Fale‘i ki he APT40

PRC MSS founga ngāue fakapulipulí ‘i hono fakahokó

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**

Tēpile hokohokó

Vakai Fakalukufuá 5

Puipuitu‘a 5

Fakamā‘opo‘opo ‘o e ‘ekitivitī 5

‘Ilo‘i ‘o e founga ngāue fakapulipuli 6

Fakanaunau 7

Ngaahi keisi ako 7

Keisi ako 1 8

Fakamā‘opo‘opo fakaepulé 8

Ngaahi ola ‘o e fakatotoló 9

Ngaahi Fakaikiiki 9

Fakafofonga‘i ‘o e ngaahi ‘ivení ‘aki ‘a e fakatātā 9

Fakaikiiki ‘o e vaha‘a taimí 10

Ngaahi founga ‘a e taha ngāue koví 11

Vakai‘i 11

Fuofua a‘ú 11

Ngāue ‘aki 11

A‘u ki he fakaikiiki faka‘ilonga‘í 11

Nga‘unu ‘i he netiueka tatau 11

Tānaki 11

To‘o ‘ikai fakamafai‘i 11

Keisi ako 2 12

Fakamā‘opo‘opo fakaepulé 12

Ngaahi ola ‘o e fakatotoló 13
Fakamā‘opo‘opo ‘o e fakatotoló 13
Ngaahi housi ‘i lotó 13
Vaha‘ataimi fakatotoló 14
Ngaahi founga ‘a e taha ngāue koví 15
Fuofua a‘ú 15
Ngāue ‘aki 15
Matauhi ‘o e a‘ú 15
Fakalahi ki he totonu ke a‘ú 15
A‘u ki he fakaikiiki faka‘ilonga‘í 15
‘Ilo‘i 16
Tānaki 16
Fekau mo e pule‘i 16
‘Ilo‘i mo e ngaahi fokotu‘u ki he fakasi‘isi‘i uesiá 17
‘Ilo‘i 17
Ngaahi Fakasi‘isi‘i Uesiá 20
MITRE ATT&CK – Founga ngāue fakapulipuli fakahisitōlia APT40 ‘oku mahu‘inga 22

Vakai Fakalūkufua:

Puipuitu‘á

Ko e fale‘i ko ‘ení, na‘e fa‘u ia ‘e he Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC), ko e United States Cybersecurity and Infrastructure Security Agency (CISA), ko e United States National Security Agency (NSA), ko e United States Federal Bureau of Investigation (FBI), ko e United Kingdom National Cyber Security Centre (NCSC-UK), ko e Canadian Centre for Cyber Security (CCCS), ko e New Zealand National Cyber Security Centre (NCSC-NZ), ko e German Federal Intelligence Service (BND) and Federal Office for the Protection of the Constitution (BfV), ko e Republic of Korea’s National Intelligence Service (NIS) and NIS’ National Cyber Security Center, mo e Japan’s National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and National Police Agency (NPA) – ‘a ia ‘e ‘uhinga ki ai ko e “ngaahi kautaha fa‘u fale‘í” – ‘okú ne fakamatala‘i ha kulupu faka‘ilekitulōnika ‘a e People’s Republic of China (PRC) ‘a ia ‘oku fakapa‘anga ‘e he pule‘angá mo ‘enau fakamanamana lolotonga ki he ngaahi netiueka ‘Aositelēliá. ‘Oku ngāue ‘aki ‘e he fale‘í ‘a e mahino ‘oku fe‘ilongaki ai ‘a e ngaahi kautaha fa‘u fale‘í ‘o kau ki he fakamanamaná kae pehē ki he ngaahi fakatotolo ‘a e ACSC ‘a e ASD ‘o e ngāue ki ha me‘a ‘oku hoko.

Kuo tāketi‘i ki mu‘a ‘e he kulupu faka‘ilekitulōnika ‘a e PRC ‘oku fakapa‘anga ‘e he pule‘angá ha ngaahi kautaha ‘i he ngaahi fonua kehekehe, kau ai ‘a ‘Aositelēlia mo e ‘Iunaiteti Siteití, pea ko e ngaahi founga ‘oku faka‘ilonga‘i atu ‘i laló ‘oku ngāue ‘aki ma‘u pē ia ‘e he kakai ngāue kovi kehe ‘a e PRC ‘oku fakapa‘anga ‘e he pule‘angá fakamāmanilahi. Ko ia ai, ‘oku tui ‘a e ngaahi kautaha fa‘u fale‘í ‘oku kei hoko pē ‘a e kulupú mo e ngaahi founga tatau ko ha fakamanamana ki he ngaahi netiueka ‘o honau ngaahi fonuá foki.

‘Oku sivi‘i ‘e he ngaahi kautaha fa‘u fale‘í ‘o pehē ‘oku fakahoko ‘e he kulupu ko ‘ení ha ngaahi ngāue kākā faka‘ilekitulōnika ma‘á e PRC Ministry of State Security (MSS). ‘Oku ‘ovalepi ‘a e ‘ekitivitií mo e ngaahi founga ngāué mo e ngaahi kulupu ‘a ia kuo muimui‘i ko e Advanced Persistent Threat (APT) 40 (toe ‘iloa ko e Kryptonite Panda, GINGHAM TYPHOON, Leviathan and Bronze Mohawk ‘i he lipōti fakangāué). Ko e kulupu ko ‘ení kuo lipōti ia kimu‘a na‘e peisi ‘i Haikou, Hainan Province, PRC pea na‘á ne ma‘u ngāue meí he PRC MSS, Hainan State Security Department.[2] ‘Oku tuku atu ‘e he Fale‘i ko ‘ení ha semipolo ‘o ha ngaahi keisi ako mahu‘inga ‘o e ngaahi founga ‘a e fili ko ‘ení ‘i hono fakahoko ki he netiueka ‘o e ongo mamahi ‘e toko ua. ‘Oku mahu‘inga ‘a e ngaahi keisi akó ki he kau fakahoko ngāue malu‘i faka‘ilekitulōniká ke ‘ilo‘i ‘aki, faka‘ehi‘ehi mo fakatonutonu ‘a e ngaahi a‘u ta‘efakamafai‘i ‘a e APT40 ki he ‘enau ngaahi netiuka pē ‘a kinautolú. Ko e ngaahi keisi ako kuo filifili maí ‘a ia kuo fakahoko ki ai ha fakatonutonu fe‘unga ‘o fakasi‘isi‘i ‘a e faingamālie ke toe-‘ohofi ‘aki ‘e he taha ngāue kovi fakamanamana ko ‘ení, pe ha ni‘ihi kehe. ‘I he ‘ene peheé, ‘oku ta‘u lahi ange ‘a e ngaahi keisi akó ‘i hono natulá, ke fakapapau‘i na‘e ‘oange ha taimi fe‘unga ki he ngaahi kautahá ke fakatonutponu ai.

Fakamā‘opo‘opo ‘o e ‘ekitivitií

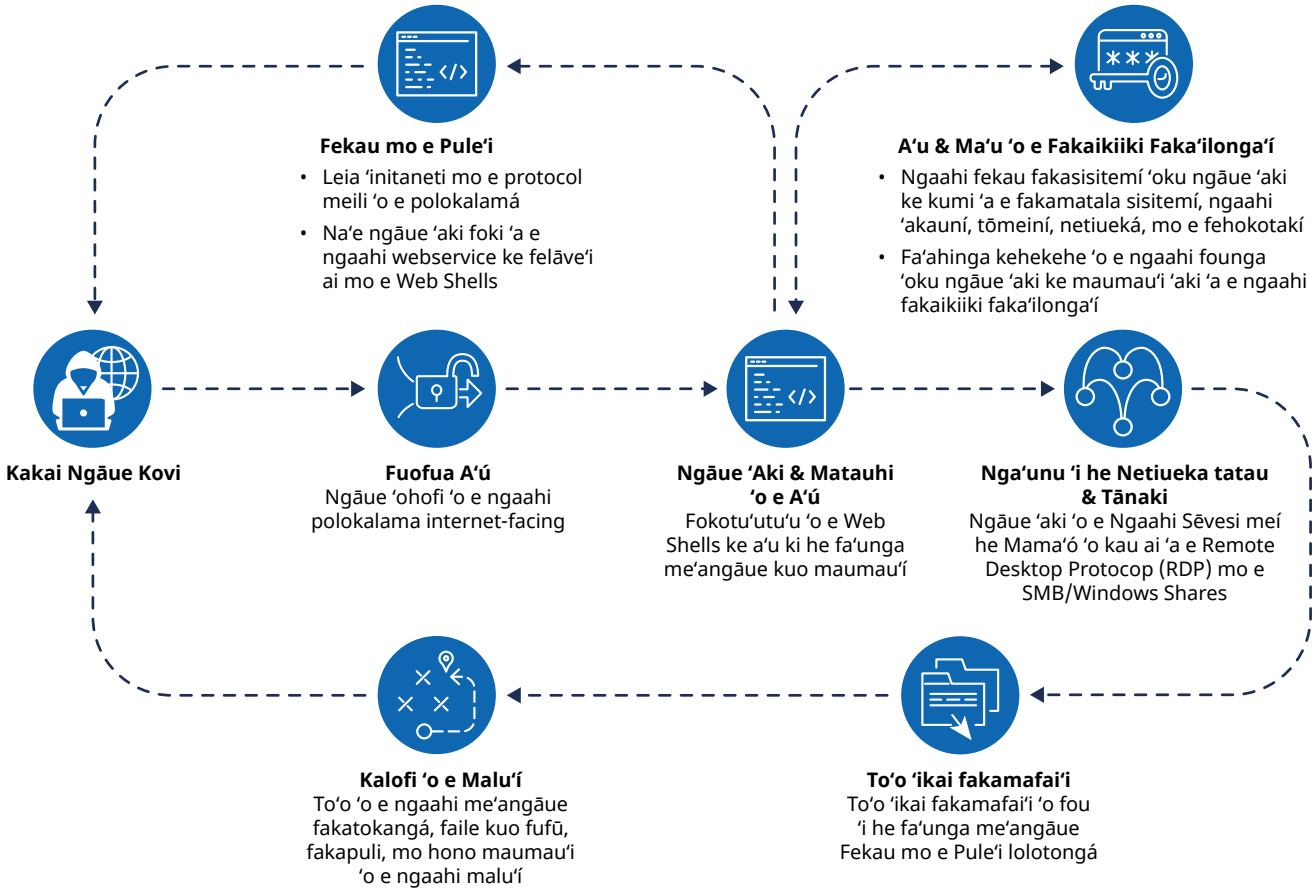
Kuo toutou tāketi ‘e he APT40 ha ngaahi netiueka ‘Aositelēlia kae pehē foki ki he ngaahi netiueka fakapule‘anga mo e sekitoa tāutaha ‘i he vāhefonuá, pea ‘oku hokohoko atu pē ‘a e fakamanamana ‘okú nau fakahoko ki he ‘emau ngaahi netiueká. Ko e founga ngāue fakapulipuli ‘oku fakamatala‘i ‘i he fale‘i ko ‘ení ‘oku siofi ma‘u pē ia ‘o fakahoa ki he ngaahi netiueka ‘Aositelēliá.

Tautefito, ‘oku ma‘u ‘e he APT40 ‘a e ivi ke liliu vave mo ngāue ‘aki mo ‘ohofi ‘a e proof-of-concept(s) (POCs) ‘o ha ngaahi matavaivai fo‘ou pea ngāue ‘aki leva ia ki he ngaahi netiueka ‘oku tāketi‘i ‘a ia ‘okú nau ma‘u ‘a e fa‘unga me‘angāue ‘o e matavaivai ko iá. ‘Oku fakahoko ma‘u pē ‘e he APT40 ha vakai‘i ki he ngaahi netiueka mahu‘ingá, kau ai ‘a e ngaahi netiueka ‘i he ngaahi fonua ‘o e ngaahi kautaha fa‘u fale‘í, ko e siofi ha ngaahi faingamālie ke maumau‘i ‘ene ngaahi tāketí. Ko e vakai‘i ma‘u pē ko ‘ení ‘okú ne fokotu‘u ‘a e kulupú ke ne ‘ilo ‘a e ngaahi me‘angāue tu‘u laveangofuá, kuo mate pe ‘ikai toe tauhi ‘i he ngaahi netiueka mahu‘ingá, pea ke ne fokotu‘utu‘u vave ha ngaahi ngāue ‘ohofí. ‘Oku hoko atu pē ‘a e ola lelei ‘o e ngāue ‘ohofi ‘a e APT40 ‘i he ngaahi matavaivaí meí he fuofua taimí ko e 2017.

‘Oku vave hono ‘ohofi ‘e he APT40 ‘a e ngaahi matavaivai fo‘ou ‘oku ‘ilo‘i fakatokolahi ‘i he polokalama ‘oku lahi hono ngāue ‘akí ‘o hangē ko e Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) mo e Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473). ‘Oku ‘amanaki ‘a e ACSC ‘a e ASD mo e ngaahi kautaha fa‘u fale‘í ke hoko atu hono ngāue ‘aki ‘e he kulupú ‘a e ngaahi POC ki he ngaahi matavaivai fo‘ou ‘oku ‘ilo lahiá ‘i loto ‘i ha ngaahi houa pe ngaahi ‘aho ‘o ha fakahā fakapule‘anga.

2 Potungāue Fakamaau‘anga ‘a ‘Ameliká. 2021. Kuo Faka‘ilo ha Tangata‘i Fonua Siaina ‘e Toko Fā ‘oku Ngāue ‘i he Ministry of State Security ki he A‘u Ta‘efakamafai‘i ki he Global Computer ‘o Tāketi ki he Koloa Fakae‘atamaí mo e Fakamatala Pisinisi Fakapulipuli, Kau Ai ‘a e Fekumi ki he Mahaki Pipihí.

Fakatātā 1: Saati TTP ki he ‘ekitivitī ‘a e APT40



‘Oku hā mai ‘oku sai‘ia ‘a e kulupú ni ‘i he ngāue ‘ohofi ‘o e fa‘unga me‘angāue ‘oku tu‘u laveangofua, public-facing ‘i he ngaahi founga ‘a ia ‘oku fie ma‘u ‘a e felāve‘i mo e taha ngāue ‘akí, ‘o hangē ko e ngaahi kemipeini phishing, pea ‘okú ne fakamahu‘inga‘i lahi ‘a hono ma‘u mai ‘o e ngaahi fakaikiiki faka‘ilonga‘i ‘oku fakalaó ke malava ai ha fa‘ahinga kehekehe ‘o e ngaahi ‘ekitivitī muimui‘í. ‘Oku ngāue ‘aki ma‘u pē ‘e he APT40 ‘a e ngaahi web shell (T1505.003) ki hono matauhi ‘o e malava ‘o e a‘ú, tautautefito ‘i he ngaahi taimi mu‘omu‘a ‘o e saikolo mo‘ui ‘o ha a‘u ta‘efakamafai‘i. Ko e angamahení, hili ‘a e ola lelei ‘a e fuofua a‘ú ‘oku tāfataha ‘a e APT40 ki hono fokotu‘u ‘o e matauhi ‘o e a‘ú ke tauhi ‘aki ‘a e a‘u ‘i he ‘ātakai ‘o e taha mamahí. Neongo iá, ‘i he hoko ‘a e matauhi ‘o e a‘ú ‘i he konga ki mu‘a ‘o ha a‘u ta‘efakamafai‘i, ‘oku lahi ange ‘a e faingamālie ke hā ia ‘i he kotoa ‘o e ngaahi a‘u ta‘efakamafai‘í - ‘o tatau pe ko e hā ‘a e lahi ‘o e maumau‘í pe ko e ngaahi ngāue makehe ‘oku fakahokó.

‘Ilo‘i ‘o e founga ngāue fakapulipuli

Neongo kuo ngāue ‘aki kimu‘a ‘e he APT40 ha ngaahi uepisaiti ‘Aositelēlia kuo maumau‘i ko ha ngaahi housi ki he fekau mo pule‘í (C2) ki he ‘ene ngaahi ngāué, kuo liliu ‘e he kulupú ‘a e founga ko ‘ení (T1594).

Kuo fakakau mai ‘e he APT40 ‘a e akenga fakamāmanilahi hono ngāue ‘aki ‘o e ngaahi me‘angāue kuo maumau‘i, kau ai ‘a e ngaahi me‘angāue ‘ōfisi-si‘isi‘i/‘ōfisi ‘i ‘api (SOHO), ko ha fa‘unga me‘angāue fakangāue mo e ngaahi last-hop redirector (T1584.008) ki he ‘ene ngaahi ngāue ‘i ‘Aositelēliá. Koe‘uhí ko ‘ení kuo malava ‘a e ngaahi kautaha fa‘u fale‘í ‘o fakamatala‘i mo muimui‘i lelei ange ‘a e ngaahi ngāue ‘a e kulupu ko ‘ení.

Ko e lahi ‘o e ngaahi me‘angāue SOHO ko ‘ení kuo mate pe kuo ‘ikai fakataha‘i pea ‘okú ne tuku atu ha tāketi vaivai ki he ngāue ‘ohofi N-day. Hilii hono maumau‘í, ‘oku tuku atu ‘e he ngaahi me‘angāue SOHO ha poini kamata‘i ki he ngaahi ‘ohofí ‘a ia kuo fa‘u ke tuofio lelei pē mo e tulēfiki mo‘oní pea ne fehangahangai mo e ngaahi malu‘i netiueká (T1001.003).

‘Oku ngāue ‘aki ma‘u pē foki ‘a e founga ko ‘ení ‘e he kakai ngāue kovi kehe ‘a e PRC ‘oku fakapa‘anga ‘e he pule‘angá ‘i he kotoa ‘o e māmaní, pea ‘oku lau eni ‘e he ngaahi kautaha fa‘u fale‘í ko ha fakamanamana ‘oku vahevahe. Ki ha fakamatala makehe, vakai ki he ngaahi kaungā fale‘í People’s Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices mo e PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.

‘Oku ngāue ‘aki fakataimi ‘e he APT40 ha fa‘unga me‘angāue kuo fakatau pe lisi ko ha fa‘unga me‘angāue victim-facing C2 ‘i he ‘ene ngaahi ngāué; neongo iá, ‘oku ngali ‘i ai ‘a e holo lahi ‘i he founga ngāue fakapulipuli ko ‘ení.

Fakanaunau

‘Oku vahevahe faka‘ilekitulōnika ‘e he ACSC ‘a e ASD ha ni‘ihi ‘o e ngaahi faile kākā kuo ‘ilo‘i lolotonga ‘a e ngaahi fakatotolo kuo fakamatala‘i atu ‘i laló. Ko e ngaahi faile ko ‘ení kuo ‘apulouti ia ki he VirusTotal ke lava ‘a e malu‘i netiueka lahi angé mo e ngaahi komiunitī ki he malu faka‘ilekitulōniká ‘o mahino‘i lelei ange ‘a e ngaahi fakamanamana ‘okú fie ma‘u kenau malu mei aí.

Ngaahi keisi akó

‘Oku vahevahe ‘e he ACSC ‘a e ASD ‘a e lipōti fakatotolo ‘e ua kuo fakapuliki ‘a e hingoa ‘i aí ke fakahā ‘a e founga ‘oku ngāue ‘aki ‘e he kakai ngāue koví ‘enau ngaahi naunaú mo e founga ngāue fakapulipulí.

MD5	Hingoa ‘o e failé	Fakamatala makehe
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

Keisi ako 1

Ko e keisi ako ko ‘ení kuo fakapuliki ‘a e hingoa ‘i aí ke lava ‘o fakamafola lahi ange ki he kakaí. Ko e kautaha kuo uesiá ‘oku ‘uhinga ki ai ‘i heni ‘ko e kautahá’. Kuo to‘o ‘a e ngaahi fakaikiiki fakamahino paú ke malu‘i ‘a e fakamatala faka‘ilonga‘i ‘o e taha mamahí mo e ngaahi founga ngāue ‘a e ACSC ‘a e ASD ki ha me‘a ‘e hoko.

Fakamā‘opo‘opo fakaepulé

‘Oku fakaikiiki ‘e he lipōti ko ‘eni ‘a e ngaahi ola ‘o e fakatotolo ‘a e ACSC ‘a e ASD ki he ola lelei hono maumau‘i ‘o e netiueka ‘a e kautahá ‘i he vaha‘a ‘o Siulai mo Sepitema 2022. Na‘e ‘oatu ‘a e lipōti fakatotolo ko ‘ení ki he kautahá ke ne fakamā‘opo‘opo ‘a e ‘ekitivī kākā kuo ‘ilo‘í mo e ngaahi fokotu‘u ki he ngāue monomono ki he fa‘ungá. ‘Oku fakahā ‘e he ngaahi olá ko e maumau‘í na‘e fakahoko ‘e he APT40.

‘I he vaeua‘anga ‘o ‘Aokosí, na‘e fakahā ‘e he ACSC ‘a e ASD ki he kautahá ‘o kau ki he ngaahi ngāue kākā ‘i he ‘enau netiueká meí ha me‘angāue ngalingali kuo maumau‘i ‘a ia ‘oku ngāue ‘aki ‘e he kulupú ‘i he konga kimui ‘o ‘Aokosí pea, na‘e fokotu‘utu‘u ‘e he ACSC ‘a e ASD ‘i he loto ki ai ‘a e kautahá, ha ngaahi me‘a fakatokanga ‘a ia ‘oku peisi ‘i he housí ki he ngaahi housi ‘a ia ‘oku ngalingali kuo uesia ‘i he netiueka ‘a e kautahá. Na‘e fakafaingofua ‘e he ngaahi me‘a fakatokanga ko ‘ení ‘a e kau ‘analaiso ngāue ki he me‘a na‘e hokó meí he ACSC ‘a e ASD ke nau fakahoko ha fakatotolo fōlenisiki faka‘ilekitulōnika ‘oku faka‘auliliki. ‘I hono ngāue ‘aki ‘o e teita na‘e ma‘u meí he me‘a fakatokangá, na‘e lava ‘e he kau ‘analaiso mei he ACSC ‘a e ASD ‘o mape‘i ‘a e ‘ekitivitī ‘a e kulupú mo fa‘u ha vaha‘a taimi kuo fakaikiiki ‘o e ngaahi me‘a kuo hoko ‘a ia ‘oku ‘ilo‘í.

Mei Siulai ki ‘Aokosi, ko e ‘ekitivitī tefito ‘a e taha ngāue koví ‘a ia na‘e ‘ilo‘i ‘e he ACSC ‘a e ASD ‘oku kau ai ‘a e:

- fakaikiiki ‘o e housí, ‘a ia ‘oku lava ai ‘e ha taha ngāue koví ‘o fa‘u ‘enau mape pē ‘a kinautolu ‘o e netiueká;
- ngāue ‘aki ‘o e web shell, ‘oange ai ki he taha ngāue koví ‘a e fuofua konga ‘i he netiueká pea ne malava ke ngāue ‘aki ‘a e ngaahi fekaú; pea
- fokotu‘utu‘u ‘o e naunau kehe kuo puke ‘e he taha ngāue koví ki ha ngaahi taumu‘a kākā.

Na‘e ma‘u ‘e he fakatotoló ‘a e fakamo‘oni ‘o e teita pelepelengesi lahi ‘a ia kuo a‘u ki ai mo e fakamo‘oni ‘o e nga‘unu ‘i he netiueka tatau ‘a e kakai ngāue koví ‘i he toenga ‘o e netiueká (T1021.002). Ko e lahi taha ‘o e maumau‘í na‘e tokoni‘i ia ‘aki hono fokotu‘u ‘e he kulupu ‘a e ngaahi faka‘atā lahi ‘i he a‘u ki he netiueká, ko e feleti ‘a e fa‘unga ‘o e netiueká, mo hono ngāue ‘aki ‘o e polokalama ‘ikai malu na‘e fa‘u pē ‘i loto ‘a ia ‘e lava ‘o ngāue ‘aki ki hono ‘apulouti ‘ikai fakangatangata ‘o e ngaahi failé. ‘Oku kau ki he teita kuo to‘o ‘ikai fakamafai‘í ‘a e ngaahi fakaikiiki faka‘ilonga‘i fakangatangata ki he fakamo‘oni‘í ‘a ia na‘e lava ai ‘a e kulupú ‘o hū ki loto, kae pehē ki he fakamatala netiueka ‘a ia te ne faka‘atā ‘a e kakai ngāue koví ke toe ma‘u ‘enau a‘u ‘ikai fakamafai‘í kapau na‘e poloka ‘a e faka‘atā ‘i he fuofua a‘ú. Na‘e ‘ikai ‘ilo‘i ha fakanaunau kākā makehe ‘o mahili atu mei he naunau ‘i he mīsini na‘e ‘uluaki ‘ohofí, neonog iá, ko e a‘u ‘a e kulupú ki he ngaahi fakaikiiki faka‘ilonga‘i mo‘oni mo fakangatangatá ‘e kaniseli ‘aki ia ‘a e fie ma‘u ki ha fakanaunau makehe. ‘Oku fakahā ‘e he ngaahi ola meí he fakatotoló na‘e ngalingali na‘e tāketi‘i ‘e he APT40 ‘a e kautahá ‘i he ‘ilo‘ilopau, ‘o kehe mei he ‘ene tō ko ha taha mamahi ki ha matavaivai ‘a ia ‘oku ‘ilo lahia.

Ngaahi ola ‘o e fakatotoló

‘I he vaeua‘anga ‘o ‘Aokosí 2022, na‘e fakahā ‘e he ACSC ‘a e ASD ki he kautahá ‘oku ‘i ai ha IP kākā kuo fakapapau‘i ‘a ia ‘oku ‘i ai ‘a e tui ‘okú ne fekau‘aki mo ha kulupu faka‘ilekitulōnika ‘oku fakapa‘anga ‘e he pule‘angá kuó ne felāve‘i mo e ngaahi netiueka komipiuta ‘a e kautahá ‘i he vaha‘a ‘o Siulai mo ‘Aokosí. Ko e me‘angāue kuo maumau‘í mahalo na‘e ‘o‘ona ia ‘e ha pisinisi si‘isi‘i pe ha taha ngāue ‘aki mei ‘api.

‘I he konga ki mui ‘o ‘Aokosí, na‘e fokotu‘utu‘u ‘e he ACSC ‘a e ASD ha fakafofonga ‘oku peisi ‘i he housí ki he ngaahi housi ‘i he netiueka ‘a e kautahá ‘a ia na‘e hā mei ai ha fakamo‘oni kuo uesia kinautolu ‘e he maumau‘í.

Na‘e ‘i ai ha ngaahi ngāue ‘aati ‘a ia na‘e mei poupou ki he ngaahi ngāue fakatotoló na‘e ‘ikai ke ‘atā koe‘uhi ko hono toe fokotu‘utu‘u ‘o e loká pe tisaini ‘o e netiueká. Neongo ‘eni, ko e maau ‘a e kautahá ke ‘oatu ‘a e kotoa ‘o e teita ‘oku ma‘ú na‘e malava ai ‘e he kau ngāue ACSC ‘a e ASD ki ha me‘a ‘oku hoko ‘o fakahoko ha ‘analaiso kakato mo fa‘u ha ‘ilo ‘o kau ki he ‘ekitivitī ngalingali na‘e fakahoko ‘e he APT40 ‘i he netiueká.

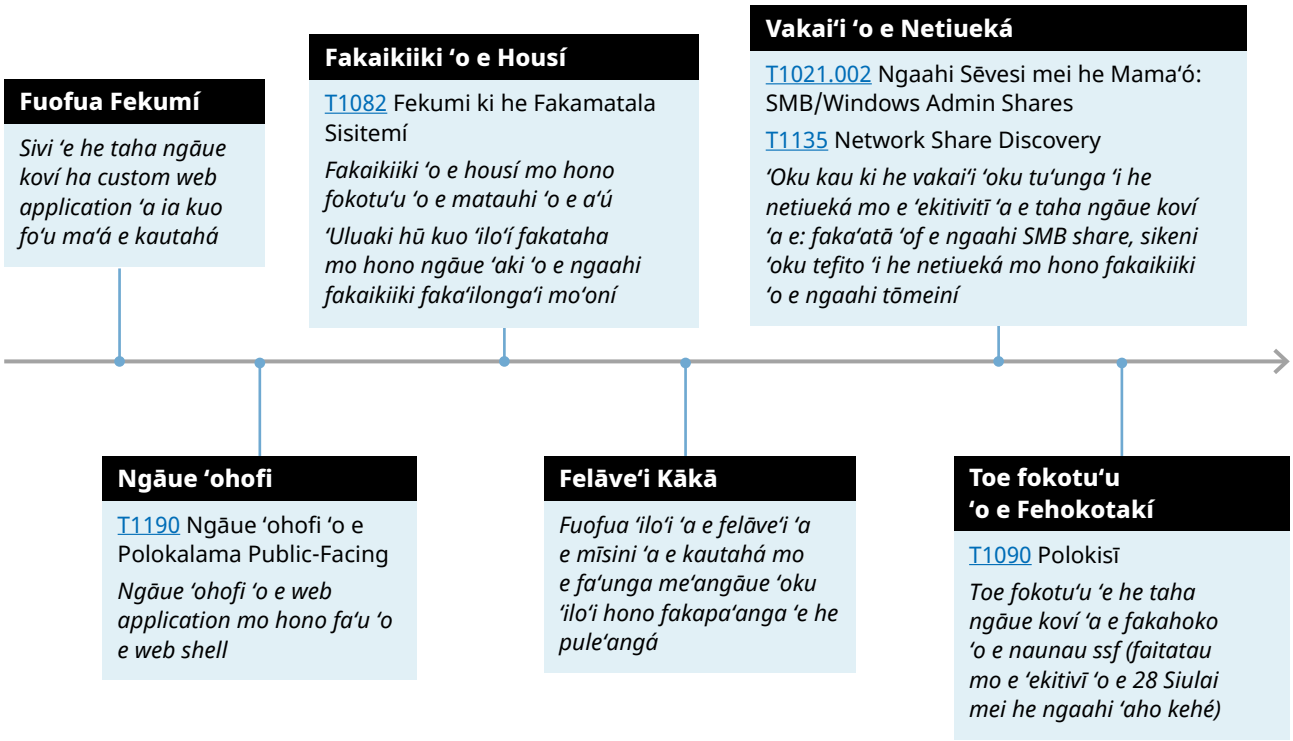
‘I Sepitema, hili ‘a e fealea‘aki mo e ACSC ‘a e ASD, na‘e tu‘utu‘uni ‘e he kautahá ke lisi ‘o faka‘ikai‘i ‘a e IP kuo ‘ilo‘i ‘i he fuofua fakatokangá. ‘I ‘Okatopa, na‘e kamata‘i ‘e he kautahá ‘a e fakatonutonú.

Ngaahi fakaikiiki

Kamta ‘i Siulai, na‘e malava ‘a e kakai ngāue koví ke sivi‘i mo ‘ohofi ha custom web application (T1190) ‘oku lele ‘i he `<webapp>2-ext`, ‘a ia na‘e malava ‘e he kulupú ke fokotu‘u ha feitu‘u ‘i he sone ‘oku ‘ikai fakamahafu ‘i he netiueká (DMZ). Na‘e puke ‘eni ke lau ‘aki ‘a e netiueká fakatou‘osi mo e kotoa ‘o e ngahi tōmeini ‘oku vakai ki aí. Na‘e ngāue ‘aki ‘a e ngaahi fakaikiiki faka‘ilonga‘i kuo maumau‘í (T1078.002) ke fakafehu‘i ‘aki ‘a e Active Directory (T1018) mo to‘o ‘ikai fakamafai‘i ‘a e teitá ‘aki hono faka‘atā ‘o e ngaahi vahevahe faile faka‘ilekitulōnika (T1039) mei he ngaahi mīsini kehekehe ‘i loto ‘i he DMZ. Na‘e fakahoko ‘e he taha ngāue koví ha ‘ohofi Kerberoasting koe‘uhi ke ma‘u mai ‘a e ngaahi fakaikiiki faka‘ilonga‘i fakalao ‘o e netiueká meí ha seeva (T1558.003). Na‘e ‘ikai ‘ilo‘i hano ma‘u ‘e he kulupú ha toe ngaahi poini makehe ‘o ha‘ane ‘i he DMZ pe ko e netiueka ‘i lotó

Fakafofonga‘i fakatātā kalafi ‘o e vaha‘a taimí

‘Oku tuku atu ‘e he vaha‘a taimi ‘i laló ha vakai lahi ange ‘o kau ki he ngaahi tu‘unga tefito ‘o e ‘ekitivitī ‘a e taha ngāue koví ‘a ia kuo ‘ilo‘i ‘i he netiueka ‘a e kautahá.



Vaha‘a taimi kuo fakaikiiki

Siulai: Na‘e fokotu‘u ‘e he kakai ngāue koví ha fuofua fakahoko ki he peesi ‘uluaki ‘o ha custom web application (T1190) ‘a ia kuo fo‘u ma‘á e kautahá (‘a ia ‘oku ‘uhinga ki ai ‘i heni ko e ‘web application’ pe ‘*webapp*’) ‘o fou ‘i he fakahoko transport layer security (TLS) (T1102). Na‘e ‘ikai ‘ilo‘i ha ‘ekitivitī kehe ‘oku mahu‘inga ke fakatokanga‘i.

Siulai: Na‘e kamata ke fakaikiiki ‘e he kakai ngāue koví ‘a e uepisaiti ‘o e web application ko e fekumi ki he ngaahi poini ngata‘angá[2] ke toe fakatotolo‘i.

Siulai: ‘Oku tāfataha ‘a e kakai ngāue koví ‘i he ngaahi ngāue ke ‘ohofi ha poini ngata‘anga pau.

Siulai: ‘Oku lava ‘a e kakai ngāue koví ‘o `POST` lelei ki he seeva uepisaití, mahalo ‘o fakafou ‘i ha web shell ‘a ia kuo fokotu‘u ‘i ha peesi ‘e taha. ‘Oku ‘i ai ha IP hono ua, ‘a ia ‘oku ngalingali kuo ngāue ‘aki ‘e he kakai ngāue kovi tatau, ‘okú ne kamata ke pousi ki he URL tatau. Na‘e fa‘u mo sivi‘i ‘e he kakai ngāue koví ha ni‘ihi ngalingali ko e ngaahi web shells.

‘Oku ‘ikai ‘ilo‘i ‘a e founga pau ‘o e ngāue ‘ohofí, ka ‘oku mahino ‘a e poini ngata‘anga pau ‘a ia na‘e tāketi‘i ke fa‘u ‘aki ‘a e ngaahi faile ‘i he `<webapp>2-ext`.

‘Oku tui ‘a e ACSC ‘a e ASD ko e ngaahi fehokotaki ‘a e ongo tu‘asila IP ko ha konga ‘o e a‘u ta‘efakamafai‘i tatau koe‘uhi ko e faitatau ‘ena kaungá mo e ngaahi fuofua fehokotaki na‘e hoko taki lau miniti pē ‘a e vā mama‘ó.

Siulai: ‘Oku hokohoko atu hono fakahoko ‘e he kulupú ‘a e fakaikiiki ‘o e housí, ‘o kumi ha ngaahi faingamālie fakalahi ki he totonu ke a‘ú, mo hono fokotu‘utu‘u ha web shell kehe. ‘Oku hū ‘a e kakai ngāue koví ki loto ki he web application ‘o ngāue ‘aki ha ngaahi fakaikiiki faka‘ilonga‘i kuo maumau‘i ki he `<firstname.surname>@<organisation domain>`.

‘Oku ‘ikai hā mai kuo a‘usia lelei ‘e he ‘ekitivitī ‘a e kakai ngāue koví ‘a e fakalahi ki he totonu ke a‘ú ‘i he `<webapp>2-ext`. Neongo ia, kuo tafoki ‘a e kakai ngāue koví ki he ‘ekitivitī ‘oku tu‘unga ‘i he netiueká.

Siulai: ‘Oku sivi ‘e he taha ngāue koví ‘a e ngaahi fakaikiiki faka‘ilonga‘i kuo maumau‘í ki ha ‘akauni sēvesi[3] ‘a ia oku ngalingali ke ma‘u ‘oku hardcoded ‘i he ngaahi binaries ‘oku lava ‘o a‘u ki ai ‘i loto.

Siulai: Oku fokotu‘utu‘u ‘e he kakai ngāue koví ‘a e naunau open-source ko e Secure Socket Funnelling, ‘a ia na‘e ngāue ‘aki ke fakahoko ki tu‘a ki he fa‘unga me‘angāue kākaá. ‘Oku ngāue ‘aki ‘a e fehokotakí ke tānolo ‘a e tulēfiki mei he ngaahi mīsini ngāue ‘ohofi ‘a e taha ngāue koví ki loto ki he ngaahi netiueka ‘i loto ‘o e kautahá, ‘a ia ‘oku fakahā hono ngaahi hingoa mīsiní ‘i he ngaahi loka ‘ivení lolotonga ‘enau feinga ke ngāue ‘aki ‘a e ngaahi fakaikiiki faka‘ilonga‘i ki he ‘akau sēvesí.

‘Aokosi: ‘Oku ‘ilo‘i hono fakahoko ‘e he kakai ngāue koví ha ‘ekitivitī ‘oku fakangatangata hono lahí, kau ai ‘a e ‘ikai lava ke toe fokotu‘u ‘a e ngaahi fehokotaki ‘oku kau ai ‘a e ‘akauni sēvesí.

‘Aokosi: ‘Oku fakahoko ‘e he kakai ngāue koví ha fakaikiiki mahu‘inga ki he netiueká mo e Active Directory. ‘Oku iku ‘o ngāue ‘aki ha ‘akauni kehe kuo maumau‘i ke ne faka‘atā ‘a e ngaahi vahevahe faka‘ilekitulōnika[4] ‘i he ngaahi mīsini Windows ‘i loto ‘i he DMZ, ‘o malava ke ola lelei hono to‘o ‘ikai fakamafai‘i ‘o e teitá.

‘Oku ngalingali ko ha ngāue ‘aki kākā ‘eni ‘o ha fakaikiiki faka‘ilonga‘i kuo kaiha‘asi ‘i he ngaahi mīsini ‘oku lava ‘o faka‘atā i he DMZ. Na‘e poloka ‘e he ngaahi firewall ‘a e taha ngāue koví mei hono tāketi‘i ‘o e netiueká ‘aki ‘a e ‘ekitivitī tatau.

‘Aokosi – Sepitema: Na‘e toe fokotu‘u ‘e he naunau SSF ‘a e fehokotaki ki ha IP kākā. ‘Oku ‘ikai ‘ilo hano fakahoko ‘e he kulupú ha ngaahi ‘ekitivitī makehe kae ‘oua kuo poloka ‘enau a‘ú.

Sepitema: ‘Oku poloka ‘e he kautahá ‘a e IP kākaá ‘aki hono lisi ia ‘o faka‘ikai‘i ‘i he ‘enau ngaahi firewalls.

2 ‘I he tu‘unga ko ‘ení, ko e poini ngata‘angá ko e fatongia ia ‘o e web application

3 ‘Oku ‘ikai ha‘i ‘a e ngaahi ‘akauni sēvesí ki he ni‘ihi ngāue ‘aki fakatāutahá, ka ki he ngaahi sēvesí. ‘I ha tōmeini fakakautaha ‘a e Microsoft, ‘oku ‘i ai ha ngaahi fa‘ahinga kehekehe ‘o e ‘akaunί.

4 Ko hono faka‘atā ‘o e ngaahi vahevahe faka‘ilekitulōniká ko e founga ia hono ngaohi ke ‘atā ‘a e ngaahi faile ‘i ha fa‘unga sisitemi faile ki ha taha ngāue ‘aki pe kulupu ngāue ‘aki.

Ngaahi founga ‘a e taha ngāue koví

Ko e fa‘unga me‘angāue MITRE ATT&CK ko ha tānaki‘anga kuo hiki ‘o e ngaahi founga kuo ngāue ‘aki ‘e he kakai ngāue kovi fakamanamaná ‘i he ‘initanetí. Ko e fa‘unga me‘angāué na‘e fa‘u ia ‘e he US not-for-profit The MITRE Corporation mo e ngaahi fatongia tokoni‘i ‘o e fetu‘utakí ‘i he ngaahi lea fakafonuá fakamāmānilahi ‘i he ‘ulungaanga ‘o e taha ngāue kovi fakamanamaná.

‘Oku sivi‘i ‘e he ACSC ‘a e ASD ‘a e ngaahi founga ko ‘ení ke felave‘i mo e ‘ekitivitī kākā ‘a e taha ngāue koví:

Vakai‘i

T1594 – Hua ‘a e Ngaahi Uepisaiti ‘oku ‘O‘ona ‘e he Mamahí

Na‘e fakaikiiki ‘e he taha ngāue koví ‘a e uepisaiti custom web application ke ‘ilo‘i ‘aki ‘a e ngaahi faingamālie ke a‘u ki he netiueká.

Fuofua a‘ú

T1190 – ‘Ohofi ‘o e Public-Facing Application (‘o kau ki hono ‘ohofi ‘o e custom web application)

T1078.002 – Ngaahi ‘Akauni Vēlitī: Ngaahi ‘Akauni Tōmeiní (fekau‘aki mo e hū ‘aki ‘a e ngaahi fakaikiiki faka‘ilonga‘i kuo maumau‘i)

Ko hono ‘ohofi ‘o e ngaahi custom web applications kuo fakahā ‘i he ‘initanetí ‘okú ne tuku atu ha fuofua poini ‘o e a‘ú ki he taha ngāue koví. Na‘e lava ‘a e taha ngāue koví ‘o ngāue ‘aki ‘a mui ange ‘a e ngaahi fakaikiiki faka‘ilonga‘i kuo nau maumau‘í ke fakalahi ‘aki ‘enau a‘u ki he netiueká.

Ngāue ‘aki

T1059 – Fekau mo e Fakatonulea Scripting (fekau‘aki mo e fekau ke fakahoko ‘o fakafou ‘i he web shell)

T1072 – Ngaahi Naunau Fokotu‘utu‘u Polokalama (fekau‘aki mo e ngāue ‘aki ‘e he taha ngāue koví ‘a e naunau open-source Secure Socket Funnelling (SSF) ke IP)

Matauhi ‘o e A‘ú

T1505.003 – Konga Fakapolokalama ‘o e Seevá: Web Shell (fekau‘aki mo hono ngāue ‘aki ‘o ha web shell mo e SSF ke fokotu‘u ha a‘u)

A‘u ki he fakaikiiki faka‘ilonga‘í

T1552.001 – Ngaahi Fakaikiiki Faka‘ilonga‘i meí he Password Stores (fekau‘aki mo e ngaahi faile password ‘oku felāve‘i mo hono fa‘u ‘o e sisitemi pule‘í (BMS))

T1558.003 – Kaiha‘asi pe Tohi Nima Loi ‘a e Ngaahi Tikite Kerberos: Kerberoasting (fekau‘aki mo e ‘ohofi ke ma‘u ‘a e ngaahi fakaikiiki faka‘ilonga‘í)

Nga‘unu ‘i he netiueka tatau

T1021.002 – Ngaahi /Sēvesi mei he Mama‘ó : SMB Shares (fekau‘aki mo hono faka‘tā ‘e he taha ngāue koví ‘a e ngaahi vahevahe faile SMB faka‘ilekitulōnika mei ha ngaahi me‘angāue kehekehe)

Tānaki

T1213 – Teita mei he Ngaahi Tānaki‘anga Fakamatalá (fekau‘aki mo e ngaahi tohi fakahinohino/tohi ngāue kuo ma‘u ‘i he seeva ‘a e BMS)

To‘o ‘ikai fakamafai‘i

T1041 – To‘o ‘ikai fakamafai‘i ‘i he C2 Channel (fekau‘aki mo e to‘o ‘ikai fakamafai‘i ‘e he taha ngāue koví ‘a e teitá mei he Active Directory mo e ngaahi faka‘atā vahevahe faile faka‘ilekitulōniká)

Keisi ako 2

Ko e keisi ako ko ‘ení kuo fakapuliki ‘a e hingoa ‘i aí ke lava ‘o fakamafola lahi ange ki he kakaí. Ko e kautaha kuo uesiá ‘oku ‘uhinga ki ai ‘i heni ‘ko e kautahá’. Kuo to‘o ‘a e ngaahi fakaikiiki fakamahino paú ke malu‘i ‘a e fakamatala faka‘ilonga‘i ‘o e taha mamahí mo e ngaahi founga ngāue ‘a e ACSC ‘a e ASD ki ha me‘a ‘e hoko.

Fakamā‘opo‘opo fakaepulé

‘Oku fakaikiiki ‘e he lipōti ko ‘eni ‘a e ngaahi ola ‘o e fakatotolo ‘a e ACSC ‘a e ASD ki he ola lelei hono maumau‘i ‘o e netiueka ‘a e kautahá ‘i ‘Epeleli 2022. Na‘e ‘oatu ‘a e lipōti fakatotolo ko ‘ení ki he kautahá ke ne fakamā‘opo‘opo ‘a e ‘ekitivī kākā kuo ‘ilo‘í mo e ngaahi fokotu‘u ki he ngāue monomono ki he fa‘ungá. ‘Oku fakahā ‘e he ngaahi olá ko e maumau‘í na‘e fakahoko ‘e he APT40.

‘I Mē 2022, na‘e fa fakahā ‘e he ACSC ‘a e ASD ki ha kautaha ‘o kau ki ha ‘ekitivitī kākā ‘okú ne uesia ‘a e netiueka ‘a e kautahá talu mei ‘Epeleli 2022. Hili ko iá, na‘e fakahā ‘e he ACSC ‘a e ASD kuo nau ‘ilo‘i ha polokalama kākā ‘i ha seeva internet-facing ‘a ia ‘okú ne ‘oatu ‘a e pōtolo hū ma‘á e a‘u fakakautaha mei he mama‘ó ki he kautahá. Na‘e ngāue ‘aki ‘e he seevá ‘a e hū mei he mama‘ó mo e koloa ki hono pule‘i ‘o e fakamatala faka‘ilonga‘í pea ‘e ‘uhinga ki ai ‘i he lipōti ko ‘ení ko e ‘naunau kuo maumau‘í.‘ ‘Oku fakaikiiki ‘e he lipōtí ‘a e ngaahi ola ‘o e fakatotoló mo e fale‘i fakatonutonu kuo fa‘u ma‘á e kautahá ke ne ngāue ‘aki ki he fakatotolo kuo fakahoko ‘e he ACSC ‘a e ASD.

‘Oku fakahā ‘e he fakamo‘oní na‘e maumau‘i ‘a e konga ‘o e netiueka ‘a e kautahá ‘e he kakai ngāue kovi ‘i he ‘initanetí ‘o fou ‘i he pōtolo hū ‘aki ‘a e a‘u mei he mama‘ó talu mei ‘Epeleli 2022. Ko e seeva ko ‘ení na‘e ala maumau‘i ia ‘e ha kakai ngāue kovi kehekehe, pea na‘e ala uesia ia ‘e ha matavaivai ko e remote code execution (RCE) ‘a ia na‘e lahi hono fakahā ‘o ofi ‘i he taimi ‘o e maumau‘í.

Ko e ‘ekitivitī tefito ‘a e taha ngāue koví ‘a ia na‘e ‘ilo‘i ‘e he ACSC ‘a e ASD ‘oku kau ai ‘a e:

- fakaikiiki ‘o e housí, ‘a ia ‘oku lava ai ‘e ha taha ngāue koví ‘o fa‘u ‘enau mape pē ‘a kinautolu ‘o e netiueká;
- ngāue ‘ohofi ‘o e ngaahi polokalama internet-facing mo e ngāue ‘aki ‘o e web shell, ‘oange ai ki he taha ngāue koví ‘a e fuofua konga ‘i he netiueká pea ne malava ke ngāue ‘aki ‘a e ngaahi fekaú
- ngāue ‘ohofi ‘o e ngaahi matavaivai ‘i he polokalamá mo fakalahi ‘a e ngaahi totonú; mo e
- tānaki ‘o e fakaikiiki faka‘ilonga‘í ke lava ‘a e nga‘unu ‘i he netiueka tatau

Na‘e ‘ilo ‘e he ACSC ‘a e ASD hono to‘o ‘ikai fakamafai‘i ‘e ha taha ngāue koví ha ngaahi pea ‘e lau ngeau lahi ‘o e username makehe mo e password ‘i he naunau kuo maumau‘í ‘i ‘Epeleli 2022, kae pehē ki ha ngaahi fika fakamo‘oni‘i multi-factor kehekehe mo ha ngaahi ngāue ‘aati fakatekinikale ‘oku felāve‘i mo e ngaahi fakataha‘anga a‘u mei he mama‘ó. ‘I hano toe vakai‘i ‘e he kautahá, na‘e ‘ilo‘i ai ‘oku mo‘oni ‘a e ngaahi passwords. Ko e sivi ‘a e ACSC ‘a e ASD ngali na‘e tānaki ‘e taha ngāue koví ‘a e ngaahi ngāue ‘aati ko ‘ení ke puke fakamālohi pe fa‘u ‘aki ha sēsini hū meí he mama‘ó ko ha taha ngāue ‘aki fakalao, mo a‘u ki he netiueka kautaha ‘i loto ‘a e kautahá ‘o ngāue ‘aki ha ‘akauni taha ngāue ‘aki ‘oku mo‘oní.

Ngaahi ola ‘o e fakatotoló

Fakamā‘opo‘opo ‘o e fakatotoló

Na‘e fakapapau‘i ‘e he ACSC ‘a e ASD na‘e maumau‘i ‘e he taha ngāue kovi ‘a e (ngaahi) naunau kuo maumau‘í ‘a ia ‘okú nau fakahoko ‘a e ngaahi sēsini hū meí he mama‘ó ki he kau ngāue ‘a e kautahá mo ngāue ‘aki ‘a e maumau‘i ko ‘ení ke feinga ke fakahoko ‘aki ha toe ‘ekitivitī. Ko e ngaahi naunau ko ‘ení ‘oku ‘i ai honau ngaahi house three load-balanaced ‘a ia na‘e ‘ilo‘i ai ‘a e fuofua fakamo‘oni ‘o e maumau‘í. Na‘e tāpuni ‘e he kautahá ‘a e ua ‘o e ngaahi housi three load-balanced ‘i ha taimi nounou pē hili ‘a e fuofua maumau‘í. Tupu mei ai, ko e ‘ekitivitī hoko aí na‘e hoko ia ‘i ha housi pē ‘e taha. Ko e ngaahi seeva kehe ‘oku fekau‘aki mo e naunau kuo maumau‘í na‘e load-balanced foki mo ia ‘i ha natula tatau. Koe‘uhí ke lava ‘o lau, ko e kotoa ‘o e ngaahi naunau kuo maumau‘í ‘oku ‘uhinga ki ai ‘i he lahi taha ‘o e lipōti ko ‘ení ko ha ‘naunau tāutaha‘.

‘Oku ‘i ai ‘a e tui na‘e ngāue ‘aki ‘e he taha ngāue kovi ha ngaahi matavaivai ‘oku ‘ilo lahia ki hono fokotu‘utu‘u ‘o e ngaahi web shell ki he naunau kuo maumau‘í mei ‘Epeleli 2022 ‘o faai atu. ‘Oku sivi‘i ‘a e kau ngāue kovi fakamanamaná kuo ma‘u ‘a e ngaahi totonu kuo fakalahí ‘i he naunaú. Na‘e ‘ikai lava ‘e he ACSC ‘a e ASD ke fakapapau‘i ‘a e tu‘unga kakato ‘o e ‘ekitivitií koe‘uhi ko e ‘ikai ke ‘i ai ha loka ‘e ma‘ú. Neongo iá, ‘oku tala ‘e he fakamo‘oni ‘i he me‘angāué ‘a hono a‘usia ‘e he taha ngāue kovi ‘a e ngaahi me‘a ko ‘ení:

- Ko hono tānaki ‘o e ngaahi pea ‘e lau ngeau lahi ‘o e username makehe mo e password; mo e
- Ko hono tānaki ‘o e ngaahi ngāue ‘aati fakatekinikale ‘a ia ‘oku ngalingali na‘a ne faka‘atā ‘a e taha ngāue kovi ke ne a‘u ki ha sēsini fa‘unga me‘angāue virtual desktop (VDI) ko ha taha ngāue ‘aki fakalao ia.

‘Oku sivi‘i ‘e he ACSC ‘a e ASD na‘e feinga ‘a e taha ngāue kovi ke fakalahi hono maumau‘i ‘o e netiueka ‘a e kautahá. Ko e ngaahi ngāue ‘aati kuo to‘o ‘ikai fakamafai‘i ‘e he taha ngāue kovi ngalingali na‘e faka‘atā ‘aki kinautolu ke puke fakamālohi pe kamata‘i ha ngaahi sēsini virtual desktop ko ha taha ngāue ‘aki fakalao ia, ngalingali ko ha taha ngāue ‘aki na‘a nau fili, kau ai ‘a e kau ‘etiminí. Ngalingali na‘e ngāue ‘aki ‘e he taha ngāue kovi ‘a e faka‘atā a‘u ko ‘ení ke fakalahi ‘ene maumau‘i ‘a e ngaahi sēvesi ‘a e kautahá ke a‘usia ‘a e matauhi ‘o e a‘ú mo ha ngaahi taumu‘a kehe.

Na‘e ‘ikai ke ‘asi ha fakamo‘oni ‘o ha maumau‘i ‘i he ngaahi naunau kehe ‘a e kautahá ‘i loto ‘i he ‘ātakai pule‘i ‘o e fakahoko ngāue housí.

A‘u

Na‘e tuku atu ‘e he housi ‘oku ‘i ai ‘a e naunau kuo maumau‘í ha fakamo‘oni‘i ‘o fakafou ‘i he Active Directory mo ha webserver, ki he ni‘ihi ngāue ‘aki ‘oku fakafehokotaki ki he ngaahi sēsini VDI (T1021.001).

Tu‘u‘anga	Ngaahi hingoa ‘o e housi (load-balanced) naunau kuo maumau‘í
Datacentre 1	HOST1, HOST2, HOST3

‘Oku kau foki ‘i he fa‘unga me‘angāue ‘o e naunaú ‘a e a‘u ki he ngaahi housi gateway ‘a ia ‘okú ne tuku atu ha tānolo ki he VDI ma‘á e taha ngāue ‘akí, ‘i he hili pē ‘enau ma‘u ha faka‘ilonga ‘o e fakamo‘oni‘í ‘a ia ‘oku fo‘u mo taunilotu meí he naunaú.

Na‘e ‘ikai ke ‘i ai ha fakamo‘oni ‘o ha maumau‘í ‘o ha taha ‘o e ngaahi housi ko ‘ení. Neongo iá, ‘oku hā mei he ngaahi loka ‘o e ngaahi housi gateway ki he ‘aú ‘a e fakamo‘oni ‘o e ngaahi felāve‘i lahi mo e ngaahi tu‘asila IP kākā ‘oku ‘ilo‘i. ‘Oku ngalingali ‘oku hā mei heni ha ‘ekitivitī na‘e hoko ‘i he housi ko ‘ení, pe na‘e ‘au ‘a e ngaahi fehokotaki netiueka mo e fa‘unga me‘angāue ‘a e taha ngāue kovi fakamanamaná ki he housi ko ‘ení. Na‘e ‘ikai lava ‘o fakapapau‘i ‘a e natula ‘o e ‘ekitivitī ko ‘ení ‘o ngāue ‘aki ‘a e fakamo‘oni oku ma‘ú ka ‘oku ne tala na‘e feinga ‘a e kulupú ke nga‘unu ‘i he netiueka tatau ‘i he netiueka ‘a e kautahá (TA0008).

Ngaahi housi ‘i lotó

Na‘e fakatotolo‘i ‘e he ACSC ‘a e ASD ‘a e teita fakangatangata mei he konga netiueka ‘i loto ‘a e kautahá. ‘Ekitivitī kākā na‘e feinga pe kuo ola lelei ‘a ia ‘oku ‘ilo‘i ‘ene uesia ‘a e konga netiueka ‘i loto ‘o e kautahá kau ai ‘a e a‘u ‘a e taha ngāue kovi ki he ngaahi ngāue ‘aati ‘oku felāve‘i mo e VDI, ko e scraping ‘o ha seeva SQL ‘i loto (T1505.001), mo e tulēfiki ‘oku ‘ikai ke fakamatala‘i ‘a ia ‘oku ‘ilo‘i ‘oku ‘alu mei he ngaahi tu‘asila IP kākā ‘oku ‘ilo‘i ‘o fou ‘i he ngaahi naunau gateway ki he a‘ú (TA0011).

Na‘e tānaki ‘e he kulupú ‘o ngāue ‘aki ‘enau a‘u ki he naunau kuo maumau‘í, ‘a e ngaahi username mo‘oni, password (T1003), mo e ngaahi tu‘unga ‘o e faka‘ilonga MFA (T1111). Na‘e tānaki foki ‘e he kulupú ‘a e JSON Web Tokens (JWTs) (T1528), ‘a ia ko ha ngāue ‘aati fakamo‘oni‘i ‘oku ngāue ‘aki ke fa‘u ha ngaahi sēsini hū ‘a e virtual desktop. ‘Oku ngalingali na‘e lava ‘a e taha ngāue kovi ke ne ngāue ‘aki eni ke fa‘u pe puke fakamālohi ‘a e ngaahi sēsini virtual desktop (T1563.002) mo a‘u ki he konga netiueka ‘i loto ‘i he kautahá ko ha taha ngāue ‘aki fakalao ia (T1078).

Na‘e ngāue ‘aki ‘e he taha ngāue koví ‘a e naunau kuo maumau‘í ke ne scrape ha seeva SQL (T1505.001), ‘a ia na‘e ‘i he netiueka ‘i loto ‘i he kautahá. ‘Oku ngalingali na‘e a‘u ‘a e taha ngāue koví ki he teitá.

‘Oku hā mei he fakamo‘oni ‘oku ma‘u mei he naunau gateway ki he a‘ú na‘e hoko ‘a e tulēfiki netiueká ‘o fou pe ki he me‘angāue ko ‘ení mei he ngaahi tu‘asila IP kākā ‘oku ‘ilo‘i. Hangē ko ia ‘oku fakamatala‘i ‘i ‘olungá, ‘oku ala tala ‘e he me‘a ni kuo uesia pe kuo ngāue ‘aki ‘e he kakai ngāue kākā ‘i he ‘initanetí ‘a e me‘angāue ko ‘ení, ‘o fakaangaanga ke fakataumu‘a ki he netiueka ‘i lotó.

Vaha‘a taimi fakatotoló

‘Oku tuku atu ‘e he lisi ‘i laló ha vaha‘a taimi ‘o e ngaahi ‘ekitivitī tefito ‘a ia kuo ‘ilo‘i lolotonga ‘a e fakatotoló.

Taimí	Me‘a Na‘e Hokó
‘Epeleli 2022	‘Oku fengāue‘aki ‘a e ngaahi tu‘asila IP kākā ‘oku ‘ilo‘i mo e housi HOST7 gateway ki he a‘ú. Na‘e ‘ikai lava ‘o fakapapau‘i ‘a e natula ‘o e ngaahi fengāue‘akí.
‘Epeleli 2022	Ko e kotoa ‘o e ngaahi housí, HOST1, HOST2 mo e HOST3, na‘e maumau‘i ia ‘e ha taha pe kakai ngāue kākā, pea na‘e fokotu‘u ‘a e ngaahi web shell ki he ngaahi housí. Na‘e fa‘u ha faile loka pe na‘e liliu ia ‘i he HOST2. ‘Oku ‘i ai ha me‘a fakaikiiki faka‘ilonga‘i ‘i he faile ko ‘ení ‘a ia ‘oku ngalingali na‘e puke ‘e ha taha ngāue kākā. Na‘e liliu ‘a e ngaahi faile /etc/security/opasswd and /etc/shadow files ‘i he HOST1 mo e HOST3, ‘oku tala ai na‘e liliu ‘a e ngaahi password. ‘Oku tala ‘e he fakamo‘oni ‘oku ma‘u ‘i he HOST1 na‘e liliu ‘a e password ki he taha ngāue ‘aki ‘sshuser‘.
‘Epeleli 2022	Na‘e tāpuni ‘e he kautahá ‘a e HOST2. Na‘e fa‘u ha ngaahi web shell makehe (T1505.003) ‘i he HOST1 mo e HOST3. Na‘e fehangahangai ‘a e HOST1 mo e ngaahi feinga fakamālohi SSH mei he HOST3. Na‘e liliu ha faile loka (T1070) ‘i he HOST3. ‘Oku ‘i ai ha me‘a fakaikiiki faka‘ilonga‘i ‘i he faile ko ‘ení (T1078) ‘a ia ‘oku ngalingali na‘e puke ‘e ha taha ngāue kākā. Na‘e puke ‘a e ngaahi JWT (T1528) pea tuku atu ia ki tu‘a ki ha faile ‘i he HOST3. Na‘e tāpuni ‘e he kautahá ‘a e HOST3. Ko e kotoa ‘o e ‘ekitivitī na‘e hoko hili ‘a e taimi ko ‘ení na‘e hoko ia ‘i he HOST1.
‘Epeleli 2022	Na‘e fa‘u ha ngaahi web shell makehe ‘i he HOST1 (T1505.003). Na‘e puke ‘a e ngaahi JWT pea tuku atu ia ki tu‘a ki ha faile ‘i he HOST1.
‘Epeleli 2022	Na‘e fa‘u ‘a e ngaahi web shell makehe ‘i he HOST1 (T1505.003), pea ‘oku fengāue‘aki ha tu‘asila IP kākā ‘oku ‘ilo‘i mo e housi (TA0011). ‘Oku fengāue‘aki ha tu‘asila IP kākā ‘oku ‘ilo‘i mo e housi HOST7 gateway ki he a‘ú.
Mē 2022	‘Oku fengāue‘aki ‘a e ngaahi tu‘asila IP kākā ‘oku ‘ilo‘i mo e housi HOST7 gateway ki he a‘ú (TA0011). ‘Oku fehokotaki ‘a e ‘iveni fakamo‘oni‘i ‘o ha taha ngāue ‘aki ki ha tu‘asila IP kākā ‘oku ‘ilo‘i ‘i he ngaahi loka ‘i he HOST1. Na‘e fa‘u ‘a e ngaahi web shell makehe ‘i he housi ko ‘ení (T1505.003).
Mē 2022	Na‘e liliu ‘e he taha ngāue koví ha tohi ‘i he HOST1 (T1543). ‘Oku ma‘u ‘i he tohí ‘a e ngāue ‘a ia te ne ala scrape ‘a e teitá mei ha seeva SQL ‘i loto.
Mē 2022	Na‘e liliu fakamuimui ha faile loka makehe ‘i he HOST1 (T1070). ‘Oku ‘i he faile ko ‘ení ‘a e ngaahi pea username mo e password ki he netiueka ‘a e kautahá, ‘a ia ‘oku ‘i ai ‘a e tui ‘oku mo‘oni (T1078).
Mē 2022	Na‘e liliu fakamuimui taha ha faile loka makehe (T1070). ‘Oku ‘i ai ‘a e ngaahi JWT ‘i he fale ko ‘ení kuo tānaki mei he HOST1.
Mē 2022	Na‘e fa‘u ha ngaahi web shell makehe ‘i he HOST1 (T1505.003). ‘I he ‘aho ko ‘ení, na‘e lipōti ‘e he kautahá ‘a hono ‘ilo‘i ‘o ha web shell ‘a ia ko hono ‘aho fa‘ú ‘i ‘Epeleli 2022 ki he ACSC a e ASD
Mē 2022	Na‘e fa‘u ha ngaahi scripts ‘i he HOST1, ‘o kau ai ha taha ‘oku ui ko e Log4jHotPatch.jar.
Mē 2022	Na‘e ngāue ‘aki ‘a e fekau iptables-save ke tānaki atu ha pooti ‘e ua ‘oku ava ki he housi gateway ki he a‘ú. Ko e ongo pootí ko e 9998 mo e 9999 (T1572).

Ngaahi founga ‘a e taha ngāue koví

‘Oku faka‘ilonga‘i atu ‘i lalo ‘a e ngaahi founga kehekehekuo ‘ilo‘i lolotonga ‘a e fakatotoló.

Fuofua A‘ú

T1190 Ngāue ‘ohofi ‘o e polokalama public facing

‘Oku ngalingali na‘e ‘ohofi ‘e he kulupú ‘a e RCE, fakalahi ‘a e totonú, mo e ngaahi matavaivai hono kalafi o e fakamo‘oni‘í ‘i he hū ‘aki ‘a e a‘u mei he mama‘ō mo e koloa pule‘i ‘o e fakamatala faka‘ilonga‘í ke mau ‘a e fuofua a‘u ki he netiueká.

‘Oku lau ko e founga ki he fuofua a‘ú ‘a ia ‘oku ngalingali tahá koe‘uhi ko e ngaahi me‘a ko ‘ení:

- Na‘e tu‘u laveangofua ‘a e seevá ki he ngaahi CVE ‘i he taimi ko iá;
- Ngaahi ngāue ke ‘ohofi ‘a e ngaahi matavaivai ko ‘ení mei ha fa‘unga me‘angāue ‘oku ‘ilo‘i ‘a e taha ngāue koví; pea
- Ko e fuofua ‘ekitivitī kākā ‘i loto kuo ‘ilo‘í na‘e hoko ia ‘i ha taimi si‘i pē hili ‘a e ngaahi feinga ‘ohofi kuo fakahokó.

Ngāue ‘aki

T1059.004 Fekau mo e Fakatonulea Scripting: Unix Shell

Na‘e ola lelei hono ‘ohofi ‘e he kulupú ‘a e ngaahi matavaivai ‘i ‘olungá na‘e ngalingali na‘e lava ‘o ngāue ‘aki ‘a e ngaahi fekau ‘i ha Uni shell ‘a ia ‘oku ma‘u ‘i he naunau kuo uesia. ‘Oku ‘ikai lava ‘o tuku atu ‘a e ngaahi fakaikiiki ‘o e ngaahi fekau ‘oku ngāue ‘aki ‘e he kakai ngāue kakaá.

Matauhi ‘o e A‘ú

T1505.003 Konga Fakapolokalama ‘o e Seevá: Web Shell

Na‘e fokotu‘utu‘u ‘e he kakai ngāue koví ‘a e ngaahi web shells lahi ‘i he naunau kuo uesiá. ‘Oku malava na‘e fokotu‘utu‘u ‘e ha kakai makehe ngāue koví tokolahi ‘a e ngaahi web shell, ka ko e toko si‘i pē ‘o e kau ngāue koví ‘oku nau fakahoko ha ‘ekitivitī ‘o ngāue ‘aki ‘a e ngaahi web shell ko ‘ení. Na‘e mei faka‘atā ‘e he ngaahi web shell hono ngāue ‘aki ‘e he taha ngāue koví ‘a e arbitrary command ‘i he ngaahi naunau kuo maumau‘í.

Fakalahi ‘o e totonu ke a‘ú

T1068 Ngāue ‘Ohofi ‘o e Fakalahi ‘o e Totonú

‘Oku ‘ikai fakamatala‘i ‘e he fakamo‘oni ‘oku ma‘ú ‘a e tu‘unga ‘o e totonu ke a‘u kuo ma‘u ‘e he kakai ngāue koví. Neongo iá, na‘e mei a‘usia ‘e he kakai ngāue koví ‘o ngāue ‘aki ‘a e ngaahi web shell, ha tu‘unga totonu ki he a‘ú ‘oku ala fakahoa ki he tu‘unga ‘o e seeva uepisaití ‘i he naunau kuo maumau‘í. Na‘e mei faka‘atā ‘e he ngaahi matavaivaí ‘oku tui na‘e ‘i ai ‘i he naunau kuo maumau‘í ‘a e kau ngāue koví kenau ma‘u ‘a e ngaahi tefito‘i totonú.

A‘u ki he fakaikiiki faka‘ilonga‘í

T1056.003 Input Capture: Web Portal Capture

Na‘e hā mei he fakamo‘oni ‘i he naunau kuo maumau‘í na‘e puke ‘e he taha ngāue koví ha ngaahi pea ‘e laui ngeau ‘o e username-password, ‘i he tohi mahino, ‘a ia ‘oku ‘i ai ‘a e tui ‘oku mo‘oni. ‘Oku ngalingali na‘e ma‘u eni ‘o ngāue ‘aki ha liliu ‘e ni‘ihi ki he founga ngāue totonu ki he fakamo‘oni‘i ‘a ia ‘oku ne tuku atu ‘a e ngaahi fakaikiiki faka‘ilonga ki ha faile.

T1111 Fakamoveuveu ki he Fakamono‘oni‘i Multi-Factor

Na‘e puke foki ‘e he taha ngāue koví ‘a e tu‘unga ‘o e ngaahi faka‘ilonga MFA ‘a ia ‘oku tauhoa ki he ngaahi hū ‘oku fakalaó. ‘Oku ngalingali na‘e puke ‘a e ngaahi me‘a ko ‘ení ‘aki hono liliu ‘o e founga ngāue totonu ki he fakamo‘oni‘í ‘a ia ‘oku ne tuku atu ‘a e ngaahi tu‘unga ko ‘ení ki ha faile. ‘Oku ‘ikai ke ‘i ai ha fakamo‘oni ki hono maumau‘i ‘o e ‘seeva fakapulipulí’ ‘a ia ‘oku ne tauhi ‘a e ngaahi tu‘unga makehe ‘oku ne tuku atu ‘a e malu‘i ‘o e ngaahi faka‘ilonga MFA.

T1040 Fakanamunamu ‘o e Netiueká

‘Oku ‘i ai ‘a e tui kuo puke ‘e he taha ngāue koví ‘a e ngaahi JWT ‘aki ‘a e tulēfiki HTTP ‘i he naunau kuo maumau‘í. ‘Oku ‘i ai ‘a e fakamo‘oni na‘e ngāue ‘aki ‘a e ‘iūtilitī tcpdump ‘i he naunau kuo maumau‘í, ‘a ia ‘oku ngalingali ko e founga ia na‘e puke ‘aki ‘e he taha ngāue koví ‘a e ngaahi JWT ko ‘ení.

T1539 Kuki ki hono Kaiha‘asi ‘o e Sēsini ‘i he ‘Initanetí

Hangē ko hono fakamatala‘i ‘i ‘olungá, na‘e puke ‘e he taha ngāue koví ‘a e ngaahi JWT, ‘a ia ‘oku faitatau mo e ngaahi kūkisi sēsini ‘i he ‘initanetí. Na‘e mei lava ‘o toe ngāue ‘aki ‘eni ‘e he taha ngāue koví ke fokotu‘u ha a‘u ‘oku toe lahi angé.

Fekumi

T1046 Fekumi ki he Sēvesi Netiueká

‘Oku ‘i ai ‘a e fakamo‘oni na‘e ngāue ‘aki ‘a e network scanning utility nmap ‘i he naunau kuo maumau‘í ke sikeni hangaahi naunau kehe ‘i he konga netiueka tatau. Na‘e ngalingali ngāue ‘aki ‘eni ‘e he taha ngāue koví ke kumi ‘aki ha ngaahi sēvesi netiueka kehe ‘e ala a‘u ki ai ‘a ia ‘oku ala hā mei ai ha ngaahi faingamālie ki ha nga‘unu ‘i he netiueka tatau.

Tānaki

‘Oku ‘ikai fakahā ‘e he fakamo‘oni ‘oku ma‘ú ‘a e founga na‘e tānaki ‘aki ‘e he kakai ngāue koví ‘a e fakamatalá pe ko e hā ‘a e me‘a totonu na‘e tānaki mei he naunau kuo maumau‘í pe mei he ngaahi sistemi kehé. Neongo iá, ‘oku ngalingali na‘e ‘au ‘a e kakai ngāue koví ki he kotoa ‘o e ngaahi faile ‘i he naunau kuo maumau‘í, kau ai ‘a e ngaahi fakaikiiki faka‘ilonga‘i kuo puké (T1003), ngaahi tu‘unga ‘o e faka‘ilonga MFA (T1111), mo e ngaahi JWT kuo fakamatala‘i ‘i ‘olungá.

Fekau mo e pule‘i

T1071.001 Protocol ‘o e Leia Polokalamá: Ngaahi Lao ‘i he ‘Initanetí

Na‘e ngāue ‘aki ‘e he kakai ngāue koví ‘a e ngaahi web shell ki he fekaú mo e pule‘í. Na‘e mei paasi ‘a e ngaahi fekau web shell ‘i he HTTPS ‘o ngāue ‘aki ‘a e seeva uepisaiti lolotonga ‘i he naunaú (T1572).

T1001.003 Teita kuo Fufū: Protocol Impersonation

Na‘e ngāue ‘aki ‘e he kakai ngāue koví ‘a e ngaahi me‘angāue kuo maumau‘í ko ha poini kamata‘i ki he ngaahi ‘ohofí ‘a ia kuo fa‘u ke tuifio lelei pē mo e tulēfiki mo‘oní.

‘Ilo‘í mo e ngaahi fokotu‘u fakasi‘isi‘i uesiá

‘Oku fokotu‘u mālohi atu ‘e he ACSC ‘a e ASD ‘a hono ngāue ‘aki ‘o e Ngaahi Pule‘i Mahu‘inga ‘e Valu ‘a ia ‘oku fekau‘aki mo e Ngaahi Founga Ngāue ke Fakasi‘isi‘i ‘Aki ‘a e Ngaahi Me‘a ‘oku Hoko ‘o Kau ki he Malu‘i Faka‘ilekitulōniká. ‘Oku hā ‘i lalo ha ngaahi fokotu‘u ki he ngaahi ngāue malu‘i netiueka ‘a ia ‘oku totonu ke fakahoko ke ‘ilo‘i ‘aki mo ta‘ofi ‘a e ngaahi a‘u ta‘efakamafai‘i ‘a e APT40, hoko ki ai ‘a e ngaahi fakasi‘isi‘i uesia pau ki he ngaahi TTP tefito ‘e fā ‘a ia kuo fakamā‘opo‘opo ‘i he Tēpile 1.

‘Ilo‘i

Ko e ni‘ihi ‘o e ngahai faile ‘a ia kuo ‘ilo‘i ‘i ‘olungá na‘e tuku ia ‘i he ngaahi tu‘u‘anga ‘o hangē ko e C:\Users\Public* mo e C:\Windows\Temp*. ‘E lava ‘a e ngaahi tu‘u‘anga ko ‘ení ‘o hoko ko ha ngaahi feitu‘u faingamālie ki hono tohi ‘o e teitá koe‘uhi ‘oku nau angamaheni ke world writable, ‘a ia, ko e kotoa ‘o e ngaahi ‘akauni ‘a e taha ngāue ‘akí kuo lēsisita ‘i he Windows ‘oku nau a‘u ki he ngaahi tailekitulī ko ‘ení mo ‘enau ngaahi tailekitulī iikí. ‘I he taimi lahi, ‘e lava ‘e ha taha ngāue ‘aki pē ‘o a‘u ki he ngaahi faile ko ‘ení, ‘o faka‘atā ‘a e ngaahi faingamālie ki he nga‘unu ‘i he netiueka tatau, kalofi ‘o e malu‘í, ngāue ‘aki ‘i he fakangatangata ‘oku ma‘ulalo mo e fakanofonofo ki he to‘o ‘ikai fakamafai‘í.

‘Oku vakai ‘a e ngaahi tu‘utu‘uni Sigma ko ‘ení ki he fakahoko mei he ngaahi tu‘u‘anga ngalikehé ko e faka‘ilonga ‘o ha ‘ekitivitī ‘oku ‘ikai faitatau. ‘I he kotoa ‘o e ngaahi me‘á, ‘oku fie ma‘u ‘a e fakatotoló ke fakapapau‘i ‘aki ‘a e ‘ekitivitī kākaá mo hono fakahā.

Hingoá: World Writable Execution - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Fakamatala: ‘Ilo‘i hono fakahoko ‘o e founga ngāué mei he C:\Windows\Temp.

Puipuitu‘á:

‘Oku vakai ‘a e lao ko ‘ení tautautefito ki he fakahoko mei he: C:\Windows\Temp*. ‘Oku lahi ange hono ngāue ‘aki ‘a e Temp ‘e he ngaahi polokalama ‘ikai fakatu‘utāmakí pea ko ia ai ko ha me‘a faka‘ilonga ‘oku si‘i ange ‘ene fakapapau‘i ha ngāue kākā ‘i hono fakahoa ki hono ngāue ‘aki mei he ngaahi world writable tailekitulī iiki ‘i he C:\Windows.

‘Oku holoki lahi ‘e hono to‘o ‘o e ngaahi polokalama kuo ngāue ‘aki ‘e he kau ngāue ‘aki SISITEMI pe SĒVESI NETIUEKA ‘a e lahi ‘o e ‘ekitivitī ‘oku ‘ikai fakatu‘utamakí ‘a ia kuo fili ‘e he lao ko ‘ení.

‘Oku ‘uhinga ‘eni ‘e ala fakalaka ‘a e laó ‘i he ngaahi ngāue ‘aki kākaá ‘i ha tu‘unga fakangatangata ma‘ōlunga ange ka ‘oku fokotu‘u atu ke ngāue ‘aki ‘a e ngaahi lao kehé ke fakapapau‘i pe ‘oku feinga ha taha ngāue ‘aki ke ne fakalahi ‘a e ngaahi totonu ki he a‘ú ki he SISITEMÍ.

Fakatotolo:

1. Sivi‘i ‘a e fakamatala ‘oku felāve‘i fakahangatonu mo e ngāue ‘aki ‘o e faile ko ‘ení, ‘o hangē ko e koniteni ‘a e taha ngāue ‘akí, tu‘unga falala‘angá ‘o e fakahokó, ‘ekitivitī muimui‘i ‘i he taimi pē ko iá mo e ngaahi ‘īmisi kuo ‘apulouti ‘e he failé.
2. Fakatotolo‘i ‘a e founga ngāue puipuitu‘á, netiueká, failé mo e teita poupou kehe ‘i he housí ke tokoni ki hono fakahoko ha sivi‘i pe ‘oku kākā ‘a e ‘ekitivitií.
3. Kapau ‘e fie ma‘ú feinga ke tānaki ha tatau ‘o e failé ki he ‘ensinia fakafokí ke fakapapau‘i pe ‘oku mo‘oni.

Ngaahi Ma‘u‘anga Fakamatalá:

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

Fa‘u Tohí: ACSC ‘a e ASD

‘Aho: 2024/06/19

Tu‘unga: fakaangaanga

Ngaahi teekí:

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

Ma‘u‘anga Fakamatala Loká:

fakakalakalasí: process_creation
koloá: windows

‘Ilo‘í:

```
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:
    Taha Ngāue ‘Akí:
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

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

tu‘unga: temp and not (common_temp_path or system_user or dismhost or known_parent)

Ngaahi positivi loi:

- Kuo ‘ilo‘i ha ngaahi polokalama ‘aotita ‘i he lisi fakangofuá ‘oku nau ngāue ‘aki ‘a e ngaahi fekau mei he Temp.
- ‘E pau ke ‘i ai mo‘oni ‘i he Temp ha fokotu‘utu‘u ‘o e ngaahi polokalama kamatá mo kinautolu tenau kamata‘í, ko ia ai ‘e ‘aonga ke vakai‘i ‘a e mafola ‘a e ‘ulunganga ni ‘i ha netiueka ‘oku pule‘i (pea pe ‘e lava pe ‘ikai ‘o faka‘atā) kimu‘a pea fokotu‘utu‘u ‘a e lao ni.

Levolo: ma‘ulalo

Hingoá: World Writable Execution - Non-Temp System Subdirectory

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

Fakamatala: ‘Ilo‘i ‘a e fakahoko ‘o e founga ngaue mei ha world writabe location ‘i ha tailekitulī si‘i ‘o e tu‘u‘anga ‘inisitolo Windows OS .

Puipuitu‘á:

‘Oku vakai fakapatonu ‘a e lao ko ‘ení ki hono fakahoko ‘o e ngaahi tailekitulī out of world writeable ‘i loto ‘i he C:\ pea tautefito ki he C:\Windows*, ‘o ‘ikai kau ki ai ‘a e C:\Windows\Temp (‘a ia ‘oku ngāue ‘aki lahi ange ‘e he ngaahi polokalama ‘ikai fakatu‘utāmakípea ko ia ko ha me‘a faka‘ilonga ‘oku si‘i ange ‘ene fakapapau‘i ha ngāue kākā).

‘Oku ‘ikai fakakau ‘a e ngaahi folder AppData kapau ‘oku ngāue ‘aki ha faile ko e SYSTEM – ko ha founga ‘ikai fakatu‘utāmaki eni ‘a ia ‘oku fakahoko ‘aki ‘a e ngaahi faile polokalama fakataimí.

Hili hono fakakakato ‘a e peisilaini ki he fuofua netiueká mo hono ‘ilo‘i ‘o e ngaahi fakahoko ‘ikai fakatu‘utāmaki mei he ngaahi tu‘u‘anga ko ‘ení, ‘oku totonu ko e lao ko ‘ení ‘e tātaaitaha ke ngāue ‘aki.

Fakatotolo:

1. Sivi‘i ‘a e fakamatala ‘oku felāve‘i fakahangatonu mo e ngāue ‘aki ‘o e faile ko ‘ení, ‘o hangē ko e koniteni ‘a e taha ngāue ‘akí, tu‘unga falala‘angá ‘o e fakahokó, ‘ekitivitī muimui‘i ‘i he taimi pē ko iá mo e ngaahi ‘īmisi kuo ‘apulouti ‘e he failé.
2. Fakatotolo‘i ‘a e founga ngāue puipuitu‘á, netiueká, failé mo e teita poupou kehe ‘i he housí ke tokoni ki hono fakahoko ha sivi‘i pe ‘oku kākā ‘a e ‘ekitivitií.
3. Kapau ‘e fie ma‘ú feinga ke tānaki ha tatau ‘o e failé ki he ‘ensinia fakafokí ke fakapapau‘i pe ‘oku mo‘oni.

Ngaahi Ma‘u‘anga Fakamatalá:

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

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

Fa‘u Tohí: ACSC ‘a e ASD

‘Aho: 2024/06/19
Tu‘unga: fakaangaanga

Ngaahi teekí:

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

Ma‘u‘anga fakamatala loká:

fakakalakalasí: process_creation
koloá: windows

‘Ilo‘í:

writable_path:

‘Īmisí|‘oku ‘i ai ‘a e:

- ':\\$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:

'Īmisí|'oku 'i ai 'a e: '\\AppData\\'
Taha Ngāue 'Akí: 'SYSTEM'

tu'unga: writable_path and not appdata

Ngaahi positivi loi:

Kuo 'ilo'i ha ngaahi polokalama 'aotita 'i he lisi fakangofuá 'oku nau ngāue 'aki 'a e ngaahi fekau mei he ngaahi tailekitulī ko 'ení.

'Oku fakapotopoto ke tu'u 'a e ngaahi tohi mo e naunau faka'etimini kuo ngāue 'aki 'i he (ngaahi) 'ātakai pule'í 'i he taha 'o e ngaahi tailekitulī ko 'ení pea 'oku totonu ke ngāue tahataha atu ki ai.

Lēvolo: ma'ōlunga

Hingoá: World Writable Execution - Users

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

Fakamatala: 'Ilo'i 'a e ngāue 'aki 'o e founga ngāué mei he C:\Users\Public* mo e ngaahi world writable folders kehe 'i loto 'i he Users.

Puipuitu'á:

'Oku 'ikai fakakau 'a e ngaahi folder AppData kapau 'oku ngāue 'aki ha faile ko e SYSTEM – ko ha founga 'ikai fakatu'utāmaki eni 'a ia 'oku fakahoko 'aki 'a e ngaahi faile polokalama fakataimí.

Fakatotolo:

1. Sivi'i 'a e fakamatala 'oku felāve'i fakahangatonu mo e ngāue 'aki 'o e faile ko 'ení, 'o hangē ko e koniteni 'a e taha ngāue 'akí, tu'unga falala'angá 'o e fakahokó, 'ekitivitī muimui'i 'i he taimi pē ko iá mo e ngaahi 'īmisi kuo 'apulouti 'e he failé.
2. Fakatotolo'i 'a e founga ngāue puipuitu'á, netiueká, failé mo e teita poupou kehe 'i he housí ke tokoni ki hono fakahoko ha sivi'i pe 'oku kākā 'a e 'ekitivitií.
3. Kapau 'e fie ma'ú feinga ke tānaki ha tatau 'o e failé ki he 'ensinia fakafokí ke fakapapau'i pe 'oku mo'oni.

Ngaahi Ma'u'anga Fakamatalá:

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

Fa'u Tohí: ACSC 'a e ASD

'Aho: 2024/06/19

Tu'unga: fakaangaanga

Ngaahi teekí:

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

Ma'u'anga fakamatala loká:

fakakalakalasí: process_creation
koloá: windows

‘Ilo‘í:

ni‘ihi ngāue ‘akí:

‘Īmisí|‘oku ‘i ai ‘a e:

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

appdata:

‘Īmisí|‘oku ‘i ai ‘a e: '\\AppData\\'
Taha Ngāue ‘Akí: 'SYSTEM'

tu‘unga: ni‘ihi ngāue ‘akí kae ‘ikai ko e appdata

Ngaahi positivi loi:

– ‘Oku fakapotopoto ke tu‘u ‘a e ngaahi tohi mo e naunau faka‘etimini kuo ngāue ‘aki ‘i he (ngaahi) ‘ātakai pule‘í ‘i he Public pe ha tailekitulī pea ‘oku totonu ke ngāue tahataha atu ki ai.

Lēvolo: mitiume

Ngaah Fakasi‘isi‘i Uesiá

Logging

Lolotonga ‘a e ngaahi fakatotolo ‘a e ACSC ‘a e ASD, ko ha kaveinga angamaheni na‘a ne holoki ‘a e ‘aonga mo e vave ‘o e ngaahi feinga fakatotoló ko e si‘isi‘i ‘o ha fakamatala loka ‘oku kakato mo fakahisitōlia ‘i ha ngaahi ‘ēlia kau ai ‘a e ngaahi loka kole ‘a e seeva uepisaití, loka ‘o e ‘iveni Windows mo e ngaahi loka ‘o e polokisī ‘initanetí.

‘Oku fokotu‘u atu ‘e he ACSC ‘a e ASD ke toe vakai‘i mo ngāue ‘aki ‘enau fakahinohino ‘i he Windows Event Logging and Forwarding kau ai ‘a e Windows Event Logging Repository mo e Information Security Manual’s Guidelines for System Monitoring, ke fakakau ai ‘a e centralizing logs mo e retaining logs ki ha vaha‘a taimi fe‘unga.

Pule‘i ‘o e ngāue fakatahataha‘í

Fakatahataha‘i taimi totonu ‘a e kotoa ‘o e ngaahi me‘angāue mo e sēvesi kuo fakahaá, kau ai ‘a e ngaahi seeva uepisaití, polokalama ‘initanetí, mo e ngaahi gateway ki he a‘u mei he mama‘ó. Vakai‘i ke ngāue ‘aki ‘a e sistemi pule‘i ‘o e ngāue fakatahataha‘i fakalukufuá ke ‘otomētiki mo fakavave‘i ‘a e founga ngāué. ‘Oku fokotu‘u atu ‘e he ACSC ‘a e ASD ‘a hono ngāue ‘aki ‘o e ISM’s Guidelines for System Management, tautefito, ki he ngaahi malu‘i ‘o e Sistemi Ngāue Fakatahataha‘í kapau ‘oku ala ngāue ‘aki.

Ko e lahi taha ‘o e ngaahi ngāue ‘ohofi kuo ngāue ‘aki ‘e he taha ngāue koví na‘e ‘ilo lahia pea na‘e ‘i ai ‘a e ngaahi fakatahataha‘i pe fakasi‘isi‘i uesia na‘e ma‘u. ‘Oku totonu ke fakapapau‘i ‘oku ngāue ‘aki ‘a e ngaahi fakatahataha‘i malu‘í pe fakasi‘isi‘i uesiá ki he fa‘unga me‘angāue internet facing ‘i loto ‘i he houa ‘e 48, pea kapau ‘e lava, ke ngāue ‘aki ‘a e ngaahi tatau fakamuimuitaha ‘o e polokalamá mo e ngaahi operating systems.

Fakakongokonga ‘o e netiueká

‘E lava ‘e he fakakongokonga ‘o e netiueká ‘o ngaohi ke faingata‘a lahi ange ki he ngaahi fakafepakí ke ‘ilo‘i mo ma‘u ‘a e a‘u ki he teita pelepelengesi ‘a e kautahá. Ngaahi konga netiueka ke fakangatanagata pe poloka ‘aki ‘a e nga‘unu ‘i he netiueka tatau ‘aki hono ta‘ofi ‘o e tulēfiki ‘i he vaha‘a ‘o e ngaahi komipiutá tukukehe kapau ‘oku fie ma‘u ia. ‘Oku totonu ke toki lava pē ke pule‘i ‘a e ngaahi seeva mahu‘inga ‘o hangē ko e Active Directory mo e ngaahi seeva fakamo‘oni‘i kehé mei ha ngaahi seeva ‘i he vaha‘á ‘oku fakangatangata hono lahí pe ha ngaahi ‘seeva puná’. ‘Oku totonu ke muimui‘i ofi ‘a e ngaahi seeva ko ‘ení, ‘oku malu pea fakangatangata ko hai ‘a e ni‘ihi ngāue ‘aki mo e ngaahi me‘angāue ‘oku lava ke fakahoko kia kinautolú.

Neongo ‘a e ngaahi me‘a kuo hoko ‘a ia kuo ‘ilo‘i ai hono ta‘ofi ‘o e nga‘unu ‘i he netiueka tataú, ‘e lava ‘e he fakakongokonga makehe ‘o e netiueká toe fakalahi ‘a e fakangatangata ki he lahi ‘o e teita ‘oku lava ‘a e kakai ngāue koví ke a‘u ki ai mo to‘ó.

Ngaahi fakasi‘isi‘i uesia makehé

Na‘e fokotu‘u atu foki ‘e he ngaahi kautaha fa‘u tohí ‘a e ngaahi fakasi‘isi‘i uesia ko ‘ení ke tau‘i ‘aki ‘a e APT40 mo e ngāue ‘aki ‘e he ni‘ihi kehé ‘a e ngaahi TTP ‘i laló.

- Tamate‘i ‘a e ngaahi netiueka sēvesi ‘ikai ke ngāue ‘akí pe ‘oku ‘ikai ke fie ma‘ú, ngaahi pootí mo e laó.
- Ngāue ‘aki ‘a e ngaahi polokalama firewall ‘initaneti (WAFs) ke malu‘i ‘a e ngaahi seeva uepisaití mo e ngaahi polokalamá.
- Ngāue ‘aki ‘a e totonu si‘isi‘i tahá ke fakangatangata ‘aki ‘a e a‘u ki he ngaahi seevá, vahevahe faka‘ilekitulōnika ‘o e failé, mo e ngaahi naunau kehé.
- Ngāue ‘aki ‘a e fakamo‘oni‘i multi-factor (MFA) mo e ngaahi ‘akauni sēvesi ‘oku puleí ke fa‘u ke faingata‘a ange ke ‘ilo‘i mo toe ngāue ‘aki ‘a e ngaahi fakaikiiki faka‘ilonga‘í. ‘Oku totonu ke ngāue ‘aki ‘a e MFA ki he kotoa ‘o e ngaahi sēvesi ‘oku lava ‘o a‘u ki ai ‘i he ‘initanetí mei he mama‘ó, kau ki ai ‘a e:
  - ‘Īmeili ‘i he ‘initanetí mo ia ‘oku ‘i he cloud
  - Ngaahi peletifoomu fengāue‘aki
  - Ngaahi fehokotaki ‘i he netiueka tāutahá
  - Ngaahi sēvesi remote desktop
- Fakafetongi ‘a e me‘angāue kuo maté.

Table 1. Ngaahi Founga Fakasi'isi'i Uesia/Ngaahi Founga

TTP	Ngaahi Founga Fakasi'isi'i Uesia Mahu'inga 'e Valu	Ngaahi Pule'i ISM
Fuofua A'ú T1190 Ngāue 'ohofi 'o e Polokalama Public-Facing	Ngaahi polokalama fakatahataha'í Fakatahataha'i 'o e ngaahi operating system Founga Fakamo'oni'i Multi-Factor Pule'i 'o e polokalamá	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Ngāue 'aki T1059 Fekau mo e Fakatonulea Scripting	Pule'i 'o e Polokalamá Fakangatangata 'a e ngaahi Microsoft Office macro Fakangatangata 'o e ngaahi totonu a'u 'a e 'etiminí	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Matauhi 'o e A'ú T1505.003 Konga Fakapolokalama 'o e Seevá: Web Shell	Pule'i 'o e Polokalamá Fakangatangata 'o e ngaahi totonu a'u 'a e 'etiminí	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Fuofua A'ú / Fakalahi ki he Totonu ke A'ú / Matauhi 'o e A'ú T1078 Ngaahi 'Akauni Vēliti	Fakatahataha'i 'o e ngaahi operating system Founga Fakamo'oni'i Multi-Factor Fakangatangata 'o e ngaahi totonu a'u 'a e 'etiminí Pule'i 'o e polokalamá User application hardening	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

Ki ha fakatotolo fakalukufua makehe mo ha fale'i fakasi'isi'i uesia, kātaki 'o kumi tokoni ki he ngaahi vahe ki he Fakasi'isi'i Uesiá mo e Fakatotoló 'i he peesi uepisaiti ki he foungá 'a e MITRE ATT&CK ki he ngaahi founga takitaha kuo 'ilo'i 'i he fakamā'opo'opo 'a e MITRE ATT&CK 'i he ngata'anga 'o e fale'i ko 'ení.

Fakamatala Faka'ata'atā

Ko e fakamatala 'i he lipooti ni 'oku 'oatu ia "'o hangē pē koiá" 'i he 'uhinga fakahinohino pē. 'Oku 'ikai fakangofua 'e he ngaahi kautaha fa'u tohí ha kautaha fakakomēsiale, ha koloa, kautaha, pe sēvesi, kau ai ha ngaahi kautaha, koloa, pe sēvesi 'oku fakafehokotaki ki ai 'i loto 'i he tohi ngāue ko 'ení. Ko ha lave ki ha ngaahi kautaha komēsiale pau, ngaahi koloa, founga ngāue, pe ha ngaahi sēvesi 'e he maaka sēvesí, faka'ilonga fefakatau'akí, taha fo'u koloa pe ha taha kehe mei ai, 'oku 'ikai ke kau pe 'e fakahā mahino ai ha fakangofua, fakaongoongolelei, pē ha sai'ia 'a e ngaahi kautaha fa'u tohí.

'Oku faka'ilonga'i 'a e tohi ngāue ko 'ení ko e TLP:CLEAR. 'Oku 'ikai fakangatangata 'a e fakahaá. 'E ala ngāue 'aki 'e he ngaahi ma'u'anga talá 'a e TLP:CLEAR 'i hono 'ave holo 'e he fakamatalá 'a e faingamālie 'oku si'isi'i pe 'ikai ke ngāue hala 'aki, 'o fakatatau mo e ngaahi lao 'e ala ngāue 'akí mo e ngaahi founga ngāue ki hono fakahā, fakapule'angá. Fakatatau ki he ngaahi lao tu'upau 'o e totonu ki he hiki tataú, 'e ala tufaki 'a e fakamatala TLP:CLEAR 'o 'ikai fakangatangata. Ki ha fakamatala lahi ange 'o kau ki he Traffic Light Protocol, vakai ki he cisa.gov/tlp

MITRE ATT&CK – Founga ngāue fakapulipuli fakahisitōlia APT40 ‘oku mahu‘inga

Vakai‘i (TA0043)	
Hua ‘a e Ngaahi Uepisaiti ‘oku ‘O‘ona ‘e he Mamahí (T1594)	Tānaki ‘o e Fakamatala Faka‘ilonga‘i ‘o e Taha Mamahí: Ngaahi Fakamatala Faka‘ilonga‘í (T1589.001)
Active Scanning: Vulnerability Scanning (T1595.002)	Tānaki ‘o e Fakamatala ‘o e Housi Mamahí (T1592)
Kumi ‘o e Ngaahi Uepisaiti ‘oku ‘Atā/Ngaahi Tōmeini: Search Engines (T1593.002)	Tānaki ‘a e Fakamatala Netiueka ‘a e Mamahí: Domain Properties (T1590.001)
Tānaki ‘o e Fakamatala Faka‘ilonga‘i ‘o e Taha Mamahí: Ngaahi Tu‘asila ‘Īmeilí (T1589.002)	

Resource Development (TA0042)	
Ma‘u Mai ‘o e Fa‘unga Me‘angāué: Ngaahi Tōmeiní (T1583.001)	Ma‘u Mai ‘o e Fa‘unga Me‘angāué (T1583)
Ma‘u Mai ‘o e Fa‘unga Me‘angāué: DNS Server (T1583.002)	Maumau‘i ‘o e Ngaahi ‘Akauní (T1586)
Fakalahi ‘o e Ngaahi Ivi Ngāué: Code Signing Certificates (T1587.002)	Maumau‘i ‘o e Fa‘unga Me‘angāue (T1584)
Fakalahi ‘o e Ngaahi Ivi Ngāué: Ngaahi Tohi Fakamo‘oni Faka‘ilekitulōnika (T1587.003)	Fakalahi ‘o e Ngaahi Ivi Ngāué: Melouea (T1587.001)
Ma‘u ‘o e Ngaahi Ivi Ngāué: Code Signing Certificates (T1588.003)	Fokotu‘u ‘a e Ngaahi ‘Akauni: Ngaahi ‘Akauni Cloud (T1585.003)
Maumau‘i ‘o e Fa‘unga Me‘angāue: Ngaahi Me‘angāue Netiueka (T1584.008)	Ma‘u ‘o e Ngaahi Ivi Ngāué: Ngaahi Tohi Fakamo‘oni Faka‘ilekitulōnika (T1588.004)

Fuofua A‘ú (TA0001)	
Ngaahi ‘Akauni Vēlití (T1078)	Phishing (T1566)
Ngaahi ‘Akauni Vēliti: Default Accounts (T1078.001)	Phishing: Spearphishing Attachment (T1566.001)
Ngaahi ‘Akauni Vēliti: Ngaahi ‘Akauni Tōmeiní (T1078.002)	Phishing: Spearphishing Link (T1566.002)
Ngaahi Sēvesi meí he Mama‘ó ‘i Tu‘á (T1133)	Ngāue ‘Ohofi ‘o e Polokalama Public-Facing (T1190)
Drive-by Compromise (T1189)	

Ngāue ‘aki (TA0002)	
Windows Management Instrumentation (T1047)	Fekau mo e Fakatonulea Scripting: Python (T1059.006)
Ngāue Kuo Faka‘aho/Ngāue: At (T1053.002)	Fekau mo e Fakatonulea Scripting: JavaScript (T1059.007)
Ngāue Kuo Faka‘aho/Ngāue: Ngāue Kuo Faka‘aho (T1053.005)	Native API (T1106)
Fekau mo e Fakatonulea Scripting (T1059)	Inter-Process Communication (T1559)
Fekau mo e Fakatonulea Scripting: Windows Command Shell (T1059.003)	Ngaahi Sēvesi Sisitemi: Service Execution (T1569.002)
Fekau mo e Fakatonulea Scripting: PowerShell (T1059.001)	Exploitation for Client Execution (T1203)
Fekau mo e Fakatonulea Scripting: Visual Basic (T1059.005)	Fakahoko ‘e he Taha Ngāue ‘Akí: Faile Kākā (T1204.002)
Fekau mo e Fakatonulea Scripting: Unix Shell (T1059.004)	Fekau mo e Fakatonulea Scripting: Apple Script (T1059.002)
Ngāue Kuo Faka‘aho/Ngāue: Cron (T1053.003)	Ngaahi Naunau Fokotu‘utu‘u Polokalama (T1072)

Matauhi ‘o e A‘ú (TA0003)	
Ngaahi ‘Akauni Vēlitί (T1078)	Konga Fakapolokalama ‘o e Seevá: Web Shell (T1505.003)
Office Application Startup: Office Template Macros (T1137.001)	Create or Modify System Process: Windows Service (T1543.003)
Ngāue Kuo Faka‘aho/Ngāue: At (T1053.002)	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Ngāue Kuo Faka‘aho/Ngāue: Ngāue Kuo Faka‘aho (T1053.005)	Boot or Logon Autostart Execution: Shortcut Modification (T1547.009)
Ngaahi Sēvesi meí he Mama‘ó ‘i Tu‘á (T1133)	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
Ngāue Kuo Faka‘aho/Ngāue: Cron (T1053.003)	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Liliu ‘o e ‘Akauní (T1098)	Ngaahi ‘Akauni Vēliti: Ngaahi ‘Akauni Cloud (T1078.004)
Ngaahi ‘Akauni Vēliti: Ngaahi ‘Akauni Tōmeiní (T1078.002)	

Fakalahi ki he Totonu ke A‘ú (TA0004)	
Ngāue Kuo Faka‘aho/Ngāue: At (T1053.002)	Create or Modify System Process: Windows Service (T1543.003)
Ngāue Kuo Faka‘aho/Ngāue: Ngāue Kuo Faka‘aho (T1053.005)	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Process Injection: Thread Execution Hijacking (T1055.003)	Boot or Logon Autostart Execution: Shortcut Modification (T1547.009)
Process Injection: Process Hollowing (T1055.012)	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)

Fakalahi ki he Totonu ke A‘ú (TA0004)	
Ngaahi ‘Akauni Vēliti: Ngaahi ‘Akauni Tōmeiní (T1078.002)	Ngāue ‘Ohofi ‘o e Fakalahi ki he Totonu ke A‘ú (T1068)
Access Token Manipulation: Token Impersonation/Theft (T1134.001)	Ngāue ‘Ohofi Fakatupu mei ha ‘Iveni: Liliu ‘o e Fokotu‘utu‘u ‘o e Unix Shell (T1546.004)
Process Injection: Dynamic-link Library Injection (T1055.001)	Ngaahi ‘Akauni Vēliti: Ngaahi ‘Akauni Tōmeiní (T1078.002)
Ngaahi ‘Akauni Vēliti: Ngaahi ‘Akauni Lōkolo (T1078.003)	

Kalofi ‘o e Malu‘í (TA0005)	
Rootkit (T1014)	Indirect Command Execution (T1202)
Ngaahi Faile pe Fakamatala kuo Fufū: (T1027)	System Binary Proxy Execution: Mshta (T1218.005)
Ngaahi Faile pe Fakamatala kuo Fufū: Software Packing (T1027.002)	System Binary Proxy Execution: Regsvr32 (T1218.010)
Ngaahi Faile pe Fakamatala kuo Fufū: Steganography (T1027.003)	Subvert Trust Controls: Code Signing (T1553.002)
Ngaahi Faile pe Fakamatala kuo Fufū: Fakatahataha‘i Hili ‘a e Tilivá (T1027.004)	File and Directory Permissions Modifications: Linux and Mac File and Directory Permissions Modification (T1222.002)
Fakapuli: Fakatauhoa ‘o e Hingoa Fakalao pe Feitu‘u (T1036.005)	Virtualisation/Sandbox Evasion: Ngaahi Sivi ‘o e Sisitemí (T1497.001)
Process Injection: Thread Execution Hijacking (T1055.003)	Fakapuli (T1036)
Reflective Code Loading (T1620)	Maumau‘i ‘a e Ngaahi Malu‘í: Tamate‘i pe Liliu ‘a e Sisitemi Firewall (T1562.004)
Process Injection: Process Hollowing (T1055.012)	Fufū ‘o e Ngaahi Ngāue ‘Aatí: Hidden Files and Directories (T1564.001)
To‘o ‘o e Me‘a Fakatokangá: Tamate‘i Failé (T1070.004)	Fufū ‘o e Ngaahi Ngāue ‘Aatí: Window Fakapulipuli (T1564.003)
To‘o ‘o e Me‘a Fakatokangá: Timestomp (T1070.006)	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
To‘o ‘o e Me‘a Fakatokangá: Clear Windows Event Logs (T1070.001)	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Liliu ‘a e Lēsisitá (T1112)	Sēvesi ‘i he Uepí (T1102)
Ngaahi Faile pe Fakamatala kuo To‘o hono Fufuú/To‘o hono Fika Fakapulipulí (T1140)	Fakapuli: Ngāue pe Sēvesi Fakapuli (T1036.004)
Maumau‘i ‘a e Ngaahi Malu‘í (T1562)	

A‘u ki he Ngaahi Fakamatala Faka‘ilonga‘í (TA0006)	
OS Credential Dumping: LSASS Memory (T1003.001)	Ngaahi Fakamatala Faka‘ilonga‘i ‘Oku ‘Ikai Malu‘i: Ngaahi Fakamatala Faka‘ilonga‘i ‘i he Ngaahi Failé (T1552.001)
OS Credential Dumping: NTDS (T1003.003)	Fakamālohi: Mate‘i ‘o e Password (T1110.001)
Fakanamunamu ‘o e Netiueká (T1040)	Fakamo‘oni‘i Fakamālohi (T1187)

A‘u ki he Ngaahi Fakamatala Faka‘ilonga‘í (TA0006)	
Ngaahi Fakamatala Faka‘ilonga‘i meí he Ngaahi Tauhi‘anga Password: Keychain (T1555.001)	Kaiha‘asi pe Tohinima Kākā ‘a e Ngaahi Tikite Kerberos: Kerberoasting (T1558.003)
Input Capture: Keylogging (T1056.001)	Fakamoveuveu ki he Fakamo‘oni‘i Multi-Factor (T1111)
Kuki Kaiha‘asi ‘o e Sēsini ‘Initanetí (T1539)	Faka‘ilonga Kaiha‘asi ‘o e A‘u ki he Polokalmá(T1528)
Ngāue ‘Ohofi ke A‘u ki he Fakaikiiki Faka‘ilonga‘í (T1212)	Fakamālohi: ‘Ilo‘i ‘o e Password (T1110.002)
Input Capture: Web Portal Capture (T1056.003)	OS Credential Dumping: DCSync (T1003.006)
Ngaahi Fakamatala Faka‘ilonga‘i meí he Ngaahi Tauhi‘anga Password (T1555)	Ngaahi Fakamatala Faka‘ilonga‘i meí he Ngaahi Tauhi‘anga Password: Ngaahi Fakamatala Faka‘ilonga‘i meí he Ngaahi Polokalama ‘Initanetí (T1555.003)

Fekumi (TA0007)	
Fekumi ki he Sēvesi Sisitemí (T1007)	‘Ilo ‘o e Fakamatala Sisitemí (T1082)
Fekumi ki he Application Window (T1010)	Fekumi ki he ‘Akaunί: ‘Akauni Lōkolo (T1087.001)
Lēsisita ki he Faka‘eke‘eké (T1012)	Fekumi ki he Fakamatala Sisitemí, Technique T1082 - Enterprise | MITRE ATT&CK®
Fekumi ki he Failé mo e Tailekitulií (T1083)	Fekumi ki he Taimi ‘o e Sisitemí (T1124)
Fekumi ki he Sēvesi Netiueká (T1046)	Fekumi ki he Taha ‘O‘ona/Ngāue ‘Aki ‘o e Sisitemí (T1033)
Fekumi ki he Remote System (T1018)	Fekumi ki he Domain Trust (T1482)
Fekumi ki he ‘Akaunί: ‘Akauni ‘Īmeili (T1087.003)	Fekumi ki he ‘Akaunί: ‘Akauni Tōmeini (T1087.002)
Fekumi ki he Ngaahi Fehokotaki Netiueka Sisitemí (T1049)	Virtualisation/Sandbox Evasion: Ngaahi Sivi ‘o e Sisitemí (T1497.001)
Fekumi ki he Process (T1057)	Fekumi ki he Polokalamá (T1518)
Fekumi ki he Permission Groups: Domain Groups (T1069.002)	Fekumi ki he Network Share, Founga T1135 - Enterprise | MITRE ATT&CK®
Fekumi ki he Fokotu‘utu‘u Netiueka Sisitemi: Fekumi ki he Fehokotaki ‘Initanetí (T1016.001)	

Nga‘unu ‘i he Netiueka Tatau (TA0008)	
Ngaahi Sēvesi meí he Mama‘ó: Remote Desktop Protocol (T1021.001)	Ngaahi Sēvesi meí he Mama‘ó (T1021)
Ngaahi Sēvesi meí he Mama‘ó: SMB/Windows Admin Shares (T1021.002)	Ngāue ‘Aki ha Naunau Fakamo‘oni‘i Kehekehe: Pass the Ticket (T1550.003)
Ngaahi Sēvesi meí he Mama‘ó: Windows Remote Management (T1021.006)	Fe‘ave‘aki Naunau Ngā‘unu ‘i he (T1570)

Tānaki (TA0009)	
Teita meí he Sisitemi Lōkoló (T1005)	‘Ākaivi ‘a e Fakamatala Kuo Tānakí: ‘Ākaivi fou ‘i he Laipelí (T1560.002)
Teita meí he Network Shared Drive (T1039)	Tānaki‘anga ‘Īmeili: Tānaki‘anga ‘Īmeili meí he Mama‘ó (T1114.002)

Tānaki (TA0009)	
Input Capture: Keylogging (T1056.001)	Clipboard Data (T1115)
Tānaki ‘Otomētiki (T1119)	Teita meí he Ngaahi Tauhi‘anga Fakamatalá (T1213)
Input Capture: Web Portal Capture (T1056.003)	Data Staged: Remote Data Staging (T1074.002)
Data Staged: Local Data Staging (T1074.001)	‘Ākaivi ‘a e Fakamatala Kuo Tānakí (T1560)
Tānaki‘anga ‘Īmeili (T1114)	

To‘o ‘Ikai Fakamafai‘i (TA0010)	
To‘o ‘Ikai Fakamafai‘i ‘i he C2 Channel (T1041)	To‘o ‘Ikai Fakamafai‘i ‘i he Alternative Protocol: To‘o ‘Ikai Fakamafai‘i ‘i he Asymmetric Encrypted Non-C2 Protocol (T1048.002)
To‘o ‘Ikai Fakamafai‘i ‘i he Alternative Protocol (T1048)	To‘o ‘Ikai Fakamafai‘i ‘i he Sēvesi ‘i he Uepí: To‘o ‘Ikai Fakamafai‘i ki he Cloud Storage (T1567.002)

Fekau mo e Pule‘í (TA0011)	
Teita kuo Fufū: Protocol Impersonation (T1001.003)	Sēvesi ‘i he Uepí: Dead Drop Resolver (T1102.001)
Pooti ‘Oku Lahi Taha Hono Ngāue ‘Akí (T1043)	Sēvesi ‘i he Uepí: Fetu‘utaki Fa‘ahi Taha (T1102.003)
Lao ‘i he Leia ‘Olunga ‘o e Polokalamá: Ngaahi Lao ‘i he Uepí (T1071.001)	Ingress Tool Transfer (T1105)
Lao ‘i he Leia ‘Olunga ‘o e Polokalamá: Ngaahi Lao ki he Feave‘aki Failé (T1071.002)	Polokisī: Polokisī ‘i Loto (T1090.001)
Polokisī: Polokisī ‘i Tu‘a (T1090.002)	Pooti Non-Standard (T1571)
Polokisī: Polokisī Multi-hop (T1090.003)	Protocol Tunnelling (T1572)
Sēvesi ‘i he Uepí: Fetu‘utaki Halanga Ua (T1102.002)	Encrypted Channel (T1573)
Encrypted Channel: Asymmetric Cryptography (T1573.002)	Ingress Tool Transfer (T1105)
Polokisī, Founga T1090 - Enterprise | MITRE ATT&CK®	

Impact (TA0040)	
Service Stop (T1489)	Disk Wipe (T1561)
Tamate‘i ‘a e Sisitemí/Reboot (T1529)	Resource Hijacking (T1496)

Ngaahi Nouti

Fakamatala Faka‘ata‘atā

Ko e ngaahi fakamatala ‘i he tohi fakahinohino ko ‘ení ‘oku natula fakalukufua pea ‘oku ‘ikai totonu ke lau koha fale’i fakalao ia pe fakafalala ki ai ka ‘i ai ha fa’ahinga me’a pe ha me‘a fakafokifā ‘e hoko. ‘I ha me‘a mahu‘inga, ‘oku tonu ke ke fekumi ki ha fale’i fakapolofesinale totonu mo tau‘ātaina ‘o felāve‘i mo e ngaahi tu‘unga ‘oku ke ‘i aí.

‘E ‘ikai ke tali ‘e he Kominiuelí ha fatongia pe ha mo‘uá koe‘uhi ko ha maumau, mole pe fakamole ‘e hoko koe‘uhi ko ha fakafalala ‘i he fakamatala ‘oku ‘oatu ‘i he tohi fakahinohino koeni.

Totonu ki he Hiki Tataú

Ngāue ‘aki ‘o e Silá

‘Oku fakaikiiki ‘a e ngaahi tu‘unga ‘a ia ‘e lava ‘o ngāue ‘aki ai ‘a e Silá ‘i he Potungāue ‘a e Palēmiá mo e uepisaiti Kapinetí Fakamatala mo e Ngaahi Fakahinohino ‘a e Sila ‘o e Kominiuelí | pmc.gov.au.

Ki ha fakamatala lahi ange, pē ke lipōti ha me‘a kau ki he malu faka‘ilekitulōniká, fetu‘utaki mai kia kimautolu:

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

‘Oku lava ke ngaue‘aki ‘a e fika ko‘eni pē ‘i ‘Aositelēlia.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre