APT40 Kamatata

PRC MSS kamwakuran te tarena

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**

Barongan Kanoana

Tarakina:

Arona ngkekei

Te kamatata aei, e karioaki iroun te Botaki ni Kamano Iaon Intanete mai Aotiteria (ASD ACSC) te Botaki ni Kamano Iaon Intanete mai America (CISA), Botaki ibukin Kamanoan te Aba mai America (NSA), Ana Botaki ni Kakae Rongorongo Tautaeka n Amerika (FBI), ana Botaki ni Kamano Iaon Intanete United Kingdom (NCSC-UK), Botaki ni Kamano Iaon Intanete mai Canada (CCCS), Botaki ni Kamano Iaon Intanete mai Aotearoa (NCSC-NZ), Ana Botaki n tibwai Tiaman (BND) ao Ana Aobiti Tiaman ibukin Kamanoan te Tua (BfV), Ana Botaki n tibwai Korea (NIS) ao ana Botaki ni Kamano Iaon Intanete NIS, ao Ana Botaki Tiaban ibukin te Tatauraoi mani Kanganga ao Anga ni Kamano nte Intanete (NISC) ao Botaki ni Bureitiman iaon Tiaban (NPA) – imwin aio ao tina arania bwa "taan anga kariaia" – aika ena kaoti ana kurubu ni intanete te tautaeka n China ae (PRC) ake a mwanenaki man-tautaeka ao aron aia kakamaku nakon tititem iaon Aotiteria. Te kamatata aei e anaki man otaia taan anga kariaia ake a tibwai otaia n taian kakamaku ao man mwin ana kakae ASD ACSC man aia ukeuke iaon kanganga ake a ribotinaki.

Te kurubu n aonrain ae-mwanenna PRC ea tia ngkoa n taketenia boboti n aba aika kakaokoro, ni ikotaki ma Aotiteria ao Amerika, ao taian anga aika i nano aki toki ni kabonganaki irouia aekita ake-mwanenia PRC. Ngaia are, taan anga kariaia a kakoaua bwa te kurubu anne, ma aia anga ni mwakuri e tiku bwa te kakamaku nakon ana tititem abaia.

Man mwin aia ukeuke taan anga kariaia ao a kaotia ae te kurubu aio e kakaraoi mwakuri ni kaikoaki aonrain ibukin te PRC Botaki ibukin Kamanoan te Aba (MSS). Aia mwakuri ma aron mwakuriana e kuri titabo ma kurubu aika taraki bwa Kakamaku aika Nakoraoi man Okioki (APT) 40 (ataki n araia aika Kryptonite Panda, GINGHAM TYPHOON, Leviathan ao Bronze Mohawk n aia riboti taan mwakuri). Te kurubu aei ea tia n ribotinaki mai mwaina ae a memena i Haikou, Hainan Province, PRC ao mani kakanoaki man te PRC MSS, Kamanoan Aba mai Hainan.[2] Taian Kamatata aikai a katauraoi katoto tabeua n aron ana mwakuri te tia ribuaka aio nakoia uoman konana aika taian tititem. Katoto tabeua aikai iai bonganana nakoia taan karaoi aron kamano aonrain ibukin kakaean, totokoan ao manga karaoan mwin rinnakon APT40 n aia tititem. Katoto tabeua ake a rineaki a tia ni karaooaki mwin mwakuri buakakia ao aio e karaooaki ibukin kauarerekean riki manga-aonikai mairouia taan kakamaku, ke tabeman riki. Ibukin aio ao, katoto tabeua aikai a tiki ni maan teutana, ngkai a anganaki moa aia tai boboti ni karaoi mwin mwakuri buaka aikai.

Te Kauarereke

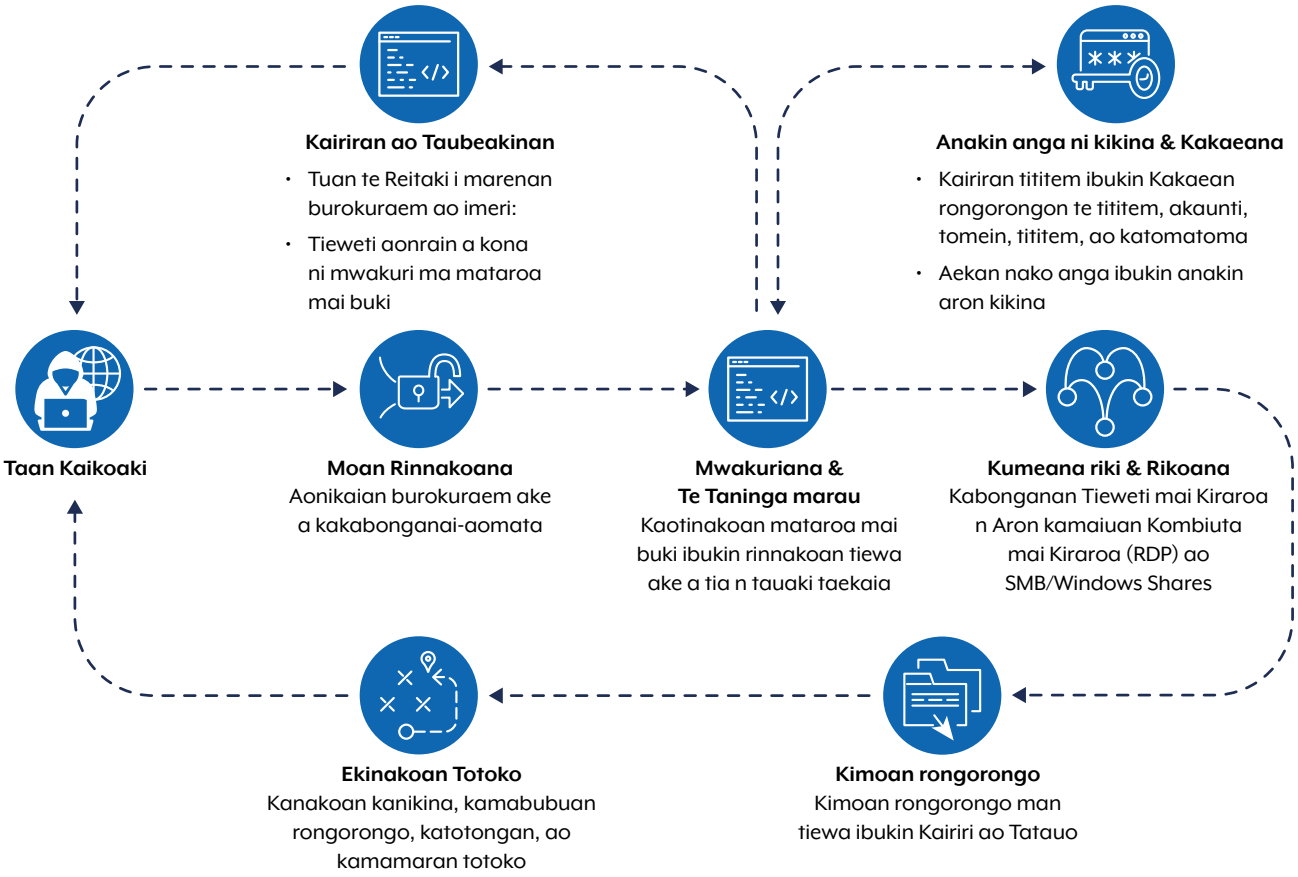
APT40 e aki toki n taketeni tititem mai Aotiteria ao ai te arona naba ma te tautaeka ao aia tititem boboti ake a onoti n ara aono, ao aia mwakuri ni kakamaku ae bon reitinako naba. Tarena ni ioawa aika kabwarabwaraki nte kamatata aio aki toki n noraki n ana tititem Aotiteria.

E noraki bwa, APT40 iai ana konabwai ni waekoa ni bita ao n tobwai taian mwakuri n aonikai-aika-boou (POCs) man memere aika boou ao ni waekoa ni kabongana ana konabwai anne ni karaoi tititem ake iai irouia te memere anne. APT40 e aki toki ni karaoi taukiroan tititem ake a nano iai, ni ikotaki ma tititem n aba ake taan anganga kariaia, ni kakaei angaia n tokobetoa aia takete. Aroia n taukiro n tainako aei a angan te kurubu aei te kona ni ukori memere, tain-tokin-mwakurin ke bwai n reitaki ake aikoa kabonganaki iaon tititem ake a nano iai, ao te kona ni moantaai ni karaoi aonikai. APT40 e reitinako ana kona n aonikai memeren te titimen man 2017.

APT40 e rang baiti n aonikai memere aika boou n taian burokuraem aika rangi ni kabonganaki n aron Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) ao Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473). ASD ACSC ao taan anga kariaia a kantaninga te kurubu anne bwa ena teimatoa ni kabonganai POC ibukin aonikaian memere ake a raka-aroia tebongina imwin kinakia irouia te koraki.

2 U.S. Botaki ibukin Kakaean te eti. 2021. Aman Kain Tiaina aika Mwakuri ma te Botaki ibukin Kamanoan te Aba a Kateaki ni Bukinaia ae a Kambein nte Aonnaba ibukin Rinnakoan Kombiuta ao a Taketeni Rabakau aika Bwainaki, ao Rongorongon Bitiniti aika Tabu, ni Ikotaki ma Kamatebwaian Man Aorakin Kombiuta.

Nambwa 1: TTP tamein tein ana mwakuri APT40



Te kurubu aio e tatangiria n aonikai memere, are kaitaraia-aomata nakon kabonganan kawai ake ana rekereke ma aomata, n aron katairake nte imeri, ao e moanibwaia karekean aron kikina ibukin manga karaoan-riki ana mwakuri aika bati imwiina. APT40 e aki toki ni kakabonganai uebutiaiti aikai (T1505.003) ibukin aia mwakuri aika okioki, moarara riki ngke a moan rinnakoi tititem. Ni bon arona, ao imwin moan reken rinnakon APT40 ao e moanibwaia karekean te kakaonimaki e aonga n rereke rinnakoan riki ana tititem konaia. Ma, ngkai a taninga marau ngke a moan rinnako, e tara n ae ana bon noraki naba n tabo ake a rinnakoi – a ngae ngke ai manra ngaiia n rinako ke tera aia mwakuri ake a wakin.

Tarena aika nonoraki

E ngae ngke APT40 ea tia ni kabonganai ana uebutiaiti Aotiteria ake e tia n rinnakoi ibukin kairiran ao taubeakinan (C2) tiewa ibukin ana mwakuri, te kurubu aei e bibiti naba tein mwakuriana. (T1594).

APT40 ea tia ni kabonganai aron aonikaian bwai n reitaki ae manga rangi ni bwainaki ngkai, n aron bwai n reitaki n aobiti aika-uarereke/aobiti-nte mwenga (SOHO), bwa ana tiewa ni mwakuri ao ibukin-kibaran ana takete (T1584.008) iaon Aotiteria. Aio are ea kakorakoraia taan anga kariaia nakon taukiroan ao ririmwian ana kakamwakuri te kurubu aio.

Angiin bwai n reitaki aika SOHO a bon kaan tain-tokin-mwakuria ke a tuai bonotaki ngaia ae a kai rotaki N-bongin te aonikai. Imwin rinnakoaia ao, bwai n reitaki aika SOHO a reke bwa ai tabo ibukin karaoan ioawa ake a karinaki naba i buakoia taan kabongana te tieweti ao a katai aron ana totoko te tititem. (T1001.003).

Aron mwakuri aikai e kakabonganaki naba irouia aekita man te PRC ake a mwanenaki man-tautaeka, ao taan anga kariaia a noora aio bwa te kakamaku ae tabangaki. Ibukin riki rongorongona, noori kamatata aikai Aia Tautaeka Aomata i China ae-mwanenia aekita ibukin Karaoan Aonikai Aonrain nakon Tititem ao Bwai n reitaki ao PRC e-mwanenia Aekita ibukin Rinnakoan ao Reitinakoan rinnakoan ana Tiewa U.S. aika Kakawaki.

APT40 n taai tabetai e kaboi ao ni kakabonganai tiewa ibukin kaitaran-konaia C2 n tain ana mwakuri; ma te tarena aio e tara ni kekerikaki.

Mwakuriana ni Bwaina

ASD ACSC e tibwai ikai tabeua mai buakon mwauea aika kaikoaki ake a kuneaki n tain te kakae ae kaotaki i nano. Rongorongo aikai a kawaerakeaki nakon Virus Total ibukin karekean otangan tititem ae tabangaki riki ao ibukia kamironron ibukin karaoan kamano bwa ana kinai kakamaku aikai.

Katoto tabeua

ASD ACSC e tibwai ikai uoua riboti imwin aia kakae aika raba ibukin reiakinan aroia taan ioawa ni kamwakuri aia bwai ao aia tarena.

MD5	Aran nnen rongorongo	Rongorongona riki
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

Katoto Tabeua 1

Te riboti aei aki kinaki aomatana e aonga n rababa riki tibwauana. Botaki ake a rotaki tina arania ikai bwa 'te boboti'. Tabeua rongorongo ake a onoti a tia ni kanakoaki ibukin kamanoan aron kinakia ake a rotaki ao bon aron naba ana ririboti ASD ACSC iaon kanganga.

Kauarereke ibukia mataniwi

Te riboti aei e kawenei kukune man mwiin ana kakae ASD ACSC ngke ukeri aia tititem boboti ake a tia n rinnakoaki man Tuun nakon Tebetembwa 2022. Ribotin te kakae e katauraoaki nakoia boboti bwa ana anga kauarereke man tarakin mwakuri kaikoaki ao aia anga ni kaoki aroia. Mwiin kakae e kaotia ae mwakuri n aonikai e karaoaki iroun APT40.

Inanon nukan-Aokati, te ASD ACSC e kaongoia boboti ake a rotaki aia tititem man mwakuri n aonikai ae iai te bwai n reitaki ae a kabongana ni banen Aokati ao, man ana kariaia te boboti, ao te ASD ACSC ea kaotinakoi bwai ni kakauongo man aia-tiewa nakon tiewa ake a rotaki n ana tititem te boboti. Bwai ni kakauongo aikai e angania ana taan ukeri kanganga ASD ACSC te kona ni karaoi kakaean mwanekaia taan ioawa aonrain. Kabonganan rongorongo man bwai ni kakauongao aikai, ao ana taan ukeri kanganga ASD ACSC ea tia ni kaotinakoi mwiin aia kakamwakuri nte tai are a mwakuri iai ao bwai ake a riki.

Man Turai nakon Aokati, ao aikai aia mwakuri aekita ake a noraki iroun te ASD ACSC:

- warebwaian tiewa, are angania aekita te konabwai ni karaoa mwaben te tititem;
- kabonganan mataroa mai buki, e angania aekita matoan tikuia nte tititem ao te kona ni karaoi kairiran tititem; ao
- kaotinakoan aia bwai n aonikai ake tabeua ibukin aia mwakuri n aonikai.

Te kakae aio e kunei bwai ni kakoaua ibukin anakin ao rinnakoan rongorongo aika tabu ao bwai naba ni kakoaua ae aekita aikai a kumekume riki inanon te tititem (T1021.002). Angin reken te rinnako e reke man karaoan anga ni karinrin aika bati nakon aia tititem boboti, te tititem ae ti teuana aron kamanoana, ao kabonganan burokuraem aika aki mano ake a kona ni kawaerakeaki bwai mai iai. Ware ake a kimoaki bon aron kikina ake a kakannato riki are a ririn mai iai kain te boboti, ni irianaki ma rongorongon te tititem are a kona iai aekita ni manga karekei rinia ae aki ataki ngkana e buraokinaki aron rinia nte moan tai. Akea riki bwai n aonikai aika kuneaki irarikin ake a tia ni karaoi nakon mitin mai mwaina; ma, ririnakoan ana tititem te boboti irouia man akaunti aika kakannato riki e aki kainnanoa manga kabonganan riki bwai n aonikai. Kukune man kakae aikai a kaotia ae boboti a taketenaki n taian APT40, ao aki reke man aonikaian memere aika a bon ataaki irouia aomata.

Kukune imwin kakae

Inanon nukan-Aokati 2022, te ASD ACSC e kaongoia boboti ae iai te IP ae kakaraoi kaikoaki ae kakoauaki bwa e irekereke ma te kurubu aonrain ae mwanenaki man-tautaeka ae ea tia ni kuai kombiutan aia tititem boboti i marenan Turai ao Aokati. Te bwai n reitaki are rotaki titabo ma bwain bitiniti aika uarereke ke bwain te auti.

N rabanen Aokati, te ASD ACSC e kaotinakoa te tia ibuobuoki ae mena n-tiewa nako nanon aia tititem boboti ake a kakoauaki bwa a tia n rotaki ke n rinnakoaki.

Tabeua burokuraem ake a kona ni kabonganaki ni boutoka aron te kakae a aki tauraoi ibukin kabonganakia ngkai e kaokoro tein te rinnako ke barongan te tititem. E ngae n anne, ao tatauraoin te boboti ni katauraoi ware nakoia taan bwainaoraki man ASD ACSC e angania te konabwai ni karaoi ukeuke ao ni kataunari ana mwakuri APT40 iaon te tititem.

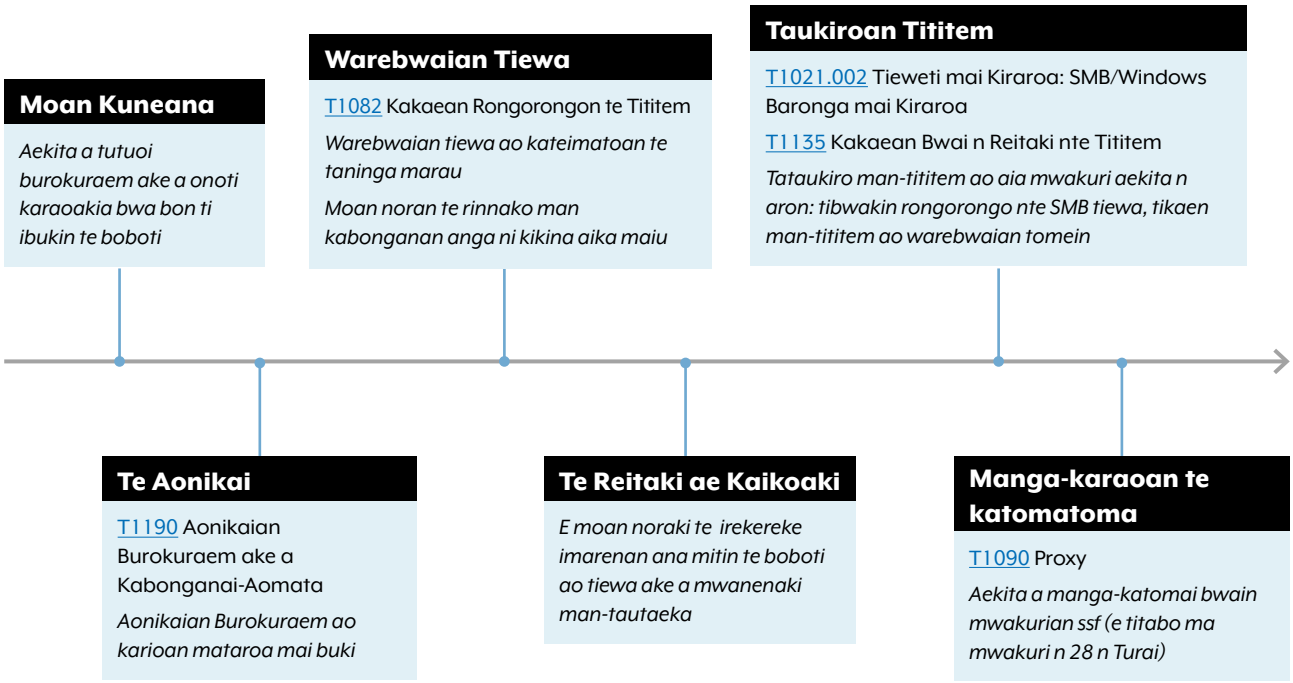
Inanon Tebetembwa, imwin maroro ma te ASD ACSC, ao boboti a bonnanoia bwa ana aki karekerekeia ma te IP are noraki nte moan kauring. Inanon Okitibwa, ao boboti a moana mwakurian kaokan aron aia tititem.

Kababanean rongorongona

Ni moa man July, ao aekita a kona n tuoi ao n aonikai burokuraem ake a karaoaki (T1190) ao ni maiu iaon `<webapp>2-ext`, aio e angania te kona ni karekea tein waeia i marenan te tititem ao taan kabongana (DMZ). Aio e katautauaki bwa ena kabonganai tititem ao tomein ake a kona n noraki. Anga ni kikina ake a tauaki taekaia (T1078.002) a kabonganaki ibukin rinnakoan Nnen Rongorongo aika Kakabonganaki (T1018) ao kaotinakoan ware man (T1039) mitin aika kakaokoro inanon te DMZ. Te aekita e karaoa te ioawa ae Kerberoasting aonga n reke aron anakin kikina man te tiewa (T1558.003). Ma te kurubu ni ioawa aika a tuai n nonoraki inanon te DMZ ke te tititem i nanoa.

Katameian taina

Tamei ae i nano e katauraoa aron taran aia mwakuri aika kaikoaki aekita ake a nonoraki inanon ana tititem te boboti.



Kabwarabwaran taina

Turai: Aekita a karaoi aron moan katomakia ma moani baan te uebutiaiti ae onoti karaoana (T1190) are karaoaki ibukin te boboti (imwin aio ao tina aranna bwa te 'web application' ke'*webapp*') man kamanoan (TLS) katomatoma (T1102). Akea riki mwakuri aika kakawaki ae a noraki.

Turai: Aekita a moana warebwaian ana uebutiaiti te burokuraem ibukin kakaean bwai n reitaki [2] ao ibukin kamatebwaiaia riki.

Turai: Aekita a kabanea aia kona n rinnakoa teuana te bwai n reitaki.

Turai: Aekita a kona ni `KATOKATOKA` nakon te tiewa, man mataroa mai buki ake a mena ni nnen tabeua uebutiaiti. Te ka uoua n IP, kanga e mwakuri naba ibukia aekita ake i eta, a moana aia katokatoka nakon te URL naba arei. Aekita a karaoi ao a manga tuoi mataroa mai buki aika tiraua.

Aia anga n aonikai e aki ataaki, ma e ataaki bwa bwai n reitaki ake a aonikaiaki a taketenaki bwa ana karaoi nnen rongorongo iaon `<webapp>2-ext`.

ASD ACSC e kakoaua ae IP akana uoua akanne a kai ni iraorao ni karaoi rinnako nte tai ae ti teuana ian ae titabo aia takete ao reken moan rinia aki man bwa ti tabeua te miniti te okoro.

Turai: Te kurubu aio ae bon waki naba ni warebwai tiewa, ibukin kakaean angana n aonikai akaunti nte tititem, ao ni kaotinakoa manin burokuraem ni kaikoaki aika kaokoro. Aekita a kona n rinnakoi burokuraem man kabonganan aron kikina ake a taui taekaia ibukin `<firstname.surname>@<organisation domain>`.

Aia mwakuri aekita aikai e tara n aki reke angana n Aonikaian Akaunti nte Tititem `<webapp>2-ext`. Man anne, ao aekita a manga bita aia mwakuri nako nanon te-tititem.

Turai: Aekita aikai a tuoi aron kinakin tieweti akaunti[3] ake a bae ni mena inanon bwainarii ake a matoa ma a kona ni kaukaki.

Turai: Aekita aikai a kamwakuri Taabo ni Katomatoma aika mano man akea booia, ao a kabonganai ibukin katoman aia tiewa ni kaikoaki. Te katomatoma aio are ea kabonganaki ibukin kairaia taan aonrain man aia mitin ni ioawa nako nanon ana tititem i nanoa te boboti, ngkanne aran mitin akanne a kona n noraki man aia taibi ngke a kabonganai aia tieweti akaunti ibukin rinnakoia.

Aokati: Aekita aikai a nonoraki ni karaoi aia mwakuri aika aki koro nanoia, n aron aki reken angan katomatoma man tieweti akaunti.

Aokati: Aekita aikai a kakaraoi naba warebwaian tititem ao Nnen Rongorongo aika Kakabonganaki. Imwin aki reken rinia ao a manga kabonganai riki anga ni kikina tabeua ao a karaoi rongorongona bwa ana kona n tibwaki[4] man Windows are mena nte DMZ, ao ngkanne a kona ni kaotinakoaki ware.

Aio e taraki bwa te anga teuana ni kabonganai aron kikina ake a kimoaki man mitin ake a kona n tibwaki kanoaia man te DMZ. Te o te ai e buraokinia aekita aikai man taketenakin tititem i nanoa man mwakuri aikai.

Aokati – **Tebetembwa:** Te bwai ni mwakuri ae SSF e manga-karaoi katomatoma nakon IP aika kaikoaki. Kurubu aikai aki noraki ni karaoi riki aia tokobeto imwin buraokinakia.

Tebetembwar: Te boboti e buraoki IP ake a kaikoaki man karinaia ibuakoia ake a totokoaki rinia nte o te ai.

2 N tarana, ao bwai n reitaki a maiu man te burokuraem

3 Akaunti n tieweti akea rekerekeia ma te tia kabongana, ma a rekereke ma te tieweti. Inanon ana tomein te kambwana ae Microsoft, ao e mwaiti aekakin akaunti.

4 Mounting shares bon aron karaon booma inanon ana tititem boboti bwa ana kona n roko iai taani kabongana te tititem.

Aia kawai aekita ao aron aia mwakuri

Aron mwakurin MITRE ATT&CK ea tia ni boretiaki ma aia kawai ao aron aia mwakuri ni kakamaku iaon te intanete. Aron mwakuri aikai e karioaki iroun te botaki n-aki-karaka mai US Te kambwana ae MITRE ao e kabonganaki nte aonnabai bwa kinakin aroaroia aekita ni kakamaku.

Te ASD ACSC e kunei aia kawai ao aron mwakuri aikai bwa a kakawaki nakon karaoan aia mwakuri aekita ni kakamaku aikai.

Taukiroo

T1594 – Kakaei aia Uebutiaiti-Konaia

Te aekita e warebwai burokuraem ibukin kakaean angan rinia nte tititem.

Moan Rinnakoana

T1190 – Aonikaian Burokuraem ake a Kabonganai-Aomata (rekereke ma aonikaian burokuraem aonrain aika karioaki)

T1078.002 – Akaunti aika Maiu: Akaunti man Tomein (rekereke ma te rinnako man aron kikina ake a tauaki taekaia)

Aonikaian burokuraem aika a onoti nte-intanete e kona n riki bwa aia tabo n rinnakoa te tititem aekita. Imwina ao te aekita ea kona ngkanne ni kabonganai aron kikina ake irouia ibukin kumean riki te tititem.

Mwakuriana

T1059 – Kairiri ao Anai nano ni Kamwamwane (rekereke ma mwakurian kairiri nakon burokuraem ni kaikoaki)

T1072 – Bwain Kaotinakoan Burokuraem (rekereke ma kabonganan bwai aika akea-booia Secure Socket Funnelling (SSF) ibukin katomatoma nakon te IP)

Taninga marau

T1505.003 – Burokuraem nte Tiewa: Mataroa mai buki (rekereke ma kabonganan mataroa mai buki ao SSF ibukin karekean te rinnako)

Anakin anga ni kikina

T1552.001 – Aron kikina man Titoan Taeka aika raba (rekereke ma rongorongon taeka aika raba ibukin karaoan barongan tititem (BMS))

T1558.003 – Kimoan ke Karaoan Kerberos Tiketi: Kerberoasting (rekereke ma ioawa ibukin karekean anga ni kikina nte tititem)

Kume riki

T1021.002 – Tieweti mai Kiraroa: Tibwakin SMB (rekereke ma karaoan booma aika kona n tibwaki SMB man bwai n reitaki aika tiraua)

Te Boota

T1213 – Ware man Nnen Rongorongo (rekereke ma manuo/boreti ake a kuneaki inanon taian BMS tiewa)

Kimoan rongorongo

T1041 – Kimoan rongorongo iaon te C2 Channel (rekereke ma ana mwakuri te aekita ni kaotinakoi ware man Nnen Rongorongo ao ni manga tibwatibwai)

Katoto tabeua 2

Nte riboti aei ao aki kinaki aomatana e aonga n rababa riki tibwauana. Botaki ake a rotaki tina arania ikai bwa 'te boboti'. Tabeua rongorongo ake a onoti a tia ni kanakoaki ibukin kamanoan aron kinakia ake a rotaki ao bon aron naba ana ririboti ASD ACSC iaon kanganga.

Kauarereke ibukia mataniwi

Te riboti aei e kawenei kukune man mwiin ana kakae ASD ACSC ngke ukeri aia tititem boboti ake a tia n rinnakoaki inanon Eberi 2022. Man te kakae aei ao a katauraoaki riboti aika uarereke nakon boboti ake a tia n rinnakoaki ao e tuangia naba aron kaokan arona. Mwiin kakae e kaotia ae mwakuri n aonikai e karaoaki iroun APT40.

Ni Meei 2022, te ASD ACSC e kaongoia boboti ae iai mwakuri ni kaikoaki aika kanamakinaki ae rota ana tititem te boboti man Eberi 2022. Imwin reken anne, ao boboti a manga kaongoa ASD ACSC ae a tia ni kunei burokuraem ni kaikoaki inanon aia tiewa ibukin te karinrin mai kiraroa. Te tiewa aio e kabonganaki ibukin te rinnako mai kiraroa ao mani katerei aron barongan bwai ni bobwai ao tina arana te tiewa aei bwa te 'te tiewa ae tauaki taekana' Te riboti aio e kawenei mwin kakae ao taeka ni bau ibukin kaokan aroia ao e karaoaki ibukia boboti imwin te kakae ae karaoia te ASD ACSC.

Bwai ni kakoaua a kaotia ae mwanangin ana tititem te boboti ea tia n tauaki taekana irouia taan kaikoaki aonrain ao a rin man te tabo are aririn iai te koraki mai kiraroa e moa aio man Eberi 2022. Te tiewa aio tao ea tia n tauaki taekana irouia aekita aika mwaiti, ao ea rotaki man te memere ae karekea kumeana mai kiraroa (RCE) are e rangi ni kakatanoataki n te tai are tauaki iai taekana.

Mwakuri ake a noraki iroun te ASD ACSC bon aikai:

- warebwaian tiewa, are angania aekita te konabwai ni karaoa mwaben te tititem;
- aonikaian burokuraem ake a kakabonganai-aomata ao kabonganan mataroa mai buki, e kona n angania aekita te konabwai ni katei waeia ao ni kairira te tititem;
- aonikaian memeren burokuraem ibukin rinnakoan akaunti; ao
- Rikoan anga ni kikina ibukin kumean nanon te tititem

Te ASD ACSC e kunea ae iai te tia kaikoaki ae ea tia ni kaotinakoi bubua ma bubua aara ma aia taeka ni karaba man te tiewa n reitaki ae tauaki taekana inanon Eberi 2022, ni ikotaki ma tabeua aron kikina aika-bati ao bwai ni mwakuria te rinnako mai kiraroa. Imwin tuoana iroun te boboti, ao taeka ni karaba ake a kabonganaki a maiu man aki kewekewe. Mwin ana tutuo ASD ACSC ao e kaotia bwa te aekita aei e bae n rikoi bwai ni mwakuri aikai ibukin mwakuri ni ioawa ke ibukin karaon ana taeka ni karaba aika aki kewekewe.

Kukune imwin kakae

Kauarerekean mwiin kakae

Te ASD ACSC e kunea bwa te aekita aei e taui taekan bwai n reitaki ake a kabongana taan mwakuri nte boboti ibukin rinnakoan aia tititem mai kiraroa. Bwai n reitaki aikai iai teniua tiewa aika-ibuobuoki are e reke iai bwain ni kakoauan ae ea tauaki taekana. Te boboti e kaini uoua mai buakon ake teniua tiewa aika-ibuobuoki teutana te tai imwin tauan taekaia. Mwin anne, ao mwakuri n aonikai ake imwina a riki n ti teuana te tiewa. Tiewa ake tabeua ake a rotaki naba man bwai n reitaki ake a tauaki taekaia a i-buobuoki naba n aron naba arei. Ibukin te kakoaua, ao nikabane bwai n reitaki ake a tauaki taekaia tina arania nte riboti aei bwa 'angkoa ti teuana'

Aekita aikai a kakoauaki bwa a kabonganai memere ake a bon ataki ibukin karinan mataroa mai buki nakon te bwai n reitaki are a taua taekana ni moa man Eberi 2022. Mwin tuoaia aekita ni kakamaku aikai ao e kaotaki bwa ea tia n reke aia anga n aonikaia te bwai n reitaki ae matoa. Te ASD ACSC e aki kona raoi ni kaotia bwa anga tabo are a kumeaki ian ae aki tauraoi aron tauan mwin taibi. Ma, bwai ni kakoaua man bwai n reitaki e kaotia ae aekita aikai a reke mwakurian aikai irouia:

- Rikoan bubua ma bubua aara ao taeka ni karaba aika maiu; ao
- Rikoan bwai ni mwakuri ake a kona iai aekita ni kaikoaki aikai n rinnakoa te virtual desktop infrastructure (VDI) bwa angkoa ngaia bon te tia kabongana ni koaua.

Te ASD ACSC e kunea naba ae te aekita aei e iangoa karaoan ae ena manga kabubura tauan mwin ana tititem te boboti. Te burokuraem are kaotinakoa te aekita aei e kona n anganna te kona ni karaoi ioawa ke ni kamaui kombiuta mai kiraroa kanga ngaia te tia mwakuri nte boboti. Te aekita e kona n tia ni kabonganai bwai n rinnako aikai ni kumei riki ana tieweti te boboti ao ni boutokai aia kouru ake tabeua.

Ana bwai ni mwakuri te boboti ake tabeua ake a mena nte tiewa ae barongaki akea noraia bwa a tauaki taekaia.

Rinnakoana

Te tiewa are e tauaki taekana ngaia a katauraoa aron te kikina ni Nnen Rongorongo aika Kakabonganaki ao te uebutiaiti, ibukia taan katomatoma nakon VDI (T1021.001).

Te Tabo	Aran Bwaini mwakuri aika tauaki taekaia (i-buobuoki)
Nnen rongorongo 1	TIEWA1, TIEWA2, TIEWA3

Te tiewa ni mwakuri iai inanona mataroa n rinnako ake a katauraoa kawaia taan kabongana te VDI, nte tai are e reke irouia token ibukin kinakia.

Akea kakoauan ae a tauaki taekan tiewa aikai. Ma, man tauan mwin taibi nte tiewa are iai mataroa n rinnako inanona ao e oti bwa iai irekerekena ma IP aetureti ni kaikoaki. E tara n ae aio e kaotia ae iai te mwakuri ae karaoaki iaon te tiewa, ke a tia n toma nakon te tiewa aio taan kakamaku aikai. Kinakin aron te mwakuri aio e aki kona n ataki man kabonganan kakoaua aika iroura ma e kaotia ae te kurubu aei e karaoa ninian kanoan ana tititem te boboti (TA0008).

Tiewa i nanoa

Te ASD ACSC e karaoa ana kakae man ware ake inanon mwakoron nako ana tititem te boboti. Mwakuri ni kaikoaki ake a kataki ao ake a reke mwakuria ao n ataki bwa a tia n taua taekan mwakoron ana tititem i nanoa te boboti ni ikotaki ma rinnakoan bwain mwakurian te-VDI, kumean taian SQL tiewa i nanoa (T1505.001), ao ai norakia taan aonrain ae kamino nano n rinnako man IP aetureti aika kaikoaki rinanon mataroan tiewa (TA0011).

Man kabonganan aron rinia inanon bwai ake a taui taekaia, te kurubu aei ea rikoi naba aara ao, taeka aika raba (T1003), ao ai token ibukin te MFA (T1111). Te kurubu aio e rikoi naba JSON Web Tokens (JWTs) (T1528), ae te bwai ni kikina ibukin te rinnako nte kombiuta mai kiraroa. Te aekita e bae ni kona ni kabonganai ibukin karaoan ke mwakuri buakan kombiuta mai kiraroa (T1563.002) ao rinnakoan ana tititem i nanoa te boboti bwa angkoa ngaia te tia mwakuri (T1078).

Te aekita e kabongana naba rinnakona n taui taekan bwai ni mwakuri ke ni kumea te SQL tiewa (T1505.001), are mena n ana tititem i nanoa te boboti. E tara n ae aekita a kona n rinnakoi rongorongo aikai.

Bwai ni kakoaua ake a tauraoi man te mataroa n rinnako nte tiewa e kaotia ae taan kabongana te tititem a kaoti rinanon ke nakon te bwai n reitaki man IP aetureti aika ataaki bwa a kaikoaki. N aron ae kabwarabwaraki i eta, ao aio e kona ni kaotia ae taan kaikoaki aonrain a rota ke a kabongana te bwai n reitaki aei, ibukin aia anga n rinnakoa te tititem i nanoa.

Tainakin te kakae

Te riti ae i nano e kataurao te tai are a karaoaki iai mwakuri ake a kuneaki n tain te kakae.

Te Tai	Te Botaki
Eberi 2022	IP aetureti aika ataaki bwa a irekereke ma mataroan rinnako n TIEWA7. Aron rekerekeia e aki kona n ataaki.
Eberi 2022	Nikabane tiewa, TIEWA1, TIEWA2, ao TIEWA3, a tauaki taekaia iroun te aekita ke taian aekita ni kaikoaki aonrain, ao mataroa mai buki a katukaki inanon tiewa. Nnen log e karaoaki ke bitaki iaon TIEWA2. Nnen rongorongo aikai iai kanoana aron kikina ake a reke irouia taan kaikoaki. Te /etc/kamano/taeka ni karaba ao /etc/nnen taeka aika raba a bitaki iaon TIEWA1 ao TIEWA3, are kaotia bwa a tia ni bitaki taeka ni karaba. Kakoaua ake iaon TIEWA1 e kaotia ae te taeka ni karaba ibukin te akaunti ae 'sshuser' ea ta ni bitaki.
Eberi 2022	TIEWA2 e kainaki iroun te boboti. Iai riki mataroa mai buki (T1505.003) ake a karaoaki iaon TIEWA1 ao TIEWA3. TIEWA1 e namakina SSH katakin ukeran manin aron kikina man TIEWA3. Ao e bitaki nnen log (T1070) iaon TIEWA3. Nnen rongorongo aei iai i nanona aron kinan akaunti (T1078) are kantaningaki bwa e a tia n reke irouia taan kaikoaki aikai. Taian JWT a tauaki (T1528) ao a kaotinakoaki nakon nnen rongorongo iaon TIEWA3. TIEWA3 e kamateaki iroun te boboti Mwakuri ni kabane imwin te tai aio a riki iaon TIEWA1.
Eberi 2022	Iai riki mataroa mai buki aika karaoaki inanon TIEWA1 (T1505.003). Taian JWT a tauaki ao a kaotinakoaki nakon nnen rongorongo iaon TIEWA1.
Eberi 2022	Iai riki mataroa mai buki ake a karaoaki inanon TIEWA1 (T1505.003), ao te IP aetureti ae ataaki bwa e kaikoaki e irekereke ma te tiewa (TA0011). Te IP aetureti ae ataaki bwa e kaikoaki e irekereke ma te mataroa n rinnako n tiewa TIEWA7.
Meei 2022	Te IP aetureti ae ataaki bwa e kaikoaki e irekereke ma te mataroa n rinnako n tiewa TIEWA7 (TA0011). Ao e karaoaki aron te kikina ibukin te katitamwa ae toma ma te IP aetureti ae kinaki man log ake a mena n TIEWA1. Iai riki mataroa mai buki aika karaoaki nte tiewa aio (T1505.003).
Meei 2022	Taekan burokuraem inanon TIEWA1 e bitaki iroun te aekita (T1543). Taekan te burokuraem aio iai inanona aron mwakurina ae kona iai ni kaotinakoi ware ma te SQL tiewa i nanoa.
Meei 2022	Iai riki nnen log iaon TIEWA1 aika tibwa bitaki (T1070). Nnen rongorongo iai inanona ara ao taeka aika raba ibukin ana tititem te boboti, are a kakoauaki bwa a mwakuri (T1078).
Meei 2022	Iai riki nnen log aika tibwa bitaki (T1070). Nnen rongorongo aei iai inanona JWTs ake a rikoaki man TIEWA1.
Meei 2022	Iai riki mataroa mai buki aika karaoaki inanon TIEWA1 (T1505.003). Nte bong aio, ao e riboti nakon ASD ACSC te boboti ae e kunea te mataroa mai buki ae karaoaki inanon Eberi 2022
Meei 2022	Iai taekan burokuraem ae a karaoaki inanon TIEWA1, n aron teuana ae aranaki bwa Log4jHotPatch.jar.
Meei 2022	Kairiran mwakurin kombiuta ibukin kawakinan-ip e kabonganaki ni kariki uoua botu ibukin karaoan mataroa n rinnako. Botu akanne bon 9998 ao 9999 (T1572).

Aia kawai aekita ao aron aia mwakuri

Aika katereaki i nano bon tabeua kawai ao aron Mwakuri buaka ake a kuneaki n tain te kakae.

Moan Rinnakoana

T1190 Anonikaian Memeren Tomein ma Bwain Kombiuta

E katauaki te kurubu aio bwa e aonikai taian RCE, nini akaunti nte tititem, ao e boriaoi aron kikina man memeren aron te rinnako mai kiraroa e aonga n reke moan rinnakona.

E katauaki bwa te anga n rinako aio ena bon reke rinna iai ao aikai bukina:

- Te tiewa e kai rotaki n taian CVE nte tai anne;
- A kataki memere aikai n aonikaiaki man ana tiewa te aekita ae kinaki; ao
- Te moan mwakuri ni kaikoaki i nanoa e ataaki bwa e reke imwin karaoan mwakuri n aonikai.

Mwakuriana

T1059.004 Kairiri ao Anai nano ni Kamwamwane: Unix Shell

Te kurubu aio e reke angan aonikaian memere akana i eta ngkai a kona ni kamaiu mwakuri buaka inanon te Unix shell are inanon te bwai n reitaki ae tauaki taekana. Tabwaninin rongorongon kairiri ake a karaoaki irouia aekita aki kona ni kaweneaki ikai ngkai aki tauaki mwia nte bwai n reitaki.

Taninga marau

T1505.003 Burokuraem inanon te Tiewa: Mataroa mai buki

Aekita a kakaotinakoi mataroa mai buki man te bwai n reitaki are a taua taekana. E bon rereke naba n tabetai ae a tiraua aekita aika kaotinakoi mataroa mai buki, ma ti tabeman mai buakoia ae a kabonganai mataroa akanne. Mataroa mai buki a kona n anga te kona ni mwakuri kairiri aika kakaokoro man bwai n reitaki ake a taui taekaia.

Aonikaian Akaunti nte Tititem

T1068 Aonikaian Akaunti nte Tititem

Bwai ni kakoaua aika iroura aki kabwarabwara bwa tera bwai ake a kona n rinnakoi aekita aikai. Man, kabonganan mataroa mai buki, aekita aikai a kona n reke angan rinnakoia nte tititem ao kona ni kabotauaki ma aron kumean te tiewa are a taua taekana. Mamara ake a kakoauaki bwa iai inanon bwai n reitaki ake a tauaki taekaia e kona n angania nakai reken rinia ni nnen rongorongon te tititem.

Anakin anga ni kikina

T1056.003 Tauan mwin Bwai aika riki: Tauan Mataroan Uebutiaiti

Bwai ni kakoaua man bwai n reitaki ake a tauaki taekaia a kaotia ae aekita aikai a tia n mwanei bubua ma bubua ara ao taeka aika raba, ma koreana ae matata, ao a kakoauaki bwa a maiu. E tara n ae a reke mwanean aikai man kabonganan tabeua bitaki nakon aron karekean te kikina are kakaotinakoi anga ni kikina nakon nnen rongorongo.

T1111 Bomwanean aron kikina-ae mwaiti

Te aekita e mwanei naba manin tain MFA token are a rekereke ma rinnako aika kinaki. A bae ni mwaneaki aikai man bitakin aron karekean te kikina ao man kaotinakoaki nakon nnen rongorongo. Akea bwain kakoaua ae e tauaki taekan te 'tiewa ni karaba' are kawakini man kamanoi taian MFA token.

T1040 Kaneneboian Tititem

E kakoauaki bwa aekita a tia ni mwanei taian JWT man kamwaneaia taan kabongana HTTP man aia bwai n reitaki aika a tauaki taekaia. Iai bwai ni kakoaua ae te bwai ni mwakuri ae tcpdump e kamaiuaki man bwai n reitaki aika tauaki taekaia, are e kona n ae aio aia anga aekita ni mwanei taian JWT aikai.

T1539 Kimoan Kuuki ni Intanete

N aron are kabwarabwaraki i eta, ao te aekita e anai taian JWT, ake a titabo ma kuuki ni intanete. Aikai a kona ni manga kabonganaki iroun te aekita ibukin karaoan riki rinnako.

Te Kakae

T1046 Kakaean Tieweti nte Tititem

Iai te kakoaua ibukin te bwai n tikaen te tititem ae nmap bwa e kakamaiuaki man bwai n reitaki aika tauaki taekaia ibukin tikaenian bwai n reitaki ake tabeua ni mwakoron te tititem ae ti teuana. E tara n ae te aekita e karaoa aei ibukin kakaean riki tititem n tieweti are kona ni manga rinnakoi ao ni kumei riki kanoana.

Te Boota

Bwai ni kakoaua aika iroura e aki kaotia bwa a kanga aekita n rikoi ware ke tera ae anaaki man te bwai n reitaki ae tauaki taekana ke man tititem ake tabeua. Ma, e tara n ae aekita a kona n rinnakoi nnen rongorongo ni kabane ake a mena ni bwai n reitaki ao n taui mwiia, ni ikotaki ma anga ni kikina ake a mwanei (T1003), taian MFA token (T1111), ao taian JWT ake a kabwarabwaraki i eta.

Kairiran ao Taubeakinan

T1071.001 Tuan Kamanoan Burokuraem: Tuan te reitaki Aonrain

Aekita a kabonganai mataroa mai buki ibukin kairiran ao taubeakinan tititem. Kamwakuran mataroa mai buki a kona ni boriaoa HTTPS man kabonganan uebutiaiti ake a mena inanon bwai n reitaki (T1572).

T1001.003 Kamanoan rongorongo aika tabu: Katotongan karaoan Tieweti

Aekita a kakabonganai bwai n reitaki ake a tauaki mwia bwa aia tabo ni karaoi aia ioawa ake a karaoi ibukin rinnakoia ibuakoia taan aonrain.

Taeka ni bau ibukin Te kakae ao Kaokan arona

Te ASD ACSC e katuruturua karaoan taian ASD Waniua katamaroa aika Kakawaki Tauan taekan am tititem ao Aroaro ibukin Kauarerekean kanganga nte kamano nte intanete. Noori i nano taeka ni bau ibukin mwakuri ake a riai ni karaoaki ibukin kakaean ao totokoan rinnako ni kamangao n taian APT40, ao ni ikotaki ma anga ni kaoka aron am tititem man kabonganan aua kingin TTP ake n Taibora 1.

Kakaeana

Tabeua nnen rongorongo ake a kaotaki i eta a nneaki n tabo aika C:\Users\Public* ao C:\Windows\Temp*. Taabo akanne a kona ni kabonganaki ibukin te tabo ni koro rongorongo ngkai angin te tai a kona ni bitaki, are nanona, bwa a kona ni kabane taan kabongana te tititem n rinnakoi nnen rongorongo akanne. Angin te tai, ao taan kamanena te tititem a kona ni kauki nnen rongorongo akanne, ao ni kariaia kumeana, boriaoi kamano, mwakuri burokuraem aika- karako ao katauraoi kaotinakoan rongorongo.

Tuua aika i nano ae aranaki bwa Sigma a kakaei karaoan mwakuri man tabo ake a kanano uoua bwa kanikinaean karaoan mwakuri aika aki riai. Ngkana e riki aio, ao e kainanoaki naba ngkekei te ukeuke ibukin kamatoan mwakuri ni kaikoaki ao kinan aomatana.

Atuna: Burokuraem ae kona ni Bitaki Mwakuriana - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Te Kabwarabwara: Kunean karaoan mwakuri man C:\Windows\Temp.

Arona ngkekei:

Te boki n tua aio e ti tatarai karaoan mwakuri ake nte C:\Windows\Temp*. Temp e tabangaki riki kabonganana n taian burokuraem aika aki bati ni kaikoaki are nanona bwa e uarereke aron ana urubwai ni kabotauaki ma mwakuri ake a karaoaki ni burokuraem ae kona ni bitaki ake a mena inanon C:\Windows.

Kanakoan burokuraem ake a maiu man te TITITEM ke mairouia taan kabongana te TITITEM N TIEWETI ena rangi ni kauarerekea mwaitin kakamwakuri ake aki nang kaikoaki ake a tarataraki nte tua aio.

Are nanona bwa te tua aio e kona n aki nori mwakurian kaikoaki ake a korakora riki ngaia are e kakawaki kabonganan tua aikai ibukin atakia taan kabongana ngkana a kataia ni karaoi kaikoaki aika korakora nakon te TITITEM.

Ukerakina:

1. Tuoi ware ake a irekereke ma kamwakuran nnen rongorongo, n aron aroaron te tia kabongana, te reworo ae kamanenaki, tao-rimwian mwakuri nte tai ae waekoa ao ai noran tamei ake a kamaiuaki man nnen rongorongo.
2. Ukeri mwin ana mwakuri te tia kabongana, taratara te tititem, nnen rongorongo ao ware ni boutoka iaon te tiewa ibukin atakin te mwakuri ae karaoaki bwa e kaikoaki ke aki.
3. Ngkana e kainnanoaki kataia ni karekea katoton nnen rongorongon aron kamatebwaiana e aonga n ataki ae bon ngaia raoi.

Reburenti:

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

Tia koro karaki: ASD ACSC

Bongin namwakaina: 2024/06/19

Teina: experimental

Taeki:

- tlp.green
- classification.au.official
- ioawa.mwakuriana

Log Source:

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

Kuneakina:

```
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:
    Te tia kabongana:
    - 'TITITEM'
    - 'TIEWETI NTE TITITEM'
```

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)

Koaua aika kairua:

- Burokuraem n oteta ake a tia ni kabwataki a tia n noraki ni kamaiu burokuraem man Temp.
- Temp iai inanona bwai ni karaoi burokuraem ao bwai ni kaotinakoi naba aika kinaki, ngaia are ena materaoi tarataran mwakuri buaka aikai n tititem ake kam tutuoi (ao n taraki bwa ena kabwataki ke ena aki) imwain kabonganan te tua aio.

Karinan: i nano

Atuna: Burokuraem ae kona ni Bitaki Mwakuriaia - Nnen Rongorongon te Tititem ake aki mena Inanon-Temp

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

Te Kabwarabwara: Kunean karaoan mwakuri man nnen rongorongo are kona ni karaoaki iai bitaki are mena ni nnen burokuraem ake a kakabonganaki nte Windows OS.

Arona ngkekei:

Te boki n tua aio e ti tatarai karaoan mwakuri man burokuraem ake a mena inanon C:\ and particularly C:\Windows*, ma tiaki inanon C:\Windows\Temp (are e tabangaki riki kabonganana n taian burokuraem aika aki bati ni kaikoaki are nanona bwa e uarereke aron ana urubwai).

Nnen rongorongon burokuraem aika raba aki kakabonganaki ngkana e maiu te burokuraem bwa te TITITEM - aio te anga are a kona ni kamaiuaki iai kaikoaki aika uarereke ma a kai bane taia.

Imwin tian moan mwakurin te tititem ao kinakin aron mwakurin kaikoaki ake aki nang kakamaku man tabo aikai, ao te tua aio ena kanganga mwakurina.

Ukerakina:

1. Tuoi ware ake a irekereke ma kamwakuran nnen rongorongo, n aron aroaron te tia kabongana, te reworo ae kamanenaki, tao-rimwian mwakuri nte tai ae waekoa ao ai noran tamei ake a kamaiuaki man nnen rongorongo.
2. Ukeri mwin ana mwakuri te tia kabongana, te tititem, nnen rongorongo ao ware ni boutoka iaon te tiewa ibukin atakin te mwakuri ae karaoaki bwa e kaikoaki ke aki.
3. Ngkana e kainnanoaki kataia ni karekea katoton nnen rongorongon aron kamatebwaiana e aonga n ataki ae bon ngaia raoi.

Reburenti:

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

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

Tia koro karaki: ASD ACSC

Bongin namwakaina: 2024/06/19

Teina: experimental

Taeki:

- tlp.green
- classification.au.official
- ioawa.mwakuriana

Log source:

category: process_creation

product: windows

Kuneakina:

writable_path:

Image|contains:

- ':\\$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:

        Tamnei|kanoana: '\\AppData\\'
        Te tia kabongana: 'TITITEM'

    condition: writable_path and not appdata

Koaua aika kairua:

Burokuraem n oteta ake a tia ni kabwataki a tia n noraki ni kamaiu burokuraem man nnen rongorongo aikai.

E bon rereke n tabetai ae manin burokuraem ao aia bwai ni mwakuri taan mwakuria te tititem ake a kabonganaki ibukin tarataran (taian) tititem ae ea manga mena inanon teuana mai buakon nnen rongorongo aikai ao e riai ni iangoaki aroia teuana-imwin-teuana.

Karinan: i eta

Atuna: Burokuraem ae kona ni Bitaki Mwakuriana - Taan Kabongana

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

Te Kabwarabwara: Kunean karaoan mwakuri man C:\Users\Public* ao Burokuraem aika kona ni bitaki kamaeuaia ake a mena n Users.

Arona ngkekei:

Nnen rongorongon burokuraem aika raba aki kakabonganaki ngkana e maiu te burokuraem bwa te TITITEM - aio te anga are a kona ni kamaiuaki iai kaikoaki aika uarereke ma a kai bane taia.

Ukerakina:

1. Tuoi ware ake a irekereke ma kamwakuran nnen rongorongo, n aron aroaron te tia kabongana, te reworo ae kamanenaki, tao-rimwian mwakuri nte tai ae waekoa ao ai noran tamei ake a kamaiuaki man nnen rongorongo.
2. Ukeri mwin ana mwakuri te tia kabongana, te tititem, nnen rongorongo ao ware ni boutoka iaon te tiewa ibukin atakin te mwakuri ae karaoaki bwa e kaikoaki ke aki.
3. Ngkana e kainnanoaki kataia ni karekea katoton nnen rongorongon aron kamatebwaiana e aonga n ataki ae bon ngaia raoi.

Reburenti:

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

Tia koro karaki: ASD ACSC

Bongin namwakaina: 2024/06/19

Teina: experimental

Taeki:

- tlp.green
- classification.au.official
- ioawa.mwakuriana

Log source:

    category: process_creation
    product: windows

Kuneakina:

```
Taan Kabongana:
    Image|contains:
    - ':\\Users\\All Users\\'
    - ':\\Users\\Contacts\\'
    - ':\\Users\\Default\\'
    - ':\\Users\\Public\\'
    - ':\\Users\\Searches\\'
  appdata:
    Tamnei|kanoana: '\\AppData\\'
    Te tia kabongana: 'TITITEM'
  condition: users and not appdata
```

Koaua aika kairua:

- E bon rereke n tabetai ae manin burokuraem ao aia bwai ni mwakuri taan mwakuria te tititem ake a kabonganaki ibukin tarataran (taian) tititem ae ea manga mena inanon nnen rongorongo aikai ao e riai ni iangoaki aroia teuana-imwin-teuana.

Karinan: i nuka

Kaokan arona

Tauan Mwin Kakamwakuri

Inanon ana tai ni ukeuke ASD ACSC, ao te bwai ae ea bon ririki naba ae urua nakoraoin ao butin te kakae bon akean tauan mwin kakamwakuri n aron tauan mwin bubuti nakon tiewa, tauan mwin Windows, ao tauan mwin intanete ake ngkoa.

E tuatua ASD ACSC ibukin tutuoan ao karaoan nanon aia taeka ni bau iaon Tauan mwin Mwakuri n Windows ao Nikirana Irouia n aron nnen aron karaoana ao taekan burokuraem ake inanon te Nnen Tauan mwin Mwakuri n Windows ao ai Te Manuo ibukin Kamanoan Rongorongo Aron Tarataran Tititem, ao ni karaoi naba kawakinan log nte tabo ae ti teuana ao ai kawakinan log nte tai ae tau.

Barongan bonobono

Barongan bonobono ae ti teuana bwa ena kona ni maiu irouna e aonga ni baiti. E tuatua ASD ACSC karaoan nanon Aron Barongan Tititem, ai moarara riki, tauan mwin Bono raranian te Tititem ngkana e riai ni karaoaki.

Angiin aonikai ake a kabonganaki irouia aekita a ataki irouia aomata ao iai angan bonotana ae tauraoi. Boboti ana riai ni kakoaua bwa bonobono ni kamano ke kaokan aron tititem a karaoaki nakon bwai n reitaki ake a toma ma te intanete inanon 48 te aoa, ao ngkana e kona, ao kabonganai tein burokuraem ake a boou.

Kamaenakoan nnen te Tititem

Kamaenakoan nnen te Tititem e kona ni kangabuakai aron aia mwakuri taan ioawa n aron kakaean nnen ao karekean rinnakoan rongorongon te boboti aika katabuaki. Kamaenakoi tititem ibukin kauarerekean ke buraokinakin mwainging inanon te tititem man aki kariaiakaia taan aonrain. Tiewa ake a bongana n aron ake a kawakinaki iai Nnen Rongorongo aika Kakabonganaki ao ake ibukin kawakinan aron kikina boto n tiewa a riai ni mwakuriaki man tiewa ni katomatoma ke 'tiewa ni kakiba'. Tiewa aikai a riai n tarataraki raoi, a riai ni mano raoi ao n tiatiania taan kabongana ao bwai n reitaki ake a kona n toma ma ngaia.

Ngkana ti aki tarai tai ake a reke iai kanganga ao man totokoaki ninian nanon te tititem, manga karaoan kamaenakoan nnen te tititem e kona riki ni kauarerekea mwaitin rongorongo ake a rinnakoaki ke ni kaotinakoaki irouia aekita.

Angan riki kaokan arona

Taan anga kariaia a tuatua iran aron kaokan tititem aika i nano ibukin buakanakin APT40 ao kabonganan taian TTP irouia tabeman.

- Kamatei tiewetin te tititem ake aki kabonganaki ao ake aki bongana, botu ao anga n te reitaki.
- Kabongana te burokuraem n totoko te o te ai aika karaoaki-raoi (WAF) ibukin katanan tiewa ao burokuraem
- Kamatoa bwa nake i nano aia akaunti ana uarereke aron kumean tiewa irouia, tibwakin nnen rongorongo, ao ritioti riki ake tabeua.
- Kabonganai aron-kikina aika mwaiti (MFA) ao akaunti ni mwakuri ake a barongaki, aonga ni matoa aron kuraekinakin ao manga kabonganan aron kikina. MFA e riai ni karaoaki nakon rinnakoan tieweti ake a toma ma te intanete n aron:
  - Imeri man Uebutiaiti ao man-tiewa
  - Te tabo ni Tamwaomwao
  - Katomatoma ma tititem ni kamano ae onoti
  - Kombiuta Tieweti mai Kiraroa
- Kaboui bwai ni mwakuri ake a kan-bane-taia.

Taibora 1: Angan Kaokan arona/Aron Mwakuriana

TTP	Waniua Kawai aika Kakawaki ibukin Kaokan Arona	ISM Mwakuriana
Moan Rinnakoana T1190 Aonikaian Burokuraem ake a kabonganai-aomata	Bonoti burokuraem Bonoti tititem ni mwakuri Aron-Kinakina ae Mwaiti Taubeakinan Burokuraem	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Mwakuriana T1059 Kairiri ao Anai nano ni Kamwamwane	Taubeakinan Burokuraem Kakeai Microsoft Office Macros Kakeai mwakaia taan mwakuria	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Taninga marau T1505.003 Kanoan ana Burokuraem te Tiewa: Mataroa mai buki	Taubeakinan Burokuraem Kakeai mwakaia taan mwakuria	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Moan Rinnakoana / Aonikaian Akaunti nte Tititem / Taninga marau T1078 Akaunti aika Maiu	Bonoti tititem ni mwakuri Aron-Kinakina ae Mwaiti Kakeai mwakaia taan mwakuria Taubeakinan Burokuraem Kamatoan Burokuraem ibukia katitamwa	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

Ibukin riki taeka ni buobuoki n aron te kakae ao kaokan arona, taiaoka noora Kakae ao Kaokan arona are iaon te uebutiaiti ae aron mwakurian MITRE ATT&CK ibukin are a kaotaki nte kauarereke ibukin MITRE ATT&CK aron mwakuriana e mena i nano raoi nte kamatata aei.

Otanga

Rongorongo aika oti n te riboti aei a katauraoaki "n aroia aei" ti ibukin am rongorongo. Rabwata ake anganga kariaia a bon aki tei ibukin rabwata ni karikirake, kaako, kambwana, ke tieweti, ni ikotaki ma rabwata, kaako, ke tieweti ake a oti nte beeba aio. Taekinakin ma reburenti nakon rabwata ni karikirake, kaako, kawai, ke tieweti man te tieweti ae iai kanikinaeana, te kanikina, taan karaobwai, ke tabeman riki, e bon aki tei ke n anga te kariaia, taeka ni bau, ke n nanonaki irouia taan anga kariaia.

E kanikinaeaki te boreti aei n TLP:CLEAR. Tai tikotikona kaotana. Ritioti a kona n TLP:CLEAR ngkana rongorongo ake i nanona e karako ke ana bon akea iai ananga ni kanganga ngkana a kabonganaki buaka, aio e iri nanon tua ao aron karaoan kaotinako rongorongo nakon te bota n aomata. Man iran nanon tuan te bwaibwai aio ao, rongorongo ake a TLP:CLEAR a kona n tibwaki n aki tiatianaki. Ibukin riki rongorongon Aron Barongan Rongorongo aika taburoroko nora cisa.gov/tlp

MITRE ATT&CK – Taraan karakin APT40 kamwakuran te tarena

Taukiroo (TA0043)	
Kakaei aia Uebutiaiti-Konaia (T1594)	Rikoan Aron kinakin Konaia: Anga ni kikina (T1589.001)
Tikaen ae Maeu: Tikaenian memere (T1595.002)	Rikoan Aron kinakin Tiewa (T1592)
Kakaei Uebutiaiti aika uki/Tomain: Intin ni Kakae (T1593.002)	Rikoan Rongorongon aia Tititem Konaia: Kaubwain Tomein (T1590.001)
Rikoan Aron kinakin Konaia: Imeri Aetureti (T1589.002)	

Karikirakean Kaubwai (TA0042)	
Karekei Kateitei: Taian Tomein (T1583.001)	Karekei Kateitei (T1583)
Karekei Kateitei: DNS Tiewa (T1583.002)	Tauan taekan Akaunti (T1586)
Karikirakean Konabwai: Certificate ibukin tiainan burokuraem (T1587.002)	Tauan taekan Bwai ni mwakuri (T1584)
Karikirakean Konabwai: Certificates Aonrain (T1587.003)	Karikirakean Konabwai: Mwauea (T1587.001)
Karekean Konabwai: Certificate ibukin tiainan burokuraem (T1588.003)	Karaoi Akaunti: Akaunti man Tiewa (T1585.003)
Compromise Infrastructure: Bwai n Reitaki nte Tititem (T1584.008)	Karekean Konabwai: Certificates Aonrain (T1588.004)

Moan rinnakoana (TA0001)	
Akaunti aika Maiu (T1078)	Katairake (T1566)
Akaunti aika Maiu: Tein Akaunti (T1078.001)	Katairake: Mwauea nte imeri (T1566.001)
Akaunti aika Maiu: Akaunti man Tomein (T1078.002)	Katairake: Mwauea nte Rinki (T1566.002)
Tieweti mai Kiraroa (T1133)	Aonikaian Burokuraem Kabonganai-Aomata (T1190)
Mauan Taekann Kawaran-Uebutiaiti (T1189)	

Mwakuriana (TA0002)	
Bwain mwakurian Barongan Windows (T1047)	Kairiri ao Anai nano ni Kamwamwane: Python (T1059.006)
Mwakuri aika Tainaki/Beku: At (T1053.002)	Kairiri ao Anai nano ni Kamwamwane: JavaScript (T1059.007)
Mwakuri aika Tainaki/Beku: Mwakuri aika Tainaki (T1053.005)	API i nanoa(T1106)
Kairiri ao Anai nano ni Kamwamwane (T1059)	Te Reitaki i Marenan Burokuraem(T1559)
Kairiri ao Anai nano ni Kamwamwane: Command are ni Windows (T1059.003)	Tieweti nte Tititem: Mwakurian Tieweti (T1569.002)
Kairiri ao Anai nano ni Kamwamwane: PowerShell (T1059.001)	Aonikaian mwin aia bobwai katitamwa (T1203)
Kairiri ao Anai nano ni Kamwamwane: Visual Basic (T1059.005)	Mwakuriana irouia taan kabongana: Nnen rongorongo aika Kaikoaki (T1204.002)
Kairiri ao Anai nano ni Kamwamwane: Unix Shell (T1059.004)	Kairiri ao Anai nano ni Kamwamwane: Apple Script (T1059.002)
Mwakuri aika Tainaki/Beku: Cron (T1053.003)	Bwain Kaotinakoan Burokuraem (T1072)

Taninga marau (TA0003)	
Akaunti aika Maiu (T1078)	Kanoan ana Burokuraem te Tiewa: Mataroa mai buki (T1505.003)
Mwauea inanon Nnen waren kamaeuana: Taian Macro man Office (T1137.001)	Karaoan ao Bitakin Mwakurin Tititem: Ana Tieweti Windows (T1543.003)
Mwakuri aika Tainaki/Beku: At (T1053.002)	Boot ke ena Maiu ngkana ko Logon: Mwin Kamaeuan Burokuraem / Nnen Waren moan Kamaeuana (T1547.001)
Mwakuri aika Tainaki/Beku: Mwakuri aika Tainaki (T1053.005)	Boot ke ena Maiu ngkana ko Logon: Bitakin Kauarereke (T1547.009)
Tieweti mai Kiraroa (T1133)	Bitakin aron mwakurin burokuraem: DLL Taumatoan Barongan aron Kakae (T1574.001)
Mwakuri aika Tainaki/Beku: Cron (T1053.003)	Bitakin aron mwakurin burokuraem: DLL Karaban Karinan-Burokuraem (T1574.002)
Kunimwanian Akaunti (T1098)	Akaunti aika Maiu: Akaunti man Tiewa (T1078.004)
Akaunti aika Maiu: Akaunti man Tomein (T1078.002)	

Aonikaian Akaunti nte Tititem (TA0004)	
Mwakuri aika Tainaki/Beku: At (T1053.002)	Karaoan ao Bitakin Mwakurin Tititem: Ana Tieweti Windows (T1543.003)
Mwakuri aika Tainaki/Beku: Mwakuri aika Tainaki (T1053.005)	Boot ke ena Maiu ngkana ko Logon: Mwin Kamaeuan Burokuraem / Nnen Waren moan Kamaeuana (T1547.001)
Karinan anga n Tokobito: Taumatoan aron Kamaeuan Burokuraem (T1055.003)	Boot ke ena Maiu ngkana ko Logon: Bitakin Kauarereke (T1547.009)
Karinan anga n Tokobito: Bitakin Burokuraem ae raba (T1055.012)	Bitakin aron mwakurin burokuraem: DLL Taumatoan Barongan aron Kakae (T1574.001)

Aonikaian Akaunti nte Tititem (TA0004)	
Akaunti aika Maiu: Akaunti man Tomein (T1078.002)	Aonikaian Akaunti nte Tititem (T1068)
Kunimwanian Token ni Karirin Katotongan Token/Te Kimoa (T1134.001)	Mwakuri aika Kamaui Mwauea: Bitakin Karaoan Unix Shell (T1546.004)
Karinan anga n Tokobito: Karinan Rinki-aika Kaikoaki nte Raiburari (T1055.001)	Akaunti aika Maiu: Akaunti man Tomein (T1078.002)
Akaunti aika Maiu: Akaunti i Nanoa (T1078.003)	

Boriaoan Kamano (TA0005)	
Rootkit (T1014)	Mwakurian Nanon Kairiri mai Kiraroa (T1202)
Nnen Rongorongo ke Rongorongo aika kamabubuaki (T1027)	Kumetoan te Binary Tititem man Proxy Tiewa: Mshta (T1218.005)
Nnen Rongorongo ke Rongorongo aika kamabubuaki: Rabwakaian Burokuraem (T1027.002)	Kumetoan te Binary Tititem man Proxy Tiewa: Regsvr32 (T1218.010)
Nnen Rongorongo ke Rongorongo aika kamabubuaki: Karaban rongorongo i matawa (T1027.003)	Boriaoan Kamanoan Tiewa aika toma: Tiainakin Burokuraem (T1553.002)
Nnen Rongorongo ke Rongorongo aika kamabubuaki: Uatabeuan Karinan Mwauea (T1027.004)	Bitakin Kariaia ibukin Nnen Ware ao Rongorongo: Bitakin Kariaia Ibukin Nnen Ware ao Rongorongo nte Linux ao Mac. (T1222.002)
Katotonga: Katitaboi Ara ma Tabo aika kinaki (T1036.005)	Aron/Karaban mwauea: Tuoan Tititem (T1497.001)
Karinan anga n Tokobito: Taumatoan aron Kamaeuan Burokuraem (T1055.003)	Katotonga (T1036)
Karinan ao Kamwakuran inanon Memori (T1620)	Kamamarai Totoko: Kamatei ke Bita te O te Ai nte Tititem (T1562.004)
Karinan anga n Tokobito: Bitakin Burokuraem ae raba (T1055.012)	Karabai Tamrurun Rongorongo: Ware ao Rongorongo aika Karabaki (T1564.001)
Kanakoan Kanikina: Kamaunan Nnen Ware (T1070.004)	Karabai Tamrurun Rongorongo: Burokuraem ake a maiu man Raba: (T1564.003)
Kanakoan kanikina: Tauan mwin te Tai (T1070.006)	Bitakin aron mwakurin burokuraem: DLL Taumatoan Barongan aron Kakae (T1574.001)
Kanakoan kanikina: Kamaunan Mwin Log ni Windows (T1070.001)	Bitakin aron mwakurin burokuraem: DLL Karaban Karinan-Burokuraem (T1574.002)
Bitan Tauan mwin rongorongo (T1112)	Uebutiaiti Tieweti (T1102)
Kaotan/Kamaenakoan nnen ware ke rongorongo (T1140)	Katotonga: Katotongan Mwakuri ke Tieweti (T1036.004)
Kamamarai Totoko (T1562)	

Anakin Anga ni kikina (TA0006)	
OS Kakaean Anga ni Kikina: LSASS Memori (T1003.001)	Anga ni Kikina aika aki mano: Anga ni Kikina inanon Nnen Rongorongo (T1552.001)
OS Kakaean Anga ni Kikina: NTDS (T1003.003)	Ukeran Manin Aron Kikina: Ketinan Taeka ni karaba (T1110.001)
Kaneneboian Tititem (T1040)	Kakaraoan aron te kikina (T1187)

Anakin Anga ni kikina (TA0006)	
Anga ni kikina man Titoan Taeka aika raba: Nnen Taeka aika raba (T1555.001)	Kimoan ke Karaoan Kerberos Tiketi: Kerberoasting (T1558.003)
Tauan mwin Bwai aika riki: Tauan mwin taibi (T1056.001)	Bobwanean Aron Kikina Aika-Bati (T1111)
Kimoan Kuuki ni Intanete (T1539)	Kimoan Token ibukin Rinnakoan Burokuraem (T1528)
Aonikai ibukin Anakin anga ni kikina (T1212)	Ukeran Manin Aron Kikina: Kinakinakin Taeka aika raba (T1110.002)
Tauan mwin Bwai aika riki: Tauan mataroan uebutiaiti (T1056.003)	OS Kakaean Anga ni Kikina: DCSync (T1003.006)
Anga ni kikina man Titoan Taeka aika raba (T1555)	Anga ni kikina man Titoan Taeka aika raba: Anga ni kikina man te Burautia (T1555.003)

Te Kakae (TA0007)	
Kakaean ana Tieweti te Tititem (T1007)	Kakaean Rongorongon te Tititem (T1082)
Kakaean Bwangabwangan te Burokuraem (T1010)	Kakaean Akaunti: Akaunti i Nanoa (T1087.001)
Tauan mwin Titiraki (T1012)	Kakaean Rongorongon te Tititem, Aron mwakuriana T1082 - Boboti | MITRE ATT&CK®
Kakaean Nnen Rongorongo (T1083)	Kakaean Tain ana tabo te tititem (T1124)
Kakaean ana Tieweti te Tititem (T1046)	Te Tia Bwaibwai nte Tititem/Kakaeaia taan kabongana (T1033)
Kakaean System mai Kiraroa (T1018)	Kakaean Tomein aika Toma (T1482)
Kakaean Akaunti: Imeri Akaunti (T1087.003)	Kakaean Akaunti: Tomein Akaunti (T1087.002)
Kakaean Bwai n reitaki ake a Toma ma te Tititem (T1049)	Aron/Karaban mwauea: Tuoan Tititem (T1497.001)
Kakaean aron mwakurina (T1057)	Kakaean buromuraem (T1518)
Kakaean aron kainakin kurubu: Tomein Kurubu (T1069.002)	Kakaean Bwai n Reitaki nte Tititem, Aron Mwakuriana T1135 - Boboti | MITRE ATT&CK®
Kakaean aron katean tititem: Kakaean te tabo ao tomaa te intanete (T1016.001)	

Kumeana riki (TA0008)	
Tieweti mai Kiraroa: Aron kamaiuan Kombiuta mai Kiraroa (T1021.001)	Tieweti mai Kiraroa (T1021)
Tieweti mai Kiraroa: SMB/Windows Baronga mai Kiraroa (T1021.002)	Kabonganai Bwain Aron Kinakim ake Tabeua: Kimoan Tiketi (T1550.003)
Tieweti mai Kiraroa: Barongan Windows mai Kiraroa (T1021.006)	Kakiban Bwai ni Kume (T1570)

Te Boota (TA0009)	
Rongorongo man Tititem Inanoa (T1005)	Kawakinan Ware ake a Bobotaki: Kawakinaki nte raiburi (T1560.002)
Ware ake a Ibuobuokaki nte Tititem (T1039)	Bota n imeri: Bobotan imeri mai Kiraroa (T1114.002)

Te Boota (TA0009)	
Tauan mwin Bwai aika riki: Tauan mwin taibi (T1056.001)	Nnen Rongorongo ni Bwai n Reitaki (T1115)
Rikoriko i bon irouna (T1119)	Ware man Nnen Rongorongo (T1213)
Tauan mwin Bwai aika riki: Tauan mataroan uebutiaiti (T1056.003)	Ware aika Karioaki: Karioan Ware mai Kiraroa (T1074.002)
Ware aika Karioaki: Karioan Ware i Nanoa (T1074.001)	Kawakinan Ware ake a Bobotaki (T1560)
Bota n imeri (T1114)	

Kimoan rongorongo (TA0010)	
Kimoan rongorongo man C2 Channel (T1041)	Kimoan rongorongo man Alternative Protocol: Kimoan rongorongo man Asymmetric Encrypted Non-C2 Protocol (T1048.002)
Kimoan rongorongo man Alternative Protocol (T1048)	Kimoan rongorongo man Web Service: Kimoan rongorongo nakon Tiewa (T1567.002)

Kairiri ao Tatauo (TA0011)	
Kamanoan rongorongo aika tabu: Katotongan Karaoan tieweti (T1001.003)	Uebutiaiti Tieweti: Aonikaian Bwai man Uebutiaiti n Tieweti (T1102.001)
Te botu ae Nang Kakabonganaki (T1043)	Uebutiaiti Tieweti: Te Reitaki ae Tabo-Itera (T1102.003)
Tuan te Reitaki i marenan Burokuraem: Tuan Uebutiaiti (T1071.001)	Karinan Mwauea n Tititem (T1105)
Tuan te Reitaki i marenan Burokuraem: Tuan Kakiban Nnen Rongorongo (T1071.002)	Proxy: Proxy i Nanoa (T1090.001)
Proxy: Proxy mai Kiraroa (T1090.002)	Botu aika Kabonganaki-Buaka Botu (T1571)
Proxy: Kabonganan Proxy aika-tiraua (T1090.003)	Tuan Karinrin nte Tititem (T1572)
Uebutiaiti Tieweti: Te Reitaki ae Kauaitera (T1102.002)	Channel aika Kamanoaki (T1573)
Channel aika Kamanoaki: Cryptography Ibukin te Kikina (T1573.002)	Karinan Mwauea n Tititem (T1105)
Proxy, Aron Mwakuriana T1090 - Bitiniti | MITRE ATT&CK®	

Rotakina (TA0040)	
Katokan Tieweti (T1489)	Kamauna Ware ni Kabane (T1561)
Kamatean Tititem/Ribuuti (T1529)	Taumatoan Ritioti (T1496)

Taeka ni Kauring

Otanga

Kanoan te kamatata e bon kabuta ao n aki taraki bwa taian ibuobuoki nakon te tua ke n rangi kabotoaki bwa ngaia buokam inanon te tai are e kainanoaki iai ke inanon te karina. E kakawaki, bwa ko bon riai ni ukeuke ni kakae nako nakoia ake a mwatai ibukin aia ibuobuoki ni kaineti ma kainanom.

Te Kaomwanwareta e aki kataua bwa ngaia ae na bukinaki n reken uruaki, ni buan ke n reken kabanemwane aika ana kaoti ae riki man kamanenaan rongorongo ake inanon te kaita aio.

Kaobiraita

Kabonganan Kanikinaean Boboti

Taian kainibaire ake a bwaka iaan Kanikinaean Boboti a kona ni kamanenaki ni kabwarabwarana ae oti n ana uebutiati te Ana Aobiti te Buraim Minitita ao an Tomain Kaebineti Kanikinaean Boboti Rongorongo ao Kainibaire | pmc.gov.au.

Ibukin rongorongona riki, ke n ribotini kanganga n te cyber security, reitaki nakoira:

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

Te number aio e ti kona ni kabonganaki iaon Aotiteria.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre