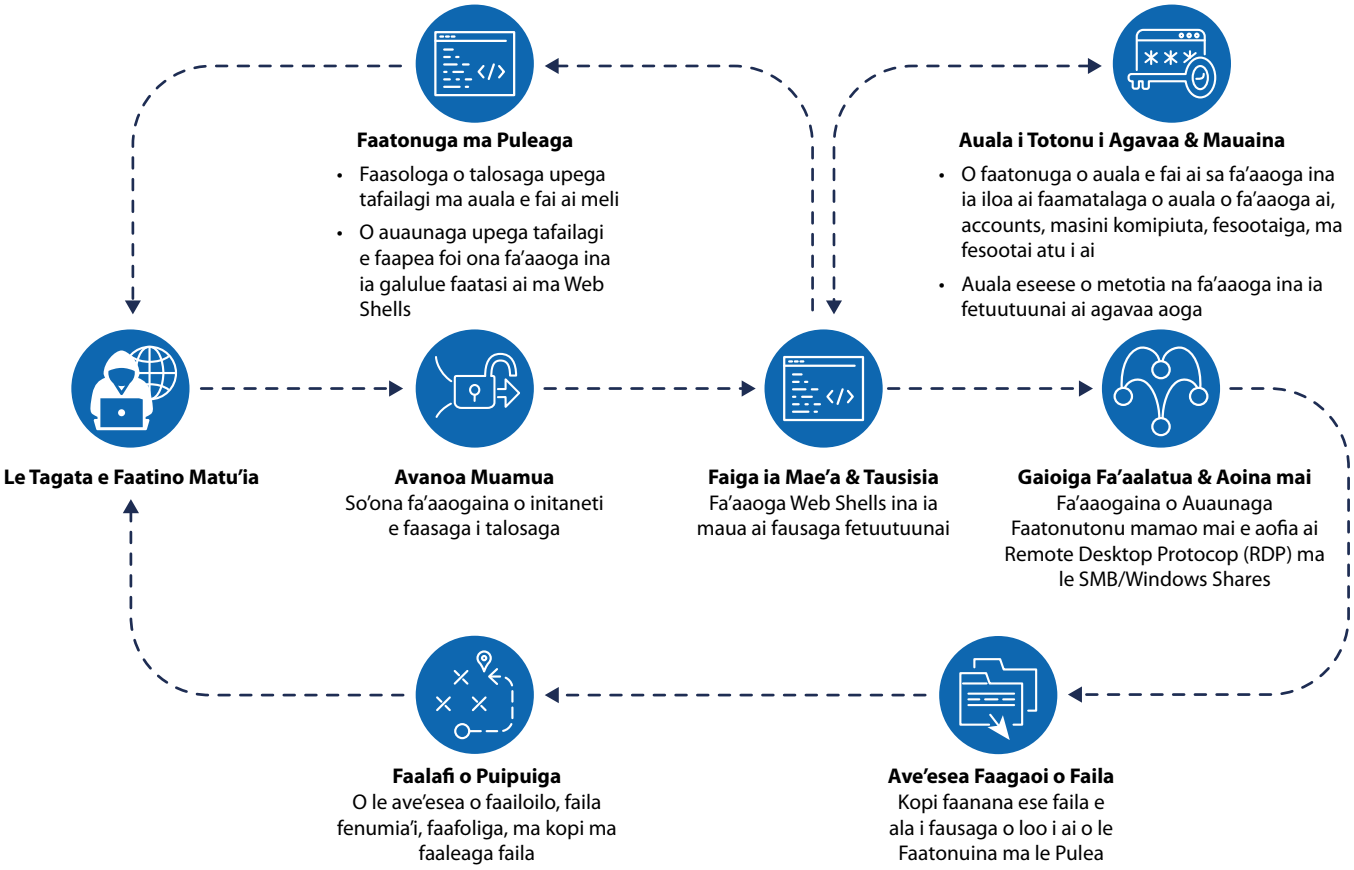
O le APT40 na faafia ona taula'i e auala o faasalalauga a Ausetalia faapea le malo ma auala o faasalalauga tuma'oti i pitonuu, ma o le faamata'u o loo latou faia i a tatou auala o faasalalauga o loo faifai pea. O auala e fai ai ma tomai na faamatalaina i lenei faufautua e masani ona maitauina e faasaga i auala o faasalalauga a Ausetalia.

Aemaise ai lava, e umia e le APT40 le mafai ina ia faaliliuina malie ai ma liliu atu e fa'aaoga faamaoniga o manatu (POCs) o vaivaiga fou ma vave ona fa'aaoga i latou e faasaga agai i auala o faasalalauga o umia fausaga o vaivaiga e faatatau i ai. E masani ona faatautaia e le APT40 suesuega e faasaga i auala o faasalalauga na fiafia i ai, e aofia ai faalapotopotoga na faavaeina a atunuu, na vaavaai i ai o fetuutuunai ai ana taulai. O lenei suesuega masani o tulaga a le kulupu ina ia iloa ai vaivaiga, faamutaina o le aoga po o masini ua le toe tausisia i luga o mea e fiafia i ai faasalalauga, ma ina ia faifai malie ona faatonutonuina e fa'aaoga. E fa'aauau e le APT40 ona maua faamanuiaga i le fa'aaogaina o mea vaivai mai le vave o tausaga e pei o le 2017.

O le APT40 e masani ona fa'aaogaina faalauaitele mea vaivai fou o loo tele ina fa'aaoga i polokalame komipiuta e pei o Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) ma le Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473). O le ASD's ACSC ma faalapotopotoga e faavaeina e vaavaai i le kulupu ina ia fa'aauau ona fa'aaoga le POC mo mea fou e iloa ai vaivaiga i totonu o itula po o aso o le faamatuuina faalauaitele.

2 U.S. Matagaluega o Faamasinoga. 2021 E toafa Tagata Saina Na Galulue i le Ministry State Security na Faasalaina i le Faalauiloaina o le Faalavelave iKomipiuta a le Lalolagi o loo Mata'ituina Meatotino Tomai ma Faamatalaga Faalilolilo faa-Pisinisi, e Aofia ai Suesuega o Faamai Pipisi..

Figure 1: TTP o le siata faasolo mo gaioiga APT40



O lenei kulupu e fiafia e fa'aaoga mea vaivai, fausaga e faasaga faalauaitele i luga o auala e fai ai faapea e manaomia le galulue faatasi o tagata e fa'aogaina, e pei o faalauiloa o imeli pepelo, ma tuuina atu se faamuamua maualuga i le mauaina mai o faamatalaga taua ina ia mafai ai se faagasologa e mulimulitaia ai gaioiga. E masani ona fa'aaoga e le APT40 se faila matau'ia le leaga e faafoliga (T1505.003) mo le fa'aauauina, aemaise ai lava taimi muamua i le faagasologa o se osofaiga. E masani lava, a uma ona faamau ia sao muamua i totonu e taulai le APT40 i le faavaeina o le fa'aauau ai pea ina ia tausisia le mauaina o siosiomaga o i latou ua afaina. Ae peita'i, e pei ona faifaipea le tulai vave mai o se osofaiga, e sili atu ai le maitauina uma o osofaiga uma – e tusa lava po o le a le tele o le fetuutuunai po o isi gaioiga e fai.

Aemaise ai lava tomai ma metotia e fai ai auala e le lelei

E ui sa fa'aaoga talu ai e le APT40 e fetuutuunai ai upega tafailagi a Ausetalia e pei ona faatonutonuina ma pulea (C2) komipiuta mo ana faagaioiga, na faia e le kulupu lenei auala e fai ai (T1594).

Na talia lelei le APT40 auala o le fa'aaogaina e le lalolagi o masini ua fetuutuunaia, e aofia ai masini i ofisa laiti/ofisa i aiga (SOHO), e pei o fausaga e faatinoina ma toe liliu ese o se mea mulimuli (T1584.008) mo lona faatinoina i totonu o Ausetalia. O lea ua mafai ai e faalapotopotoga na faavaeina ina ia sili atu le faamatalaina ma tulituliloaina gaioiga a le kulupu lenei.

O le tele o nei masini SOHO ua uma le aoga po ua le faamaopoopoina na ofoina mai ai se taulai faigofie mo le fa'aaogaina i le N-day. O le taimi lava e fetuutuunai ai, o masini SOHO e ofoina atu se tulaga e faalauiloa ai mo osofaiga faapea ua faataatia ina ia mili faatasi ai i totonu ma feoaiga moni ma luitai ai feteenaiga ma fesootaiga (T1001.003).

O lea faiga e fai ai e faapea foi ona masani ona fa'aaoga e isi PRC e lagolagoina e le setete o i latou e faatinoina i le lalolagi atoa, ma ua vaavaai i ai faalapotopotoga e faavaeina faapea o se faasoaina o faamata'u. Mo faamatalaga fa'aopopo, tagai ane i fautuaga tuufaatasi Faalauiloaina o le Faalavelave iKomipiuta a le Lalolagi o loo Mata'ituina Meatotino Tomai ma Faamatalaga Faalilolilo faa-Pisinisi, e Aofia ai Suesuega o Faamai Pipisi ma le Lagolagoina e le Setete PRC o i Latou e Faatinoina le Fetuutuunau ma Tausisia le Maua Pea o Auala i Fausaga Ua i ai Faaletonu a le Iunaite Setete.

O nisi taimi o le APT40 e fa'aaoga mea ua maua po o fausaga na lisiina faapea o i latou ua afaina fausaga C2 i lona faatinoina; ae peitai, o lenei faiga o faatinoga e foliga mai e i'u ina te'ena.

Polokalame e fa'aaoga i komipiuta

O le ASD's ACSC o loo faasoaina nisi o faila matu'ia na iloa i taimi o suesuega o loo 'oto'otoina i lalo ifo. O nei faila na lolomiina i luga i VirusTotal ina ia mafai ai ona tete'e atu i fesootaiga lautele ma le puipuiga o komipiuta a le komiuniti ina ia sili atu le malamalama i faamata'u latou te manaomia ina ia tete'e atu i ai.

Suesuega o mataupu

O loo faasoaina e le ASD's ACSC lipoti faalilolilo e lua ina ia tuuina atu ai le iloa pe faapefea ona faafaigaluegaina e latou o faatinoina a latou mea faigaluega ma auala e faatino ai.

MD5	Igoa o le faila	Faamatalaga fa'aopopo
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

Suesuega o le mataupu 1

O lenei lipoti na faalilolilоina ina ia mafai ai faasalalauga faalauaitele. O le faalapotopotoga na afaina ua i ai nei ua faasino faapea ‘o le faalapotopotoga’. O nisi faamatalaga faapitoa na ave’esea ina ia puipuia ai mea e iloa ai le tagata ua afaina ma metotia e tali atu ai i mea na tulai mai i le ASD’s ACSC.

Aotelega o Mea aupito taua

O lenei lipoti o loo faamatalaina ai mea na maua i suesuega a le ASD’s ACSC i le faamanuiaina o fetuunaiga o fesootaiga a le faalapotopotoga i le va o lulai ma Setema 2022. O le suesueina o lenei lipoti na tuuina atu i le faalapotopotoga ina ia tuufaatasia gaioiga matu’ia na maitauina ma fautuaina le toe faaleleia. O mea na maua na iloa ai fetuutuunaiga sa faia e le APT40.

I le ogatotonu o Aukuso, na faailoa e le ASD’s ACSC le faalapotopotoga i faiga matu’ia o loo faia i a latou fesootaiga mai se masini e foliga mai ua fetuutuunai sa fa’aaogaina e le kulupu i le faaiuga o Aukuso ma, faatasi ai ma le faatagana a le faalapotopotoga, na faafaigaluega e le ASD’s ACSC o se polokalame komipiuta e maitauina ma iloilo faailoilo o komipiuta ua afaina i luga o fesootaiga a faalapotopotoga. O nei faailoilo e faatagaina le ASD’s ACSC mea e tali atu ai e auiliili ai ina ia faia e ala i se suesuega faafuainumera o sailiga. Fa’aaogaina o faamaumauga o faailoilo, e auiliili manuia ai e le ASD’s ACSC le faiga o faafanua o gaioiga a le kulupu ma fausia ai se taimi auiliili o le maitauina o mea fai.

Mai ia lulai ia Aukuso, o gaioiga autu a le tagata e faatinoina na maitauina e le ASD’s ACSC o loo aofia ai:

- komipiuta faanumeraina, faapea e mafai ai e le tagata o faatinoina ona fausia a latou lava faafanua o fesootaiga;
- Fa’aaogaina o se tusitusiga matu’ia le leaga, tuuina atu ai i le tagata o loo faatinoina le vae e muamua mau ai i totonu o le fesootaiga ma se mafai ona faataunuuina faatonuga; ma
- Faafaigaluegaina o isi mea faigaluega ia faaleleia ai e le tagata o loo faatinoina mo le faamoemoe ia faaleagaina.

O suesuega na maua ai faamaoniga tetele o faamaumauga ma’ale’ale na mauaina ma faamaoniga faapea na ave’esea fa’aalatua e ala i fesootaiga (T1021.002). O le tele o fetuutuunaiga sa faatautaia e ala i le faavaeina e le kulupu o le tele o faasologa faalausoso’o o fuainumera i totonu o fesootaiga, o le fesootaiga e lauga tasi lona faavae, ma le fa’aaogaina o polokalame komipiuta e le mautu lelei faapea e mafai ona fa’aaoga ina ia upload mai ai faila ma le fuafuaina. Faamaumauga e faanana ona to’esea e aofia ai mea e faamaonia ai faapea ua mafai ai e le kulupu ona log in, faapea foi faamatalaga o fesootaiga e faataga ai tagata o loo faatinoina ina ia toe maua ai ma le faatagaina pe afai sa poloka le faasologa muamua o fuainumera. E leai se mea faigaluega fa’aopopo komipiuta na maua i tua atu o mea na maua i le masini; ae peitai, o le mauaina e le kulupu o mea aoga ma le taua o le a ave’esea ai le manaoga mo mea faigaluega fa’aopopo. O mea na maua mai i suesuega na iloa ai o le faalapotopotoga na maitauina ma le faamoemoeina e le APT40, e pei ona tete’e atu faapea ua pa’u i avanoa ua afaina i se vaivaiga ua iloa faalauaitele.

Mea na maua mai suesuega

I le ogatotonu o Aukuso 2022, na faailoa ai e le ASD's ACSC le faalapotopotoga faapea o se IP matu'ia ua faamautuina na talitonuina e faifai mea faatasi ma le kulupu faamata'u e lagolagoina e le setete na faifai mea faatasi ma fesootaiga komipiuta a le faalapotopotoga i le va a itiiti ane a o lulai ma Aukuso. O le masini na fetuutuunai masalo e umia e se pisinisi laitiiti po o se tagata o loo fa'aaogaina mai le fale.

I le faaiuga o Aukuso, na fa'aaoga ai e le ASD's ACSC se komipiuta a se tagata o le faalapotopotoga ina ia fa'aaoga ai le fesootaiga a le faalapotopotoga faapea na iloa ai faamaoniga faapea ua afaina e ala i fetuutuunaiga.

O nisi mea moni faapea atonu e mafai ona lagolagoina ai taumafaiga e lei maua ona o le fetuunaiga o le saini i totonu po o le fausiaina o fesootaiga. E ui o lea, o le tapena a le faalapotopotoga ina ia tuuina atu uma faamaumauga o loo maua ia mafai ai e le ASD's ACSC ona tali atu i mea e tulai mai ina ia faatautaia ai se auiliiliga atoa ma ia faatulai ai se malamalamaga o le APT40 i gaioiga i luga o fesootaiga.

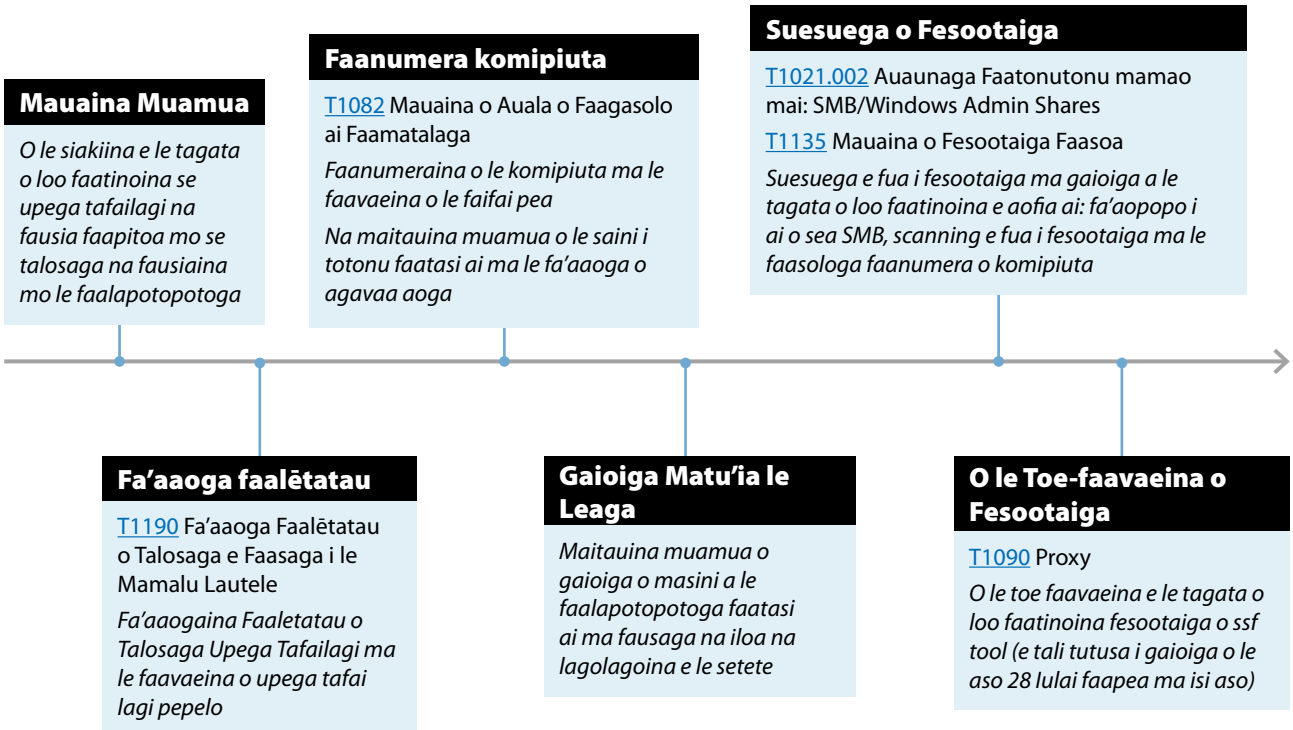
la Setema, ina ua uma faatalanoaga ma le ASD's ACSC, na filifili le faalapotopotoga ina ia poloka le lisina o le IP na iloa i le faailoaga muamua. la Oketopa, na amata ai e le faalapotopotoga ona fai faaleleiga.

Faamatalaga

E amata ia lulai, na mafai e i latou o faatinoina ona siaki ma fa'aaoga se talosaga upega tafailagi masani (T1190) na fa'aalu i luga o le `<webapp>2-ext`, faapea na mafai ai e le kulupu ona faavae se mea e mau ai i se sone e faasa e le militeri (DMZ). O le auala e fa'aaoga ai ina ia faanumeraina mea uma e lua o le fesootaiga faapea foi komipiuta o loo mafai ona iloa atu. Fetuutuunai agavaa (T1078.002) sa fa'aaoga ina ia fesiligia ai le Active Directory (T1018) ma ave'esea faamalosi faamaumauga e ala faapea o loo faasoaina faila (T1039) mai masini e tele i totonu o le DMZ. E faatinoina e le tagata o loo faia se osofaiga Kerberoasting ina ia maua mai ai se fesootaiga aoga o agavaa mai se komipiuta (T1558.003). E lei maitauina le kulupu i le mauaina o maka fa'aopopo o le auai a le o le DMZ po o fesootaiga i totonu.

Faatino taimi e iloa ai

O le faasologa o taimi e iloa ai o i lalo ifo o loo tuuina atu ai se vaaiga faalauaitele o tulaga autu o gaioiga a tagata e faatinoina mea matu'ia na maitauina e le fesootaiga a le faalapotopotoga.



Auiliiliina o le faasologa o taimi

Iulai: Na faavae e i latou o loo faatinoina se fesootaiga muamua i le itulau pito i luma o se talosaga upega tafailagi (T1190) na fausia mo le faalapotopotoga (mulimuli ane na faasino i ai faapea o le 'talosaga upega tafailagi' po o se '*webapp*') e ala i se malu puipuia o fesootaiga o faasologa o feoaiga (TLS) (T1102). E leai se isi gaioiga aoga na maitauina.

Iulai: Na amata ona faanumeraina e i latou o faatinoina talosaga upega tafailagi na vaavaai ai mo maka e faamuta ai[2] ina ia suesueina atili ai.

Iulai: E tulimatai e i latou o faatinoina taumafaiga ina ia fa'aaoga faaletatau se maka e faapitoa e faamuta ai.

Iulai: E mafai e i latou o faatinoina ona sao `POST` i le komipiuta upega tafailagi, masalo e ala i se upega tafailagi pepelo na tuuina i luga o se isi itulau. O se IP lona lua, e foliga mai na faafaigaluegaina e i latou lava ia e faatinoina, faapea foi na amata ona tuuina i luga i le URL lava e tasi. O i latou o faatinoina na faavaeina ma siakiina se numera o upega tafailagi pepelo.

O le metotia sa'o o le fa'aaoga faaletatau e le o mailoa, ae manino faapea o le maka faamuta faapitoa sa taulai i ai ina ia faavae ai ni faila i luga o le `<webapp>2-ext`.

E talitonu le ASD's ACSC faapea o tuatusi IP e lua o fesootaiga o ni vaega o le osofaiga lava e tasi talu ai ona e tutusa mea e fiafia i ai na faasoaina ma fesootaiga muamua na tulai mai i ni minute na va ai.

Iulai: Na fa'aauau e le kulupu ona faatautaia le faanumeraina o komipiuta, na vaavaai mo se avanoa e maualuga aia tatau, ma faafaigaluegaina se upega tafailagi pepelo e ese ai. E saini i totonu i latou o faatinoina i talosaga upega tafailagi e fa'aaoga ai agavaa fetuutuunai mo `<igoamuamua.faaiu>@<komipiuta a le faalapotopotoga>`.

O gaioiga a i latou o faatinoina e foliga mai e lei sao se aia tatau maualuga i luga o le `<webapp>2-ext`. A lē o lea, e fesuia'i e i latou o faatinoina i gaioiga e fua i fesootaiga.

Iulai: E siaki e le tagata o faatinoina agavaa fetuutuunai mo se aacount o loo fa'aaoga[3] faapea e foliga mai e maua i faaupuga faigata i totonu o faila e maua i totonu.

Iulai: E faafaigaluega e i latou o faatinoina le mea faigaluega open-source o le Secure Socket Funnelling, faapea sa fa'aaoga e fesootai ai i fausaga matu'ia le leaga. O lenei fesootaiga o loo faafaigaluegaina ina ia faalafi ai feoaiga mai masini osofai a i latou o faatinoina i totonu o fesootaiga i totonu a le faalapotopotoga, faapea o igoa o masini o loo faalauiloa i taimi e saini ai i totonu a o latou taumafai e fa'aaoga agavaa o le account o loo fa'aaoga.

Aukuso: Na iloa i latou o faatinoina o faatautaia se gaioiga e laitiiti se vaega, e aofia ai ua le mafai ona faavae fesootaiga e aafia ai le account o loo fa'aaogaina.

Aukuso: Na faatino e i latou o faia se fesootaiga uiga ese ma le faanumeraina o le Active Directory. O se account fetuutuunai e ese ai o loo fai ma faafaigaluega tulaga o sea[4] i luga o masini Windows i totonu o le DMZ, ina ia mafai ai ona aveesea faagaoi ma le manuia faamaumauga.

O lea e foliga mai o avanoa e fa'aaoga ai agavaa gaoia faaputu i luga o masini i le DMZ. E poloka e Firewalls le tagata o faatinoina mai le taulai o fesootaiga i totonu faatasi ai ma gaioiga tali tutusa.

Aukuso – Setema: O le SSF tool na toe faavaeina se fesootaiga i se IP e matu'ia le leaga. E le o maitauina faagaioiga fa'aopopo a le kulupu seiloga ua poloka le latou oso mai i totonu.

Setema: E poloka e le faalapotopotoga le IP e matuia le leaga e ala i le polokaina i luga o le latou pa puipui.

2 I lenei tusitusiga, o se faamuta ai o se gaioiga a le talosaga upega tafailagi

3 O accounts fa'aaoga e le iloa o tagata o loo fa'aaogaina, ae o auaunaga. I se tuatusi upeqa tafailagi Microsoft a se kamupani tele, o loo i ai ni accounts e eseese ituaiga.

4 Fetuunai le masini ina ia fesootai i alagaoa o sea o le faagasologa o le faia o faila i luga o auala o galueaina ai faila i luga o le fausaga e mafai e le tagata o fa'aaogaina po o se kulupu o loo fa'aaogaina.

Togafiti a le tagata o faatinoina ma auala e fai ai

O le faavae a le MITRE ATT&CK o se faaputuga pepa o faamatalaga o togafiti ma auala e fai ai e i latou o faatinoina faamata'u i luga o komipiuta. O le faavae na faavaeina e le U.S e le-mo-ni-polofiti. O le MITRE Corporation ma faagaioiga faapea o se gagana masani i le lalolagi i autafa o amioga faamata'u a i latou e faatinoina.

O le ASD's ACSC na mauaina auala nei e fai ai ma togafiti ina ia talafeagai i gaioiga matu'ia le leaga a le tagata o faatinoina:

Siakiina o se tulaga

T1594 – Upega Tafai Lagi e Ana e i Latou o Sailia Tagata ua Afaina

O le tagata o faatinoina na faanumeraina le upega tafailagi faapitoa a le tagata na apalai ina ia iloa ai avanoa mo le mauaina o fesootaiga.

Avanoa Muamua

T1190 – Talosaga e Feagai ma le Fa'aaoga Faaletatau Lautele (e faatatau i le fa'aaoga faaletatau o talosaga upega tafailagi faapitoa)

T1078.002 – Accounts o loo Aogā: Domain Accounts (e faatatau i le saini ai i totonu faatasi ai ma agavaa fetuutuunai)

Fa'aaogaina faaletatau o talosaga upega tafailagi faapitoa na iloa i luga o le initaneti na tuuina atu ai se tulaga o le oso ai i totonu mo le tagata o faatinoina. Na mafai e le tagata o faatinoina ona fa'aaoga agavaa na latou fetuutuunaia ina ia atili ai ona latou oo i fesootaiga.

O le faia o se fuafuaga ina ia mae'a ai

T1059 – Faatonu ma le Faaliliu-upu (e faatatau i le faia ia uma faatonuga e ala i le upega tafailagi pepelo)

T1072 – Meafaigaluega e Fa'aaoga i Polokalame Komipiuta (e faatatau i le fa'aaogaina e le tagata o faatinoina open-source tool Secure Socket Funnelling (SSF) ina ia fesootai ai i se IP)

Faifai pea

T1505.003 – Se Vaega o Polokalame Komipiuta: Tusitusiga e matu'ia le leaga (e faatatau i le fa'aaogaina o tusitusiga matu'ia le leaga ma le SSF ina ia faavae ai le mauaina)

Mauaina agavaa

T1552.001 – Agavaa mai Mea o loo Teu ai Upu Faalilolilo (e faatatau i faila e i ai upu faalilolilo e faatatau ina ia fausia ai auala e pulea ai (BMS))

T1558.003 – Gaoi pe Kopi Faagaoi Tusi Faamaonia: Kerberoasting (e faatatau i osofaiga ina ia maua ai agavaa o fesootaiga)

Gaioiga fa'aalatua

T1021.002 – Auaunaga Faatonutonu Mamao mai: Punaoa e mafai ona faasoa atu i isi Masini SMB Shares (e faatatau i le faapipi'iina e le tagata o faatinoina vaevaega o SMB mai masini e tele)

Aoina mai

T1213 –Faamaumauga mai Nofoaga o Teu ai Faamaumauga (e faatatau i tusi taiala/pepa o faamatalaga na maua i luga o komipiuta BMS)

Ave'esea Faagaoi o Faila

T1041 – Ave'esea faagaoi Over C2 Channel (e faatatau i le ave'esea faagaoi e le tagata o faatinoina faamaumauga mai le Active Directory ma faapipi'i i ai sea)

Suesuega o le mataupu lona 2

O lenei lipoti na faalilolilоina ina ia mafai ai faasalalauga faalauaitele. O le faalapotopotoga na afaina ua i ai nei ua faasino faapea ‘o le faalapotopotoga’. O nisi faamatalaga faapitoa na ave’esea ina ia puipuia ai mea e iloa ai le tagata ua afaina ma metotia e tali atu ai i mea na tulai mai i le ASD’s ACSC.

Aotelega o Mea aupito taua

O lenei lipoti o loo auiliili ai mea na maua i suesuega a le ASD’s ACSC i le manuia o fetuutuunaiga o fesootaiga a le faalapotopotoga ia Aperila 2022. O le lipoti o lenei suesuega na tuuina atu i le faalapotopotoga ina ia tuufaatasia ai gaioiga matu’ia na maitauina ma fautuaga e faaleleia ai fausaga i lalo. O mea na maua na iloa ai fetuutuunaiga sa faia e le APT40.

Ia Me 2022, na faailoa ai e le ASD’s ACSC se faalapotopotoga o gaioiga matu’ia le leaga na masalomia ua afaina ai fesootaiga a le faalapotopotoga talu mai Aperila 2022. Mulimuli ane, na faailoa e le faalapotopotoga le ASD's ACSC faapea na latou mauaina polokalame komipiuta matu’ia le leaga i luga o se komipiuta initaneti faapea na tuuina atu vaega e saini ai i totonu mo le faalapotopotoga tele faaiuga o le faatonutonu mamao mai. O lenei komipiuta sa fa’aaogaina se saini i totonu na faatonutonu mamao mai ma iloa ai puleaga o oloa ma o le a faasinoina i ai i le lipoti lenei faapea o le ‘masini na fetuutuunai’. O lenei lipoti o loo auiliiliiina ai mea na maua i suesuega ma faavae ai fautuaga faaleleiga mo le faalapotopotoga e tali atu ai i suesuega na faatautaia e le ASD’s ACSC.

Na iloa i faamaoniga faapea o le vaega o fesootaiga a le faalapotopotoga na fetuutuunaia e i latou o faatinoina matu’ia leaga i komipiuta e ala i le faatonutonu mamao mai o vaega e saini ai i totonu a le faalapotopotoga talu mai a itiiti ane a o Aperila 2022. O lenei komipiuta sa fetuutuunaia e le tele o i latou o faatinoina, na foliga mai na afaina i se faiga o se upu faalilolilo faatonutonu mamao mai ai vaivaiga (RCE) faapea na faasalalauina faalauaitele i le taimi o le fetuutuunai.

O gaioiga autu a le tagata o faatinoina na maitauina e le ASD’s ACSC na aofia ai:

- komipiuta faanumeraina, faapea e mafai ai e le tagata o faatinoina ona fausia a latou lava faafanua o fesootaiga;
- fa’aaogaina faaletatau o talosaga e feagai ma initaneti ma fa’aaoga tusitusiga matu’ia le leaga o upega tafailagi, tuuina atu ai i le tagata o faatinoina se vae muamua e mau ai i le fesootaiga ma mafai ai ona faataunuuina faatonuga;
- fa’aaogaina faaletatau o polokalame komipiuta vaivai ina ia faateleina ai avanoa; ma
- aoina o agavaa ina ia mafai ai gaioiga fa’aalatua

Na mauaina e le ASD’s ACSC faapea o se tagata na faatinoina sa faagaoi ona ave’esea le tai selau o igoa uiga ese e saini ai i totonu ma upu faalilolilo na fai faapa’aga i luga o masini na fetuutuunaia ia Aperila 2022, faapea foi le tele o upu faalilolilo faamaonia ma mea taulima faatekonolosi e faatatau i taimi o faatonutonu mamao mai ai. I se iloiloga e le faalapotopotoga, o upu faalilolilo na maua ane faapea e moni. Na maua e le ASD’s ACSC faapea o le tagata o faatinoina atonu na aoina mai nei mea taulima faatekonolosi ina ia faagaoi ai pe fausia se taimi e saini ai i totonu faapea o se tagata moni o loo fa’aaogaina, ma maua ai fesootaiga i totonu o le kamupani a le faalapotopotoga e fa’aaoga ai le account a le tagata moni o loo fa’aaogaina.

Mea na maua mai suesuega

Aotelega o suesuega

Na aiaia e le ASD's ACSC faapea o le tagata na faatinoina na fetuutuunaia masini faapea na faia ai taimi e saini mamao mai ai i totonu mo le aufaigaluega a le faalapotopotoga ma fa'aaoga ai le fetuutuunai lea ina ia taumafai ai ina ia faatautaia nisi gaioiga. O nei masini o loo i ai komipiuta e tolu vaega e paleni ai faapea o le vave o faamaoniga o fetuutuunai na iloaina. Na tapunia e le faalapotopotoga le lua o mea e tolu e paleni ai o komipiuta i le taimi vave lava o le fetuutuunai muamua. Faapea o se mea na iu i ai, o gaioiga soso'o ai na tulai mai i luga o se komipiuta e tasi. O isi komipiuta e faatatau i masini fetuutuunai na faapea foi ona tufatufaina atu i ai galuega fai i se auala e tali tutusa. Mo le mafai ona faitauina, o masini uma na fetuutuunai ua faasinoina i le tele o le lipoti lenei faapea o se 'masini e tasi'.

Ua talitonuina faapea o le tagata o faatinoina na fa'aogaina faalauaitele mea ua iloa o vaivai ina ia faafaigaluega ai tusitusiga matu'ia le leaga o upega tafailagi i le masini na fetuutuunai mai ia Aperila 2022 ma luga atu. O le tagata faamata'u mai le kulupu o loo iloiloina faapea na faateleina le maua o avanoa i luga o le masini. E lei mafai e le ASD's ACSC ona aiaia le atoa o le gaioiga ona ua le lava saini i totonu na maua. Ae peitai, o faamaoniga o le masini na iloa ai faapea o le tagata o faatinoina na ausia mea nei:

- O le aoina o le tai selau o igoa fa'aaoga ma fai faapa'aga ma upu faalilolilo; ma
- O le aoina o mea taulima faatekonolosi faapea atonu na faatagaina ai se tagata o faatinoina matu'ia leaga i se fausaga o se polokalame komipiuta e mamao ese (VDI) se vaega faapea o se tagata moni o loo fa'aaogaina.

Na iloilo e le ASD's ACSC faapea o le tagata o faatinoina sa vaavaai ina ia faia nisi fetuutuunai o fesootaiga a le faalapotopotoga. O mea taulima na ave'esea faanana e le tagata o faatinoina atonu na faatagaina i latou ina ia ave faagaoi pe faatino se taimi o komipiuta faatonutonu mamao mai faapea o se tagata moni o fa'aaogaina o le latou filifiliga, e aofia ai i latou o faia galuega ofisa. Atonu na fa'aaoga e le tagata o faatinoina le auala lea e oso ai i totonu i mea e tele ina ia fetuutuunai atili ai auaunaga a le faalapotopotoga ina ia ausia ai le faifaipea ma isi sini autu.

O isi masini a le faalapotopotoga i totonu o komipiuta na pulea siosiomaga e lei iloa ai faamaoniga o fetuutuunaiga.

Iloilo

O le komipiuta ua fetuutuunaia masini na tuuina atu mea e faamaonia ai e ala i le Active Directory ma se komipiuta e fa'aaogaina upega tafailagi, mo i latou o fa'aaogaina e fesootai i taimi o VDI (T1021.001).

Nofoaga	Masini ua fetuutuunaia igoa o komipiuta (tufatufaina paleni galuega)
Nofoaga tutotonu o faamaumauga 1	HOST1, HOST2, HOST3

O le fausaga o le masini o loo aofia ai foi faitotoa e maua ai komipiuta faapea e tuuina atu se ana i le VDI mo le tagata e fa'aaogaina, o le taimi lava latou te mauaina ai se faailoga e faamaonia ai na faatupuina ma lolomi i totonu mai le masini.

E lei i ai se faamaoniga o fetuutuunaiga i soo se isi o komipiuita nei. Ae peitai, o auala na maua ai faitotoa i saini i totonu o komipiuita na iloa ai faamaoniga o le tele o gaioiga faatasi ai ma tuatusi IP matu'ia le leaga. E foliga mai faapea o lea e iloa ai faapea o gaioiga na tulai mai i le komipiuta lenei, po o sootaga o fesootaiga ma le tagata na faatinoina faamata'u o fausaga faapea na oo mai i le komipiuta lenei. O le natura o lenei gaioiga e le mafai ona aiaia le fa'aaogaina o faamaoniga o loo maua ae iloa ai faapea o le kulupu na faufau ina ia migoi fa'aalatua i totonu o fesootaiga a le faalapotopotoga (TA0008).

Komipiuta i totonu

E tapulaa faamaumauga na suesueina e le ASD's ACSC mai totonu o le vaega o fesootaiga a le faalapotopotoga. Na taumafaia po o gaioiga faamanuiaina o gaioiga matu'ia le leaga na iloa ua afaina ai totonu o vaega o fesootaiga a le faalapotopotoga e aofia ai le oso i ai i totonu o le tagata o faatinoina i mea taulima e faatatau i le VDI, o le ma'osia o le komipiuta i totonu o le SQL (T1505.001), ma feaveaiga e le mafaamatalaina na maitauina na alu atu mai le tuatusi IP na iloa le matu'ia o le leaga e ala i le ui atu i faitotoa o masini (TA0011).

Fa'aogaina o le latou mauaina o masini fetuutuunai, na aoina e le kulupu igoa moni o tagata e fa'aaogaina, ma upu faalilolilo e saini ai i totonu (T1003), ma faailoga aoga MFA (T1111). Na aoina foi e le kulupu JSON Web Tokens (JWTs) (T1528), faapea o se mea taulima na faamaonia sa fa'aaogaina ina ia faavae ai taimi e saini ai i totonu o polokalame komipiuta e mamao ese. Atonu na fai e le tagata o faatinoina ona fa'aaoga mea

nei ina ia fausia ai pe ave faagaoi vaega o polokalame komipiuta e mamao ese (T1563.002) ma oso ai i totonu o vaega o fesootaiga a le faalapotopotoga faapea o se tagata fa'aaoga moni (T1078).

Na fa'aaoga foi e le tagata o faatinoina auala ina ia fetuutuunai ai masini ina ia leaga ai le komipiuta SQL (T1505.001), faapea na nofo i totonu o fesootaiga a le faalapotopotoga. E foliga mai sa i ai auala i totonu amai e tagata o faatinoina i le nei faamaumauga.

O faamaoniga o loo maua mai le mauaina o auala i masini na iloa ai faapea o fesootaiga o feagai na tulai mai e ala po o lenei masini mai tuatusi IP matu'ia le leaga. E pei ona faamatalaina atu i luga, o lea atonu e iloa ai faapea o aafiaga o tagata o faatino matu'ia leaga i luga o komipiuta pe sa fa'aaogaina le masini lenei, ma le faamoemoe ina ia tuusa'o i totonu o fesootaiga.

Faasoloina o taimi o suesuega

O le lisi o i lalo ifo e tuuina atu ai se faasologa o taimi o gaioia autu na mauaina i taimi o suesuega.

Taimi	Mea na tupu
Aperila 2022	Tuatusi matu'ia le leaga o IP na i ai faatasi ma auala e maua ai faitotoa i komipiuta HOST7. O le natura o gaioiga e lei mafai ona faamautuina.
Aperila 2022	O komipiuta uma o fesootaiga, HOST1, HOST2 ma le HOST3, na fetuutuunaia e le tagata o faatinoina po o i latou o faia gaioiga matu'ia, ma tusitusiga o upega tafailagi pepelo na tuuina i luga o komipiuta o fesootaiga. O se faila e saini ai i totonu na faavaeina pe sa fesuiai i luga o le HOST2. O lenei faila o loo i ai mea taua e foliga mai ua mauaina e le tagata o faatinoina gaioiga matu'ia. O le /etc/security/opasswd ma le /etc/faila sa faalafi na fesuia'i i luga o le HOST1 ma le HOST3, faailoa ai faapea o upu faalilolilo na fesuia'i. O faamaoniga o loo maua i luga o le HOST1 o loo fautuaina ai faapea o le upu faalilolilo mo le tagata na fa'aaogaina le 'sshuser' sa sui.
Aperila 2022	HOST2 na tapunia e le faalapotopotoga. O tusitusiga fa'aopopo o upega tafailagi pepelo (T1505.003) na faavaeina i luga o le HOST1 ma le HOST3. HOST1 na oo i taumafaiga faamalosi a le SSH mai le HOST3. O se faila e saini ai i totonu na fesuia'i (T1070) i luga o le HOST3. O lenei faila o loo i ai mea taua (T1078) e foliga mai ua mauaina e le tagata o faatinoina gaioiga matu'ia. JWTs na mauaina (T1528) ma faasolo atu i se faila o i luga o le HOST3. HOST3 na tapunia e le faalapotopotoga. O gaioiga uma ina ua pasi le taimi lea na tulai mai i luga o le HOST1.
Aperila 2022	O tusitusiga fa'aopopo o upega tafailagi pepelo na faavaeina i luga o le HOST1 (T1505.003). JWTs na mauaina ma faasolo atu i tua i se faila i luga o le HOST1.
Aperila 2022	O tusitusiga fa'aopopo o upega tafailagi pepelo sa faavaeina i luga o le HOST1 (T1505.003), ma se tuatusi IP matuia le leaga na iloaina o faifaimea ma le komipiuta o faasoasoaina (TA0011). O se tuatusi IP matu'ia le leaga na iloaina o faifaimea faatasi i auala e maia ai avanoa i komipiuta HOST7.
Me 2022	O se tuatusi IP matu'ia le leaga na iloaina o faifaimea faatasi i auala e maia ai avanoa i komipiuta HOST7 (TA0011). O se mea na tupu i se faamaoniga mo se tagata e fa'aaogaina e fesootai i se tuatusi IP ua matu'ia le leaga i mea e saini ai i totonu o le HOST1. O se fa'aopopoga o tusitusiga upega tafailagi pepelo na faavaeina i luga o le komipiuta lenei (T1505.003).
Me 2022	O se tusitusiga i luga o le HOST1 sa fesuia'i e se tagata o faatinoina gaioiga (T1543). O lenei tusitusiga o loo i ai faagaioiga faapea e mafai ona soloia faamaumauga mai se polokalame komipiuta SQL.
Me 2022	O se faila fa'aopopo e saini ai i totonu i luga o le HOST1 na fesuia'i mulumuli ane (T1070). O lenei faila o loo i ai faapa'aga igoa fa'aaoga ma upu faalilolilo mo fesootaiga a le faalapotopotoga, fapea e talitonuina ina ia moni (T1078).
Me 2022	O se faila fa'aopopo e saini ai i totonu na fesuia'i mulimuli ane (T1070). O lenei faila o loo i ai JWTs na aoina mai le HOST1.
Me 2022	O tusitusiga fa'aopopo o upega tafailagi pepelo na faavaeina i luga o le HOST1 (T1505.003). I le aso lea, na lipotia ai e le faalapotopotoga le mauaina o se tusitusiga upega afailagi pepelo faatasi ai ma le aso na faavaeina ai ia Aperila 2022 i le ASD's ACSC
Me 2022	O se vaega o tusitusiga na faavaeina i luga o le HOST1, e aofia ai le tasi e igoa o le Log4jHotPatch.jar.
Me 2022	O le polokalame komipiuta na faatonuina sa fa'aaoga ina ia fa'aopopo ai vaega o kmoipiuta e lua i le mauaina o faitotoa o komipiuta. O vaega komipiuta nei sa 9998 ma le 9999 (T1572).

Togafiti a le tagata o faatinoina ma auala e fai ai

Faamatamata tetele o i lalo ifo o nai togafiti ma auala e fai ai na iloa i le taimi o le suesuega.

Avanoa muamua

T1190 Fa'aaoga faaletatau o talosaga e feagai ma le mamalu lautele

E foliga mai sa fa'aaoga faaletatau e le kulupu le RCE, faateleina avanoa, ma faamaonia ia sao vaivaiga i le maua mamao o le saini i totonu ma iloa ai oloa o pulea ina ia maua muamua ai auala i totonu i fesootaiga.

O le metotia mmuamua lea e maua ai ua vaavaai i ai faapea o lea ona o mea nei:

- O le polokalame komipiuta o faasoasoania sa vaivai i nei CVEs i le taimi lea;
- O taumafaiga ina ia so'ona fa'aaoga vaivaiga nei mai fausaga a i latou e faatinoina ua iloa; ma
- O le gaioiga matu'ia i totonu na iloa muamua ae e lei leva ina ua uma taumafaiga e so'ona fa'aaoga.

O le faia o se fuafuaga ina ia mae'a ai

T1059.004 Faatonuga ma le Tagata e Faaliliuina Tusitusiga: Unix Shell

Na faamanuiaina le fa'aaoga faaletatau a le kulupu i vaivaiga o i luga ma na mafai ona fa'aalu faatonuga i se Unix shell o loo maua i luga o masini ua afaina. O faamatalaga mae'a o faatonuga na fa'aaoga e le aufaamata'u e lei mafai ona tuuina atu ona faapea latou te lei saini ai i totonu i le masini.

Faifai pea

T1505.003 Vaega o Polokalame o Komipiuta: Polokalame Matu'ia le Leaga

Na faafaigaluegaina e le aufaamata'u nai tusitusiga upega tafailagi pepelo i luga o le masini na aafia. E mafai faapea o le aufaamata'u e toatele na faafaigaluegaina tusitusiga upega tafailagi pepelo, ae na o se vaega laitiiti o le aufaamata'u na faatautaia gaioiga e fa'aaoga ai tusitusiga upega tafailagi nei. O tusitusiga upega tafailagi faapea na faatagaina mo faatonuga e fai fua le faataunuuina e le faamata'u i uga o masini ua fetuutuunai.

Faateleina avanoa

T1068 Fa'aaoga Faaletatau mo le Faateleina o Avanoa

O faamaoniga o loo maua e le faamatalaina ai le tulaga o avanoa na maua e le aufaamata'u. Ae peitai, o le fa'aaogaina o tusitusiga upega tafailagi, sa tatau i le aufaamata'u ona ausia se tulaga faatusatusa o avanoa i lena o le polokalame komipiuta i luga o masini ua fetuutuunai. O vaivaiga e talitonuina na i ai i luga o masini ua fetuutuunai ma atonu na faataga ai le aufaamata'u ina ia mauaina avanoa loloto i totonu.

Mauaina agavaa

T1056.003 Faasologa e Pu'e ai le Aoga o Faamaumauga o le Taimi: Faasologa o le Sefeina o se Ata i Luga o Upega Tafailagi

Faamaoniga i luga o masini fetuutuunai na iloa ai faapea o le faamata'u na mauaina le tai selau o faapa'aga o igoa fa'aaoga-upu faalilolilo, i tusitusiga manino, faapea e talitonuina ina ia moni. E foliga mai faapea o mea nei na maua i le fa'aaogaina o nisi fesuia'iga i le faagasologa o le faamaoniga faapea e fa'aalu ai i tua agavaa i se faila.

T1111 Taofia le Faamaonia e Manaomia ai ni IDs e lua ia Mautinoa ai

Na maua foi e le faamata'u le tau o faailoga MFA e fesootai i saini i totonu e moni. O nei mea e foliga mai na maua e ala i le fesuiaiga o le faasologa o faamaoniga moni ina ia fa'aalu ai i tua tau nei i se faila. O loo i ai faamaoniga o fetuutuunai o le 'secret server' faapea o loo teu ai tau e uiga ese faapea e tuuina atu mo le malu puipuia o faailoga MFA.

T1040 Faasalavei i Fesootaiga

Ua talitonuina o le faamata'u na mauaina JWTs e ala i le mauaina o feoaiga HTTP i luga o masini ua fetuutuunai. O loo i ai molimau faapea o le aogā o le tcpdump sa faataunu'uina i luga o masini ua fetuutuunai, faapea atonu pe na faapefea ona maua e le faamata'u nei JWTs.

T1539 O se tagata e tete'e atu i faaletonu e ono gaoia Web Session Cookie ia maua ia initaneti

E pei ona faamatalaina atu i luga, na maua e le faamata'u JWTs, faapea e faatusa i vaega pupu'u o faamaumauga. O nei mea na mafai ona toe fa'aogaina e le faamata'u ina ia faavae ai nisi auala e maua ai.

Mauaina

T1046 O se Faagasologa i Luga o Fesootaiga na Otomeki ona Mauaina (Network Service Discovery)

O loo i ai molimau faapea o le aoga o le fa'aata o fesootaiga map sa faataunu'uina i luga o le masini fetuutuunai ina ia fa'aata ai isi masini i le vaega lava e tasi o fesootaiga. O lea sa foliga mai na fa'aaoga e le faamata'u ina ia mauaina ai isi auaunaga o fesootaiga e mafai ona oo i ai faapea atonu na i ai avanoa mo gaioiga fa'aalatua.

Aoina mai

O molimau o loo maua e le o faailoa mai ai pe faapefea ona aoina e le faamata'u faamaumauga pe faapea tonu po o fea sa ao mai ai masini fetuutuunai pe mai isi auala o galueaina ai. Ae peitai, e foliga mai faapea o le aufaamata'u na maua auala i faila uma i luga o masini na fetuutuunai, e aofia ai agavaa na maua (T1003), tau o fa'ailoga MFA (T1111), ma JWTs o loo faamatalaina atu i luga

Faatonuga ma Puleaga

T1071.001 Application Layer Protocol: Tulaga o Tulafono e pulea faamaumauga

E fa'aaoga e le aufaamata'u tusitusiga upega tafailagi mo faatonuga ma le pule faatonutonu. O faatonuga o tusitusiga upeqa tafai lagi atonu na pasi atu i luga o le HTTPS e fa'aaoga ai le polokalame upega tafailagi o i ai nei i luga o le masini (T1572).

T1001.003 Faamaumauga Fenumia'i: Faafoliga o Tulafono

E fa'aaoga e le aufaamata'u masini ua fetuutuunai faapea o se faalauiloa mo osofaiga faapea o loo fafauina ina ia mili faatasi ai ma feoaiga moni.

Faate'ia ma fautuaga ina ia faatitiitia ai

E fautuaina malosi e le ASD's ACSC le faatuina o le ASD Essential Eight (Mea Taua e Valu) Pule Faatonutonu ma faatatau Auala e Fai ina ia Tuuitiitia ai Mea e Tutupu mai i le Malu Puipuia i Luga o Initaneti. O i lalo ifo o fautuaga mo gaioiga malu puipuia o fesootaiga faapea e tatau ona faia ina ia faate'ia ai ma foia osofaiga e ala i le APT40, mulimulitai faapitoa ia faaitiitia ai mo ki autu e fa o TTPs o loo tuufaatasia i le Table 1.

Faate'ia

O nisi o faila ua faailoaina i luga sa tuuina mai i lalo i nofoaga e pei o C:\Users\Public* and C:\Windows\Temp*. O nei nofoaga e mafai ona avea ma tulaga faigofie mo le tusia o faamaumauga pei ona masani ona tusia e le lalolagi, faapea, o accounts uma a tagata e fa'aaogaina e lesitalaina i le Windows e i ai auala e maua ai faasinoala nei ma o latou faasinoala laiti. E masani ai lava, soo se tagata fa'aaoga e mafai ona maua mulimuli ane faila nei, e faataga ai avanoa mo gaioiga fa'aalatua, le mafai e le aufaamata'u ona faatino e le iloaina a o osofaia auala o masini, maualalo avanoa e faataunuuina ai ma faatulaga mo le ave faagaoi o faamaumauga.

O mea nei o Sigma rules e vaavaai mo le faataunuuina mai nofoaga masalomia faapea o se faailoilo o se gaioiga na tupu a'e mai se isi mea. I tulaga uma, o suesuega mulimuli ane ai o loo manaomia ina ia faamautu ai gaioiga masalomia ma mafua'aga.

Ulutala: O Faila po o Faasinoala e mafai e soo se tasi ona fesuiai

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Faamatalaga: Faate'ia faasologa o faataunuuga mai C:\Windows\Temp.

Tala'aga:

O lenei tulafono e vaavaai faapitoa mo le faataunuuina i tua atu o C:\Windows\Temp*. Temp e sili atu le fa'aaogaina faalauaitele o talosaga e leai se aoga ma faapea e maualalo ai le mautinoa o faailoilo masalomia nai lo le faataunuuina i tua atu o isi faasinoala tusitusia laiti i le lalolagi C:\Windows.

O le ave'esea o le faataunuuina o talosaga e le SYSTEM po o NETWORK SERVICE tagata e fa'aaogaina tele le faaitiitia o le tele o gaioiga e le aoga na filifilia e ala i le nei tulafono.

O le uiga o lea e faapea o le tulafono atonu e misi le masalomia o le faataunuuina i se avanoa maualuga le tulaga ae e fautuaina ina ia fa'aaoga isi tulafono ina ia faamautu ai pe afai o se tagata fa'aaoga o loo taumafai ina ia faateleina avanoa i le SYSTEM.

Suesuega:

1. Suesue faamatalaga tuusa'o e faatatau i lenei faataunu'uga, e pei o tusitusiga a le tagata fa'aaoga, faataunu'uga i tulaga o amio sa'o, vave toe siaki gaioiga ma ata na tuu i luga e ala i le faila.
2. Suesue faasologa o tusitusiga, fesootaiga, faila ma isi faamaumauga e lagolagoina i luga o le komipiuta o faasoasoaina ina ia fesoasoani ai ia faia se suesuega pe faapea o se gaioiga e masalomia.
3. Afai e tatau ai taumafaiga ina ia ao mai se kopi o le faila mo le toe faafoi i tua e le inisinia ina ia faamautu ai pe moni.

Faamatalaga e Faamaonia ai:

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

Tusitala: ASD's ACSC

Aso: 2024/06/19

Tulaga: faataitaiga

Tags:

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

Punaoa Uiga ese e aoina mai faamaumauga:

```
category: process_creation
product: windows
```

Faate'ia:

```
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:
    O tagata e fa'aaogaina:
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

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

condition: temp and not (common_temp_path or system_user or dismhost or known_parent)

False positives:

- Faataga le lisi su'etusi o talosaga na maitauina na mafai ona faatino ai faila mai le Temp.
- Temp o le a i ai moni se vaega e faatulaga ai talosasga ma i latou e faalauiloaina, o le mea lea o le a taua ai le vaavaai i ai pe faapefea ona taatele lenei amioga e lua o se fesootaiga maitauina (ma pe mata pe le mafai ona faatagaina e lisi) ae lei faafaigaluegaina lenei tulafono.

Tulaga: maualalo

Ulutala: Faataunuuina o Tusitusiga i le Lalolagi - Soo se Faila i Luga o Komipiuta e Fa'aagaga e le umi

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

Faamatalaga: Faate'ia faasologa o le faataunuuina mai nofoaga o tusitusiga a le lalolagi i se faasinoala laitiiti o le Windows OS nofoaga e faapipi'i ai.

Tala'aga:

O lenei tulafono e vaavaai faapitoa mo le faataunuuina i tua atu o faasino ala tusitusia i le lalolagi i totonu o le C:\ ma aemaise ai lava C:\Windows*, faatasi ai ma le faatagana a le C:\Windows\Temp (faapea e sili atu le da'aaoga faalauaitele e talosga e le aoga ma faapea o le maualalo o le mautinoa i faailoilo masalomia).

O faila o AppData e le o aofia ai pe afai o se faila o loo fa'aalu faapea o se SYSTEM - o se auala e le aogā lea faapea o le tele o talosaga e le umi taimi o faila o loo faataunuuina ai.

A uma ona faamae'a faiga faavae muamua o se fesootaiga ma iloa ai faataunu'uga le aoga mai nofoaga nei, o lenei tulafono e tatau ona seasea faaumatia.

Suesuega:

1. Suesue faamatalaga tuusa'o e faatatau i lenei faataunu'uga, e pei o tusitusiga a le tagata fa'aaogaina, faataunu'uga i tulaga o amio sa'o, vave toe siaki gaioiga ma ata na tuu i luga e ala i le faila.
2. Suesue faasologa o tusitusiga, fesootaiga, faila ma isi faamaumauga e lagolagoina i luga o le komipiuta o faasoasoaina ina ia fesoasoani ai ia faia se suesuega pe faapea o se gaioiga e masalomia.
3. Afai e tatau ai taumafaiga ina ia ao mai se kopi o le faila mo le toe faafoi i tua e le inisinia ina ia faamautu ai pe moni.

Faamatalaga e Faamaonia ai:

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

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

Tusitala: ASD's ACSC

Aso: 2024/06/19
Tulaga: faataitaiga

Tags:

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

Punaoa Uiga ese e aoina mai faamaumauga:

category: process_creation
product: windows

Faate'ia:

writable_path:

Ata|o i totonu:

- ':\\$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:

Image|contains: '\\AppData\\'
O tagata e fa'aaogaina: 'SYSTEM'

tulaga: writable_path and not appdata

False positives:

Faataga le lisi o talossga e su'etusi na maitauina na mafai ona fa'atino mai nei faasinoala.

E talafeagai faapea o tusitusiga ma mea faigaluega faaofisa na fa'aaoga i le mata'ituina o siosiomaga atonu o loo i totonu o se tasi o faasinoala nei ma e tatau ona faatuatusi i luga o tulaga tasi i le tasi.

Tulaga: maualuga

Ulutala: Faataunu'uga o Tusitusiga i le Lalolagi - Tagata e Fa'aaogaina

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

Faamatalaga: Faate'ia faasologa o faataunu'uga mai C:\Users\Public* ma isi faila tusitusia i le lalolagi i totonu e Tagata e Fa'aaogaina.

Tala'aga:

O faila o AppData e le o aofia ai pe afai o se faila o loo fa'aalu faapea o se SYSTEM - o se auala e le aogā lea faapea o le tele o talosaga e le umi taimi o faila o loo faataunuuina ai.

Suesuega:

1. Suesue faamatalaga tuusa'o e faatatau i lenei faataunu'uga, e pei o tusitusiga a le tagata fa'aaoga, faataunu'uga i tulaga o amio sa'o, vave toe siaki gaioiga ma ata na tuu i luga e ala i le faila.
2. Suesue faasologa o tusitusiga, fesootaiga, faila ma isi faamaumauga e lagolagoina i luga o le komipiuta o faasoasoaina ina ia fesoasoani ai ia faia se suesuega pe faapea o se gaioiga e masalomia.
3. Afai e tatau ai taumafaiga ina ia ao mai se kopi o le faila mo le toe faafoi i tua e le inisinia ina ia faamautu ai pe moni.

Faamatalaga e Faamaonia ai:

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

Tusitala: ASD's ACSC

Aso: 2024/06/19

Tulaga: faataitaiga

Tags:

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

Punaoa Uiga ese e Aoina mai Faamaumauga:

category: process_creation
product: windows

Faate'ia:

o tagata e fa'aaogaina:

Ata|o i totonu:

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

appdata:

Image|contains: '\\AppData\\'
O tagata e fa'aaogaina: 'SYSTEM'

condition: users and not appdata

False positives:

- E talafeagai faapea o tusitusiga ma meafaigaluega faaofisa na fa'aaoga i le mata'ituina o siosiomaga atonu o loo i le Mamalu Lautele po o se faasinoala laitiiti ma e tatau ona faatuatusi i luga o tulaga tasi i le tasi.

Tulaga: faaleogolua

Auala ina ia tu'uiiitia ai le leaga tele

Saini i totonu o se komipiuta

I taimi o suesuega a le ASD's ACSC, o se mataupu masani faapea e faaitiitia ai le aoga ma le vave o taumafaiga o suesuega o se le lava o le aofia uma ai ma faamatalaga o le saini ai i totonu i le tele o vaega e aofia ai polokalame upega tafailagi e talosagaina saini i totonu, mea e tulai mai i saini i totonu i le Windows, ma faamaoniga e saini ai i totonu mo se isi i initaneti.

E fautuaina e le ASD's ACSC iloiloga ma faatuina le latou taiala i luga o le Windows Event Logging and Forwarding e aofia ai le faatulagana o faila ma tusitusiga i le Windows Event Logging Repository ma Information Security Manual's Guidelines for System Monitoring, ina ia aofia ai ia ogatotonu ai saini i totonu ma taofia saini mo se taimi talafeagai.

Polokalame Komipiuta Laiti

O le vave o polokalame laiti o initaneti uma ua faailoaina atu masini ma auaunaga, e aofia ai polokalame upega tafailagi, talosga upega tafailagi, ma faitotoa e faatonutonu mamao mai. Mafaufau i le faatuina o se polokalame tutotonu e pulea auala o fai ai galuega ina ia otomeki ma faavave ai le faasologa. E fautuaina e le ASD's ACSC le faatuina o le ISM's Guidelines for System Management, faapitoa lava, le System Patching e pule faatonutonu i mea e apalai i ai.

O le tele o le fa'aaoga faaletatau e fa'aaoga e le tagata o faatinoina na iloa faalauaitele ma na i ai polokalame laiti po o mea e faaitiitia ai o loo maua. E tatau i faalapotopotoga ona ia mautinoa faapea ia malu puipuia polokalame laiti po o mea e faaitiitia ai o loo apalai i fausaga o loo feagai ma initaneti i totonu o le 48 itula, ma mea e mafai ai, fa'aaoga le vaega lata mai nei o polokalame komipiuta ma auala e faagaioi ai.

Polokalame malupuipuia e vaevaeina fesootaiga o komipiuta

O polokalame malupuipuia e vaevaeina fesootaiga o komipiuta e mafai ona faia ina ia sili atu le faafaigata mo faaletonu ina ia iloa ma maua ai auala i faamaumauga ma'ale'ale a se faalapotopotoga. Polokalame malupuipuia ina ia faatapulaa pe poloka ai gaioiga fa'aalatua e ala i le te'ena o feoaiga i le va o komipiuta sei vagana ai ua manaomia. O komipiuta taua e tuuina atu faamatalaga i isi komipiuta e pei o le Active Directory ma isi tautua faamaonia e tatau na mafai ona tuuina atu faamatalaga mai se vaega tapulaa o fesootaiga po o 'jump servers'. O nei polokalame e tatau ona mata'ituina vavalalata, ia lelei le malupuipuia ma faatapulaa tagata e fa'aaogaina ma masini e mafai ona fesootai atu i ai.

Tusa lava po o a mea na tutupu na iloaina faapea o gaioiga fa'aalatua ua foia, o polokalame laiti malupuipuia fa'aopopo e mafai ona faatapulaa nisi vaega e tele o faamaumauga na mafai ona maua e le faamata'u ma aveesea faagaoi.

Auala fa'aopopo e faaitiitia ai

O faalapotopotoga e fausia ma tuuina atu e faapea foi ona fautuaina auala nei ia faaitiitia ai ina ia tete'e atu ai i le APT40 ma isi o fa'aaogaina TTPs o i lalo.

- Faaleaoga auaunaga o fesootaiga ua le toe fa'aaogaina po ua le toe aoga, vaega o komipiuta ma tulafono.
- Fa'aaoga talosaga o pa pupuni ua lelei le faasologa o Web (WAFs) ina ia puipuia ai polokalame upega tafailafgi ma talosaga.
- Faamalosia ia itiiti avanoa ina ia tapulaa ai le mauaina o polokalame komipiuta, faasoaina o faila, ma isi alaga'oa.
- Fa'aaoga le faamaoniga e tele mea e manaomia (MFA) ma pulea accounts o auaunaga ina ia faafaigata ai agavaa ona maua ma toe fa'aaoga. E tatau i le MFA ona apalai i auaunaga uma o le initaneti e mafai ona maua ai faatonutonu mamao mai e aofia ai:
  - Upega tafailagi ma imeli e teu i le cloud
  - O se mea faigaluega digital faapea e mafai ai e kulupu ona galulue faatasi
  - Ia malu puipuia fesootaiga
  - Auaunaga e faatonutonu mamao mai lau komipiuta
- Toe sui mea faigaluega ua uma le aoga.

Table 1. Auala e Faaitiiti ai/Auala e faatino ai

TTP	Essential Eight Mitigation Strategies	ISM Controls
Avanoa Muamua T1190 Fa'aaoga faaletatau o Talosaga e Feagai ma le Mamalu Lautele	Faasologa o le faafouina o polokalame komipiuta Faasologa o le faapipi'iina o polokalame fou O se Fua Faatatau o Puipuiga e Manaomia ai Tagata e Fa'aaoga ina ia tuuina mai nisi Faamatalaga e iloa ai O se puipuiga faapea po o a talosaga e mafai ona fa'aalu i le system	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
O le faia o se fuafuaga ina ia mae'a ai T1059 Faatonuga ma le Faaliliuina o Tusitusiga	O se puipuiga faapea po o a talosaga e mafai ona fa'aalu i le system Ia foia tagata fa'aaoga po o le aufaamata'u mai le oso atu i tulaga malupuipuia. Faatapulaa avanoa o galuega ofisa	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Faifai pea T1505.003 O polokalame taitoatasi po o mea e galulue faatasi ina ia maua ai se auala atoa o auaunaga: Web Shell	O se puipuiga faapea po o a talosaga e mafai ona fa'aalu i le system Faatapulaa avanoa o galuega ofisa	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Tulaga Muamua o Osofaiga / Faateleina Avanoa / Faifaipea T1078 Accounts o loo aoga	Faasologa o le faapipi'iina o polokalame fou O se Fua Faatatau o Puipuiga e Manaomia ai Tagata e Fa'aaogaina ina ia tuuina mai nisi Faamatalaga e iloa ai Faatapulaa avanoa o galuega ofisa O se puipuiga faapea po o a talosaga e mafai ona fa'aalu i le system E puipuia se faalapotopotoga mai faamata'u	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

Mo mea lautele fa'aopopoo faate'ia ma fautuaga e faaitiitia ai, faamolemole faatalanoa le Tu'uitiitia le Leaga tele ma le Faateia vaega o le MITRE ATT&CK itulau upega tafailagi i auala e fai ai mo auala taitasi e fai ai ua iloa i le aotelega a le MITRE ATT&CK i le faaiuga o lenei fautuaga.

O se Faamatalaga e te'ena ai

O faamatalaga i lenei lipoti ua saunia i le "tulaga o i ai nei" mo na o faamoemoega lava tau faamatalaga. O faalapotopotoga e fausia ma gaosia e lē faatagaina soo se kamupani faipisinisi, oloa, kamupani, po o se auaunaga, e aofia ai soo se faalapotopotoga, oloa, po o auaunaga e fesootai i totonu o lenei pepa o faamatalaga. Soo se faauigaina i faapitoa faapisinisi e tuuina i ai, ni oloa, faasologa, po o auaunaga e ala i se maka o auaunaga, igoa pisinisi, kamupani gaosi oloa, po o isi, e le faia pe apalai i ai faamaoniga, fautuaga, pe faapito i ai le faalapotopotoga e fausia ma tuuina atu.

O lenei pepa o faamatalaga ua makaina TLP:CLEAR. E leai se faasa po o se tapulaa i faamatalaga e faasoaina O alaga'oa atonu e fa'aaogaina TLP:CLEAR pe a tauaveina e faamatalaga e itiiti pe leai se lamatia o le so'ona fa'aaogaina, e faatatau i tulafono e apalai i ai ma mea fai mo le faamatuuina i le mamalu lautele. E faatatau itulaga o tulafono o aia tatau, TLP:CLEAR o faamatalaga atonu e tufatufaina atu e aunoa ma le faasaina. Mo nisi faamatalaga i luga o Traffic Light Protocol, tagai ane i le cisa.gov/tlp

MITRE ATT&CK – Tala'aga o faiga fa'atino a le APT40 e tāua

Siaki Muamua ae lei Faatinoina (TA0043)	
Upega Tafailagi e ana e i Latou o Faia Sailiga (T1594)	Aoina mai o Faamatalaga e iloa ai Tagata ua Afaina: Faailoga Aoga (T1589.001)
esootaiga ma faasologa malu puipuia: Auala e iloa ai Faaletonu (T1595.002)	Aoina mai o Faamatalaga o i Totonu (T1592)
Upega Tafailagi Tatala e Saili ai: Enesini Saili ai (T1593.002)	Aoina mai o Faamatalaga o Fesootaiga o Tagata ua Afaina: Mea Totino o Komipiuta (T1590.001)
Aoina mai o Faamatalaga e iloa ai Tagata ua Afaina: Tuatusi Imeli (T1589.002)	

Atina'eina o Alaga'oa Fou (TA0042)	
Ia maua Fausaga: Domains (T1583.001)	Mauaina o Fausaga (T1583)
Ia maua Fausaga: DNS Server (T1583.002)	Accounts ua Fetuutuunai (T1586)
Faavae Mea Eseese o le mafai ma faatino ai: Code Signing Certificates (T1587.002)	Fausaga ua Fetuutuunai (T1584)
Faavae Mea Eseese o le mafai ma faatino ai: Digital Certificates (T1587.003)	Faavae Mea Eseese o le mafai ma faatino ai: Malware (T1587.001)
Obtain Capabilities: Code Signing Certificates (T1588.003)	Faavae ni Accounts: Cloud Accounts (T1585.003)
Compromise Infrastructure: Network Devices (T1584.008)	Se Masini e Faatau ma Fa'aaoga: Faila po o se Upu Faalilolilo faa-Komipiuta (T1588.004)

Ilaasaga Muamua o Osofaiga i Luga o Komipiuta (TA0001)	
E Fa'aaoga le Augaoi Accounts o Fa'aaogaina (T1078)	PImeli Pepelo (T1566)
Accounts Fa'aaoga: Accounts ua Faaletonu (T1078.001)	Lafoina o Imeli e le moni: Spearphishing Attachment (T1566.001)
Accounts Fa'aaoga: Accounts fa'aaoga ia maua ai upega tafailagi (T1078.002)	Lafoina o Imeli e le moni: Spearphishing Link (T1566.002)
External Remote Services (T1133)	So'ona Fa'aaoga App e Feagai ma le Mamalu Lautele (T1190)
Fetuutuunai Mai Fafo (T1189)	

Faia ia mae'a (TA0002)	
Pulea o Mea e Fa'aaoga e Windows (T1047)	Faatonuga ma le Faamatala-upu e faaliliuina tusitusiga: Python (T1059.006)
Galuega Faatulagaina (T1053.002)	Faatonuga ma le Faamatala-upu e faaliliuina tusitusiga: JavaScript (T1059.007)
Galuega Faatulagaina: Gaioiga Faatulagaina (T1053.005)	Native API (T1106)
Faatonuga ma le Faaliliu-upu o Tusitusiga (T1059)	Vaega o galueaina masini e faatagaina fesuiaiga o faamaumauga (T1559)
Faatonuga ma le Faamatala-upu e faaliliuina tusitusiga: Windows Command Shell (T1059.003)	Faagasologa faatekonolosi e fafau ina ia kiliva ai auaunaga: Matafaioi faapolofesa (T1569.002)
Faatonuga ma le Faamatala-upu e faaliliuina tusitusiga: PowerShell (T1059.001)	Atonu e gaoia e le augaoi faamaumauga e ala i le kopi faanana (T1203)
Faatonuga ma le Faamatala-upu e faaliliuina tusitusiga: Visual Basic (T1059.005)	O se Tulaga faapea e faaleaga ai e le au osofai gaioiga a se tagata o loo fa'aaogaina ina ia maua ai se code e faauma ai: Malicious File (T1204.002)
Faatonuga ma le Faamatala-upu e faaliliuina tusitusiga: Unix Shell (T1059.004)	Faatonuga ma le Faamatala-upu e faaliliuina tusitusiga: Apple Script (T1059.002)
Gaioiga/Galuega Faatulagaina: Cron (T1053.003)	Polokalame o Meafaigaluega e Fa'aaoga (T1072)

Faifai pea (TA0003)	
Accounts Fa'aaoga (T1078)	O polokalame taitoatasi po o mea e galulue faatasi ina ia maua ai se auala atoa o auaunaga: Web Shell (T1505.003)
Talosaga Amata i le Ofisa: Polokalame o Faamatalaga o le Ofisa (T1137.001)	Atia'e pe Fesuiai Faagasologa o Faasolo ai Gaioiga Fai: Auaunaga Windows (T1543.003)
Gaioiga/Galuega Faatulagaina: At (T1053.002)	Faaola pe Faamae'a le Otomeki ona Saini i Totonu: Ki Lesitala e Fa'aalu ai / Faila e Amata ai (T1547.001)
Gaioiga/Galuega Faatulagaina: Gaioiga Faatulagaina (T1053.005)	Faaola pe Faamae'a le Saini i Totonu: Fesuiaiga Faapuupuu (T1547.009)
Auaunaga Faatonutonu Mai Fafo (T1133)	Faasolo ia Mae'a Faagaoi: DLL Search Order Hijacking (T1574.001)
Gaioiga/Galuega Faatulagaina: Cron (T1053.003)	Faasolo ia Mae'a Faagaoi: DLL Side-Loading (T1574.002)
Ta'aina sese Account (T1098)	Accounts Fa'aaoga: Cloud Accounts (T1078.004)
Accounts Fa'aaoga: Accounts e saini ai i se komipiouta (T1078.002)	

Faateleina avanoa (TA0004)	
Gaioiga/Galuega Faatulagaina: At (T1053.002)	Atia'e pe Fesuiai Auala o Faagasolo ai Gaioiga fai: Windows Service (T1543.003)
Gaioiga/Galuega Faatulagaina: Gaioiga Faatulagaina (T1053.005)	Faaola pe Faamae'a le Otomeki ona Saini i Totonu: Ki e Fa'aalu ai le Lesitala / Faila e Amata ai (T1547.001)
E Fa'aaoga e le Aufaamata'u: Maua e le au osofai auala i imeli ma fa'aopopo i ai latou faagaoi (T1055.003)	Faaola pe Faamae'a le Otomeki le Saini i Totonu: Fesuiaiga Faapuupuu (T1547.009)
E Fa'aaoga e le Aufaamata'u: Polokalame matu'ia e faalafi ai (T1055.012)	Faasolo Faamae'a Faagaoi: DLL Search Order Hijacking (T1574.001)

Faateleina avanoa (TA0004)	
Accounts Fa'aaoga: Accounts e Saini ai i Komipiuta (T1078.002)	So'ona Fa'aaoga mo Osofaiga e Maualuga Aafiaga (T1068)
Fa'ailoga e Maua ai Fesuiaiga: Faailoga Faafoliga/Faagaoi (T1134.001)	Fai ia mae'a Mea e Fai ma Oso ai: Polokalame Faasolo Fesuiaiga o Faatonuga (T1546.004)
Faasologa e Faasolo ai i Totonu: Sootaga Fesuisuia'i e faasolo ai i totonu fale tusi (T1055.001)	Accounts Fa'aaoga: Accounts e Saini ai i Komipiuta (T1078.002)
Accounts Fa'aaoga: Accounts Faalotoifale (T1078.003)	

Faiga 'alo o puipuiga (TA0005)	
Rootkit - Polokalame natia e pulea le faiga (T1014)	Faiga e fa'aaoga e le augaoi i luga initaneti (T1202)
Kopi faanana o Faila po o Faamatalaga (T1027)	Maitauina faasologa mo le saini faatasi atonue fa'aaoga e faaamae'a ai faila matu'ia: Mshta (T1218.005)
O Faila e Faalilolilo po o Faamatalaga: Faasologa o le tuufaatasia po o le faaliliuina o faila (T1027.002)	Maitauina faasologa mo le saini faatasi atonue fa'aaoga e faaamae'a ai faila matu'ia: Regsvr32 (T1218.010)
O Faila e Faalilolilo po o Faamatalaga: Faapipii Faamatalaga Faatamala (T1027.003)	Saini igoa faalilolilo mai le tagata na fausia: Code Signing (T1553.002)
O Faila e Faalilolilo po o Faamatalaga: Tuufaatasi pe a Uma ona Kiliva (T1027.004)	Fesuiaiga atonu e aofia ai suiga o aia faapitoa e maua ai (T1222.002)
Faafoliga: Faatusatusa Igoa Moni po o le Nofoaga (T1036.005)	O se Vaega e Fa'aaoga e Mea vaivai ina ia maua ai Virtualisation/Sandbox Evasion: System Checks (T1497.001)
Faasologa o le Tuuina i Totonu: Thread Execution Hijacking (T1055.003)	Faafoliga (T1036)
Upu Faalilolilo e Tuuina i Totonu e Iloa ai (T1620)	Fesuiai Auala e Tete'e ai: Faaleaoga pe Fesuiai Puipuiga e Tete'e ai (T1562.004)
Faasologa o le Tuuina i Totonu: Faasologa o le Aveesea mai Totonu (T1055.012)	Faalafi Mea e Gaosi e Tagata: Faanana Faila ma Faasinoala (T1564.001)
Aveesea le Faailoilo: Titina ese Faila (T1070.004)	Faalafi Mea e Gaosi e Tagata: Faamalama Faanana (T1564.003)
Aveesea Faailoilo: Timestomp (T1070.006)	Faasolo Faamae'a Faagaoi Flow: DLL Faatonuga e Saili ai le Faagaoi (T1574.001)
Aveesea Faailoilo: Kilia Faamaumauga o Mea na Tutupu (T1070.001)	Faasolo ia Mae'a le Faagaoi: DLL Tuuina i Totonu Fa'aalatua (T1574.002)
Fesuiai Lesitala (T1112)	Auaunaga Upega tafailagi (T1102)
Kopi ese faanana/Feliuai Faila po o Faamatalaga (T1140)	Faafoliga: Gaioiga Faafoliga po o Auaunaga (T1036.004)
Faaleaga Mea e Tete'e ai (T1562)	

Gaoi i luga o initaneti o se auala e fa'aaoga e le augaoi (TA0006)	
Lafoai Agavaa ina ia maua ai saini i totonu i accounts: LSASS Memory (T1003.001)	Taumafaiga a se tagata fa'aaoga e maua ai le auala i fesootaiga: Fafauina o faila (T1552.001)
Lafoai Agavaa ina ia maua ai saini i totonu i accounts: NTDS (T1003.003)	Ave Faamalosi: Fumigaina o Upu Faalilolilo (T1110.001)
Gaioiga o le faateia ma siaki faamaumauga (T1040)	Faamalosia le Faamaoniga (T1187)

Gaoi i luga o initaneti o se auala e fa'aaoga e le augaoi (TA0006)	
Tusi Faamaonia mai Fale Teu Upu Faalilolilo: Keychain (T1555.001)	Gaoi pe Saini Faanana Mea e iloa ai: Au osofai e so'ona fa'aaoga mea e faamaonia ai (T1558.003)
Aoina o Fa'amatalaga Ulufale: Keylogging (T1056.001)	Faateia Faamaoniga o mea e faamaonia ai (T1111)
E ono gaoia talosaga upega tafailagi ma fa'aaoga (T1539)	Gaoi Talosaga e maua ai meaalofa (T1528)
Mea aoga ma faamaoniga e ono taulai mo le so'ona fa'aaogaina (T1212)	Ave Faamalosi: Taumafaiga i Upu faalilolilo (T1110.002)
Aoina o Fa'amatalaga Ulufale: Aoina i Uepu (T1056.003)	Lafoai Agavaa ina ia maua ai saini i totonu i accounts: DCSync (T1003.006)
Agavaa mai mea o teu au upu faalilolilo (T1555)	Agavaa mai mea e teu ai upu faalilolilo: Agavaa mai Upega tafailagi (T1555.003)

Mauaina (TA0007)	
System Service Mauaina o Auala i Masini (T1007)	Maua Faamatalaga o Faatinoga (T1082)
Mauaina o Talosaga i le Window (T1010)	Mauaina le Account: Account faalotoifale (T1087.001)
Lesitala o Faafesili (T1012)	Maua Faamatalaga o Auala o faatino ai, Gaioiga e faatino ai T1082 - Poloketi | MITRE ATT&CK®
Mauaina o Faila ma Faasinoala (T1083)	Maua Taimi o Auala o fai ai (T1124)
Mauaina o fesootaiga i auaunaga (T1046)	Mauaina le tagata e anaina auala o fai ai/ le Tagata Fa'aaoga (T1033)
Mauaina o Gaioiga Faatonutonu mamao mai (T1018)	E tuuina atu mea faigaluega e faataga ai ia maua alagaoa (T1482)
Mauaina o le Account: Account Imeli (T1087.003)	Mauaina le Account: Account i Masini (T1087.002)
Mauaina o Fesootaiga o Auala o Faagasolo ai (T1049)	Siaki mo le maitauina o malu puipuia: Siaki auala o fai ai (T1497.001)
Mauaina Faagasologa (T1057)	Mauaina polokalame komipiuta (T1518)
Mauaina Faatagana a Kulupu: Kulupu o Masini e saini ai (T1069.002)	Mauaina Fesootaiga Faasoa, Gaioiga e fai ai T1135 - Poloketi | MITRE ATT&CK®
Mauaina o Faatulagana o Auala o Faatino ai Fesootaiga: Maua Fesootaiga Initaneti (T1016.001)	

Gaioiga Fa'aalatua (TA0008)	
Auaunaga Faatonutonu mamao mai: Protocol Laumua Mamao (T1021.001)	Auaunaga Faatonutonu Mamao mai (T1021)
Auaunaga Faatonutonu mamao mai: SMB/Windows Admin Shares (T1021.002)	Mea e sui ai mea e faamaonia ai: Pasia le Ticket (T1550.003)
Auaunaga Faatonutonu mamao mai: Windows Remote Management (T1021.006)	Meafaigaluega faaaliliu fa'aalatua (T1570)

Aoina mai (TA0009)	
Faamaumauga mai Auala o Faia ai faalotoifale (T1005)	Teu faatasi Faamaumauga na aoina mai: Tuufaatasi e ala i le Faletusi (T1560.002)
Faamaumauga mai Fesootaiga Faasoa o Komipiuta (T1039)	Aoina mai Imeli: Remote Email Collection (T1114.002)

Aoina mai (TA0009)	
Aoina o Fa'amatalaga Ulufale: Keylogging (T1056.001)	Faamaumauga e le umi o teuina i le masini (T1115)
Otomeki ona aoina mai (T1119)	Faamaumauga mai Faamatalaga mea o teu ai (T1213)
Aoina o Fa'amatalaga Ulufale: E maua ai upega tafailagi (T1056.003)	Faasologa vave: Faasologa vave faatonutonu mamao mai (T1074.002)
Faasologa vave: Faasologa vave faalotoifale (T1074.001)	Teuina o Faamaumauga na Aoina mai (T1560)
Tuufaatasia o Imeli (T1114)	

Kopi faanana o faila (TA0010)	
Kopi faanana i luga o Uaealesi C2 (T1041)	Aveesea faanana o faila i auala e ese a fai ai: Aveesea faanana i luga o auala e fai ai Faaliliuga o Vaega e le fetaui-C2 Protocol (T1048.002)
Kopi faanana i luga o Auala e sui ai (T1048)	Aveesea faanana i luga o auaunaga upega tafailagi: Aveesea faanana i mea e teu ai a le cloud (T1567.002)

Faatonuga ma Pulea (TA0011)	
Ave faagaoi o faamaumauga: faafoliga auala e fai ai (T1001.003)	Auaunaga upega tafailagi: Dead Drop Resolver (T1102.001)
Mea masani o komipiuta e fa'aaoga (T1043)	Auaunaga upega tafailagi: Faatalanoaga auala e tasi (T1102.003)
Faatulagana o Tulafono ma tulaga e manino ai faatalanoaga a polokalame Web Protocols (T1071.001)	Faaliliu mai faila mai tua i totonu (T1105)
Faatulagana o Tulafono ma tulaga e manino ai faatalanoaga a polokalame File Transfer Protocols (T1071.002)	Faamaonia e sui ai: Faamaonia e sui i totonu (T1090.001)
Faamaonia e sui: Faamaonia e sui mai tua (T1090.002)	Vaega komipiuta e le masani ai (T1571)
Faamaonia e sui: Faamaonia e tele ituaiga (T1090.003)	Auala o fesootaiga (T1572)
Auaunaga upega tafailagi: Faatalanoaga i auala e lua (T1102.002)	Uaealesi faaliliuina faalilolilo (T1573)
Uaealesi faaliliu faalilolilo: e fa'aaoga ai ki e lua (T1573.002)	Faaliliuina o faila mai tua agai i totonu (T1105)
Faamaonia e sui, Gaioga e fai ai T1090 - Poloketi | MITRE ATT&CK®	

A'afiaga (TA0040)	
Taofia Auaunaga (T1489)	Titina ese o faamaumauga (T1561)
Tape Auala o Ola ai Komipiuta /Toe Faaola (T1529)	Ave Faamalosi o Alaga'oa (T1496)

Faamaumauga

O se Faamatalaga e te'ena ai

O mea faitino o i lenei taiala faapea o se mataupu lautele ma e lē tatau ona faapea o se fautua faaletulafono pe faamoemoe i ai mo fesoasoani i soo se tulaga faapitoa po o tulaga faafuasei. I soo se mataupu tāua, e tatau ona e sailia fautuaga faapolofesa tuma'oti talafeagai e faatatau i lau oe lava mataupu.

E lē taliaina e le Commonwealth se isi lava matāfaioi po o ni mea e totogi mo ni mea faaleagaina, leiloloa po o ni tupe fa'aalu mafua mai ona o le faalagolago i faamatalaga o loo aofia atu i lenei taiala.

Fa'aaogāina o le Coat of Arms

O tuutuuga i lalo o le Coat of Arms faapea e mafai ona fa'aaogaina o loo auiliiliina i luga o le upega tafailagi a le Matagaluega a le Palemia ma le Kapeneta Commonwealth Coat of Arms Information ma Guidelines | pmc.gov.au.

Mo nisi faamatalaga, pe lipoti mai se mataupu tau le puipuiga mai osofaiga i luga o initaneti faafesootai mai matou:

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

O lenei numera ua avanoa e faaaoga mo na'o totonu o Ausetalia.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre