APT40 Advisory

PRC MSS tradecraft in action

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**

Talaan ng nilalaman

Pangkalahatang-ideya

Background

Ang pabatid na ito, na isinulat ng Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), United States Cybersecurity and Infrastructure Security Agency (CISA), United States National Security Agency (NSA), United States Federal Bureau of Investigation (FBI), United Kingdom National Cyber Security Centre (NCSC-UK), Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NCSC-NZ), German Federal Intelligence Service (BND) at Federal Office for the Protection of the Constitution (BfV), National Intelligence Service (NIS) ng Republika ng Korea at ang National Cyber Security Center ng NIS, at National Center of Incident Readiness and Strategy for Cybersecurity (NISC) at National Police Agency (NPA) ng Japan – na tatawagin dito bilang "mga ahensiyang may-akda" – ay naglalarawan ng isang cyber group na suportado ng estado ng People's Republic of China (PRC) at ang kasalukuyan nilang banta sa mga network ng Australya. Ang pabatid ay batay sa pinagsamang pag-unawa ng mga ahensiyang may-akda tungkol sa banta, pati na rin sa mga pagsisiyasat ng ASD's ACSC hinggil sa pagtugon sa insidente (incident response).

Ang PRC state-sponsored cyber group na ito ay dati nang umatake sa mga organisasyon sa iba't ibang bansa, kabilang ang Australya at Estados Unidos, at ang mga teknik na itinatampok sa ibaba ay karaniwang ginagamit ng iba pang mga cyber actor na suportado ng PRC sa buong mundo. Dahil dito, naniniwala ang mga ahensiyang may-akda na ang grupong ito, at mga katulad na teknik, ay patuloy na banta sa mga network ng kanilang mga bansa.

Tinataya ng mga ahensiyang may-akda na ang grupong ito ay nagsasagawa ng mga malicious cyber operation para sa PRC Ministry of State Security (MSS). Ang mga aktibidad at teknik ay may pagkakapareho sa mga grupong sinusubaybayan bilang Advanced Persistent Threat (APT) 40 (kilala rin bilang Kryptonite Panda, GINGHAM TYPHOON, Leviathan at Bronze Mohawk sa mga report ng industriya). Inireport noon na ang grupong ito ay nakabase sa Haikou, Hainan Province, PRC at tumatanggap ng mga utos mula sa PRC MSS, Hainan State Security Department.[2] Ang sumusunod na Pagpapayo ay nagbibigay ng halimbawa ng mga makabuluhang case study kung paano ginamit ng kalabang ito ang kanilang mga teknik laban sa dalawang network ng biktima. Mahalaga ang mga case study na ito para sa mga practitioner ng cyber security upang tukuyin, pigilan, at maremedyuhan ang mga pagsalakay ng APT40 sa kani-kanilang mga network. Ang mga napiling case study ay ang mga naaksyunan nang maayos upang mabawasan ang panganib ng muling pagsamantala ng naturang threat actor o iba pa. Dahil dito, ang mga case study ay likas na mas luma upang mabigyan ang mga organisasyon ng sapat na panahon para maremedyuhan.

Buod ng aktibidad

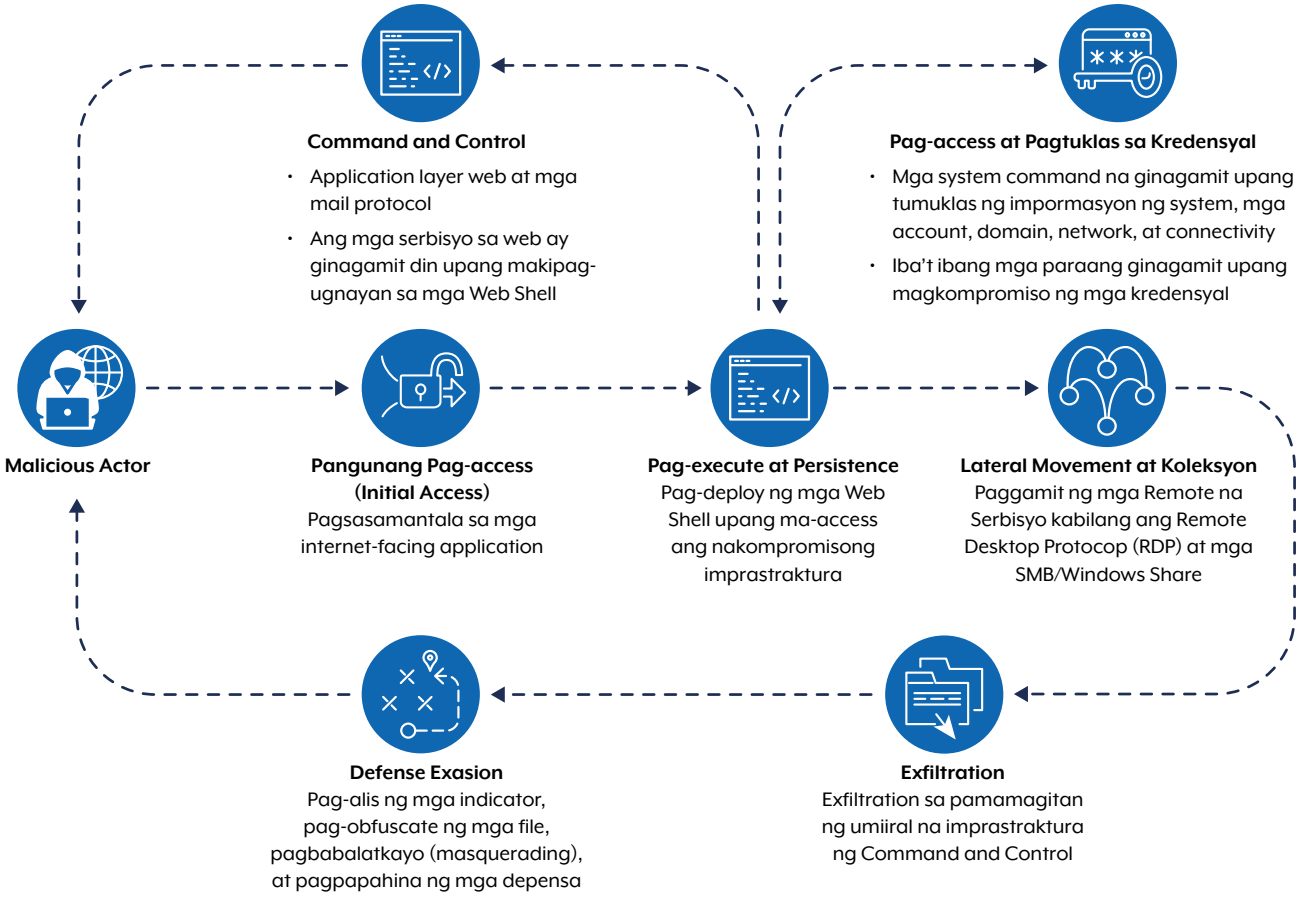
Paulit-ulit nang tina-target ng APT40 ang mga network sa Australya gayundin ang mga network ng gobyerno at pribadong sektor sa rehiyon, at patuloy ang banta na dulot nila sa ating mga network. Ang mga tradecraft na inilarawan sa pabatid na ito ay regular na inoobserbahang laban sa mga network sa Australya.

Partikular, ang APT40 ay may kakayahang mabilis na baguhin at iangkop ang mga exploit proof-of-concept (POCs) ng mga bagong kahinaan at agad itong gamitin laban sa mga target na network na may imprastraktura ng kaugnay na kahinaan. Regular na nagsasagawa ang APT40 ng reconnaissance sa mga network na nais nitong atakehin, kabilang ang mga network sa mga bansa ng mga ahensiyang may-akda, upang maghanap ng mga oportunidad para makompromiso ang mga target nito. Ang regular na reconnaissance na ito ay naglalagay sa grupo sa posisyon upang matukoy ang mga device na may kahinaan, malapit ng mawalan ng bisa (end-of-life), o hindi na mine-maintain sa mga network na nais nilang atakehin, at mabilis na mag-deploy ng mga exploit. Patuloy na nagtatagumpay ang APT40 sa pagsasamantala sa mga kahinaan mula pa noong 2017.

Mabilis ding sinasamantala ng APT40 ang mga bagong labas na kahinaan sa malawakang ginagamit na software gaya ng Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) at Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473). Inaasahan ng ACSC ng ASD at ng mga ahensiyang may-akda na patuloy na gagamitin ng grupo ang mga POC para sa mga bagong high-profile na kahinaan sa loob lamang ng ilang oras o araw mula sa paglabas nito sa publiko.

2 U.S. Department of Justice. 2021 Apat na Tsino na Nagtatrabaho sa Ministry of State Security na Naatasan sa Pandaigdigang Kampanya ng Pag-intrude sa Kompyuter na Tinatarget ang Intellectual Property at Kumpidensyal na Impormasyon ng Negosyo, Kasama ang Pananaliksik sa Nakahahawang Sakit.

Larawan 1: TTP flowchart para sa aktibidad ng APT40



Tila mas gusto ng grupong ito ang pagsasamantala sa mga public-facing na imprastraktura na may kahinaan kaysa sa mga teknik na nangangailangan ng interaksyon ng user, gaya ng mga phishing campaign, at binibigyan nila ng mataas na prayoridad ang pagkuha ng mga balidong kredensyal upang maisagawa ang marami pang mga kasunod na aktibidad. Madalas gumagamit ang APT40 ng mga web shell (T1505.003) para sa persistence, partikular sa unang yugto ng buhay ng isang panghihimasok (intrusion). Karaniwan, matapos matagumpay na makakuha ng pangunang pag-access, nakatuon ang APT40 sa pagtatatag ng persistence para mapanatili ang access sa kapaligiran ng biktima. Dahil ang persistence ay nangyayari sa maagang yugto ng isang intrusion, malamang na makita ito sa lahat ng intrusion - anuman ang lawak ng kompromiso o mga sumunod na hakbang.

Mahahalagang sining sa paniniktik (tradecraft)

Bagama't dati nang ginamit ng APT40 ang mga na-kompromisong website sa Australya bilang mga command and control (C2) host para sa kanilang mga operasyon, pinaunlad na ng grupo ang teknik na ito (T1594).

Tinanggap ng APT40 ang pandaigdigang trend na paggamit ng mga nakompromisong device, kabilang ang mga small-office/home-office (SOHO) device, bilang operational infrastructure at mga last-hop redirector (T1584.008) para sa kanilang operasyon sa Australya. Dahil dito, mas mahusay na nagagawang ilarawan at subaybayan ng mga ahensiyang may-akda ang mga galaw ng grupong ito.

Marami sa mga SOHO device na ito ay end-of-life na o unpatched at nagiging madaling target para sa N-day exploitation. Kapag nakompromiso, nagiging launching point ang mga SOHO device para sa mga atake na idinisenyong magmukhang lehitimong trapiko at pahirapan ang mga tagapagtanggol ng network (T1001.003).

Regular ding ginagamit ang teknik na ito ng iba pang mga PRC state-sponsored actor sa buong mundo, at itinuturing ito ng mga ahensiyang may-akda bilang isang pinagsasaluhang banta (shared threat). Para sa karagdagang impormasyon, tingnan ang mga magkatuwang na pabatid (joint advisory) People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices at PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.

Paminsan-minsan, gumagamit ang APT40 ng biniling o inuupahang imprastraktura bilang victim-facing C2 infrastructure sa kanilang mga operasyon; gayunpaman, tila bumababa na ang paggamit sa tradecraft na ito.

Tooling

Ibinabahagi ng ACSC ng ASD ang ilan sa mga malicious file na natukoy sa panahon ng mga pagsisiyasat na nakabalangkas sa ibaba. Na-upload ang mga file na ito sa VirusTotal upang matulungan ang mas malawak na komunidad ng depensa sa network at cyber security na mas maunawaan ang mga banta na kailangan nilang labanan.

Mga case study

Ibinabahagi ng ACSC ng ASD ang dalawang hindi pagkakakilanlang reports ng pagsisiyasat upang magbigay-kaalaman kung paano ginagamit ng mga actor ang kanilang mga kasangkapan at teknik.

MD5	Filename	Karagdagang impormasyon
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Pinagmulan ng Java
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

Case study 1

Ang report na ito ay hindi nagpapakilala upang mas malawak na maipakalat. Ang naapektuhang organisasyon ay tutukuyin mula ngayon bilang 'ang organisasyon'. Ang ilang partikular na detalye ay inalis upang protektahan ang pagkakakilanlan ng biktima at mga paraan ng pagtugon sa insidente (incident response) ng ACSC ng ASD.

Pang-ehekutibong buod (Executive summary)

Ipinapaliwanag ng report na ito ang mga natuklasan ng pagsisiyasat ng ACSC ng ASD hinggil sa matagumpay na pagkompromiso sa network ng organisasyon mula Hulyo hanggang Setyembre 2022. Ang report ng pagsisiyasat na ito ay ibinigay sa organisasyon upang ibuod ang mga nakitang malicious activity at upang magbigay ng mga mungkahi sa pagremedyo. Ipinapakita ng mga natuklasan na ang pagkompromiso ay isinagawa ng APT40.

Noong kalagitnaan ng Agosto, ipinaalam ng ACSC ng ASD sa organisasyon ang tungkol sa mga malisyosong interaksyon sa kanilang network mula sa isang device na malamang ay nakompromiso at ginagamit ng grupo noong huling bahagi ng Agosto at, sa pahintulot ng organisasyon, nag-deploy ang ACSC ng ASD ng mga host-based sensor sa mga host na malamang naapektuhan sa network ng organisasyon. Dahil dito, nagkaroon ng pagkakataon ang mga incident response analyst ng ACSC ng ASD na magsagawa ng masusing digital forensics investigation. Gamit ang nakuhang sensor data, matagumpay na nagawa ng mga analyst ng ACSC ng ASD na imapa ang mga aktibidad ng grupo at gumawa ng detalyadong timeline ng mga naobserbahang pangyayari.

Mula Hulyo hanggang Agosto, ang mga pangunahing aktibidad ng actor na naobserbahan ng ACSC ng ASD ay kinabibilangan ng:

- host enumeration, na nagbibigay-daan sa actor na bumuo ng sarili nitong mapa ng network;
- paggamit ng web shell, na nagbibigay sa actor ng pangunang pagtuntong (foothold) sa network at kakayahang mag-execute ng mga command; at
- pag-deploy ng iba pang mga tooling na ginamit ng actor para sa mga malisyosong layunin.

Natuklasan ng pagsisiyasat ang ebidensya na malalaking halaga ng sensitibong data ang na-access at ebidensya na ang mga actor ay nakagalaw nang lateral sa loob ng network (T1021.002). Maraming bahagi ng kompromiso ang naging posible dahil sa pagtatatag ng grupo ng maraming access vector papasok sa network, pagkakaroon ng flat structure ng network, at paggamit ng hindi ligtas na software na binuo sa loob ng organisasyon na maaaring gamitin upang mag-upload ng mga file nang hindi awtorisado. Kabilang sa mga na-exfiltrate na data ang mga privileged authentication credential na nagbigay-daan sa grupo na makapag-log in, gayundin ang network information na makatutulong sa mga actor na muling makapasok nang walang awtorisasyon kung sakaling maharang ang original access vector. Walang nadiskubreng karagdagang malicious tooling bukod sa mga nasa pangunang nasamantalang machine; subalit, ang pagkakaroon ng grupo ng mga lehitimo at may pribilehiyong kredensyal ay nag-aalis ng pangangailangan para sa karagdagang tooling. Ipinapahiwatig ng mga natuklasan sa pagsisiyasat na ang organisasyon ay malamang na sadyang tinarget ng APT40, sa halip na basta na lamang nabiktima dahil sa kahinaang kilala ng publiko.

Mga natuklasan sa pagsisiyasat

Noong kalagitnaan ng Agosto 2022, ipinaalam ng ACSC ng ASD sa organisasyon na may nakumpirmang malicious IP na pinaniniwalaang kaugnay ng isang state-sponsored cyber group na nakipag-ugnayan sa mga computer network ng organisasyon sa pagitan ng Hulyo hanggang Agosto. Ang nakompromisong device ay malamang na pag-aari ng isang maliit na negosyo o isang home user.

Noong huling bahagi ng Agosto, nag-deploy ang ACSC ng ASD ng isang host-based agent sa mga host sa network ng organisasyon na nagpapakita ng ebidensya na naapektuhan sila ng pagkompromiso.

Ang ilang artefact na sana'y makatutulong sa mga pagsisikap ng pagsisiyasat ay hindi nagamit dahil sa configuration ng logging o network design. Sa kabila nito, ang kahandaan ng organisasyon na ibigay ang lahat ng magagamit na data ay nagbigay-daan sa mga incident responder ng ACSC ng ASD na magsagawa ng komprehensibong pagsusuri at makabuo ng malinaw na pag-unawa sa posibleng aktibidad ng APT40 sa network.

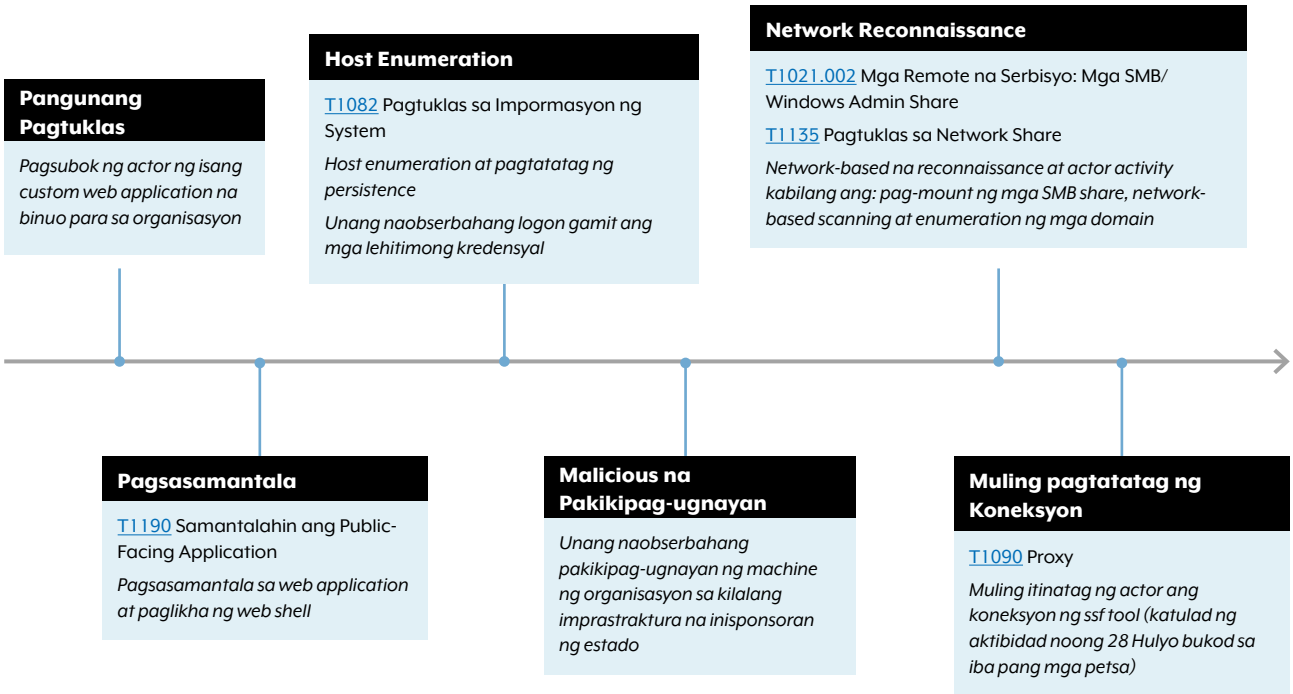
Noong Setyembre, matapos ang konsultasyon sa ACSC ng ASD, nagpasya ang organisasyon na i-denylist ang IP na natukoy sa paunang pabatid. Noong Oktubre, sinimulan ng organisasyon ang pagremedyo.

Mga Detalye

Noong simula ng Hulyo, nagawa ng mga actor na subukan at samantalahin ang isang custom web application (T1190) na tumatakbo sa `<webapp>2-ext`, na nagbigay sa grupo ng kakayahan na makapagtatag ng foothold sa network demilitarized zone (DMZ). Ginamit ito upang ma-enumerate ang parehong network at lahat ng nakikitang domain. Ginamit ang mga nakompromisong kredensyal (T1078.002) upang i-query ang Active Directory (T1018) at i-exfiltrate ang data sa pamamagitan ng pag-mount ng mga file share (T1039) mula sa maramihang machine sa loob ng DMZ. Isinagawa ng actor ang isang Kerberoasting attack upang makakuha ng mga balidong mga kredensyal ng network mula sa isang server (T1558.003). Walang naobserbahang mga karagdagang point of presence ang grupo sa DMZ o sa internal network.

Visual timeline

Ang timeline sa ibaba ay nagbibigay ng pangkalahatang buod ng mga pangunahing yugto ng malicious actor activity na naobserbahan sa network ng organisasyon.



Detalyadong timeline

Hulyo: Nagtatag ang mga actor ng paunang koneksyon sa front page ng isang custom web application (T1190) na binuo para sa organisasyon (mula ngayon ay tutukuyin bilang 'web application' o '*webapp*') sa pamamagitan ng koneksyon ng transport layer security (TLS) (T1102). Walang ibang kapansin-pansing aktibidad ang naobserbahan.

Hulyo: Sinimulan ng mga actor ang pag-enumerate sa website ng web application na naghahanap ng mga endpoint[2] upang higit pang mag-imbestiga.

Hulyo: Ang mga actor ay tumutok sa mga pagtatangka na samantalahin ang isang partikular na endpoint.

Hulyo: Ang mga actor ay matagumpay na nakapag-`POST` sa web server, marahil sa pamamagitan ng isang web shell na inilagay sa ibang page. Ang pangalawang IP, na malamang na ginagamit ng parehong mga actor, ay nagsisimula ring mag-post sa parehong URL. Ang mga actor ay lumikha at sumubok ng ilang malamang na mga web shell.

Ang eksaktong paraan ng pagsasamantala ay hindi pa nalalaman, ngunit malinaw na ang partikular na endpoint ay na-target upang lumikha ng mga file sa *<webapp>2*-`ext`.

Naniniwala ang ACSC ng ASD na ang dalawang koneksyon sa IP address ay bahagi ng parehong intrusion (panghihimasok) dahil sa kanilang ibinahaging interes at mga paunang koneksyon na nagaganap ilang minuto ang pagitan.

Hulyo: Ang grupo ay patuloy na nagsasagawa ng host enumeration, naghahanap ng mga pagkakataon sa pagtaas ng pribilehiyo (privileged escalation), at nagde-deploy ng ibang web shell. Nag-log in ang mga actor sa web application gamit ang mga nakompromisong kredensyal para sa *<firstname.surname>@<domain ng organisasyon>*.

Mukhang hindi matagumpay na nakamit ng aktibidad ng mga actor ang pagtaas ng pribilehiyo (privilege escalation) sa *<webapp>2*-`ext`. Sa halip, lumipat ang mga actor sa aktibidad na network-based.

Hulyo: Sinusubukan ng actor ang mga nakompromisong kredensyal para sa isang service account[3] na malamang na nakita nitong naka-hardcode sa mga binary na naa-access sa loob.

Hulyo: Ini-deploy ng mga actor ang open-source na tool Secure Socket Funnelling, na ginamit upang kumonekta sa malicious infrastructure. Ang koneksyon na ito ay ginagamit upang i-tunnel ang trapiko mula sa mga attack machine ng actor patungo sa mga internal network ng organisasyon, na ang mga pangalan ng machine ay nakalantad sa mga event log habang sinusubukan nilang gamitin ang mga kredensyal para sa service account.

Agosto: Nakikita ang mga actor na nagsasagawa ng limitadong dami ng aktibidad, kabilang ang hindi magawang pagtatag ng mga koneksyon na kinasasangkutan ng service account.

Agosto: Ang mga actor ay gumaganap ng makabuluhang network at Active Directory enumeration. Ang ibang nakompromisong account ay kasunod na ginagamit upang mag-mount ng mga share[4] sa mga Windows machine sa loob ng DMZ, na nagpapagana ng matagumpay na pag-exfiltrate ng data.

Ito ay tila oportunistang paggamit ng isang ninakaw na kredensyal sa mga mountable machine sa DMZ. Hinarangan ng mga firewall ang actor sa pag-target sa internal network na may katulad na aktibidad.

Agosto – Setyembre: Muling itinatag ng SSF tool ang koneksyon sa isang malicious IP. Ang grupo ay hindi naobserbahang nagsasagawa ng anumang karagdagang aktibidad hanggang sa ma-block ang kanilang pag-access.

Setyembre: Bina-block ng organisasyon ang malicious IP sa pamamagitan ng pag-denylist nito sa kanilang mga firewall.

2 Sa kontekstong ito, ang isang endpoint ay isang function ng web application

3 Ang mga service account ay hindi nakatali sa mga individual user, kundi sa mga serbisyo. Sa isang Microsoft corporate domain, mayroong iba't ibang uri ng mga account.

4Ang pag-mount ng shares ay ang proseso ng paggawa ng mga file sa istraktura ng file system na naa-access ng isang user o user group.

Mga taktika at mga teknik ng actor

Ang balangkas ng MITER ATT&CK ay isang dokumentadong koleksyon ng mga taktika at teknik na ginagamit ng mga threat actor sa cyberspace. Ang balangkas ay nilikha ng US not-for-profit na The MITRE Corporation at gumaganap bilang isang karaniwang pandaigdigang wika sa pag-uugali ng threat actor.

Tinatasa ng ACSC ng ASD ang mga sumusunod na teknik at taktika kung may kaugnayan sa malicious activity ng actor:

Pagmamanman (Reconnaissance)

T1594 – Maghanap sa mga Website na Pag-aari ng Biktima

Nag-enumerate ang actor ng website ng custom web application upang matukoy ang mga pagkakataon para maka-access sa network.

Pangunang Pag-access (Initial Access)

T1190 – Samantalahin ang Public-Facing Application (tungkol sa pagsasamantala sa custom web application)

T1078.002 – Mga Balidong Account: Mga Domain Account (tungkol sa pag-log on na may nakompromisong mga kredensyal)

Ang pagsasamantala sa mga custom na web application na nakalantad sa internet ay nagsilbing paunang punto ng pag-access para sa actor. Nang lumaon, nagamit ng actor ang mga kredensyal na kinompromiso nito upang palawakin ang kanilang access sa network.

Pag-execute

T1059 – Command and Scripting Interpreter (tungkol sa pag-execute ng command sa pamamagitan ng web shell)

T1072 – Mga Software Deployment Tool (tungkol sa actor na gumagamit ng open-source tool Secure Socket Funneling (SSF) upang kumonekta sa IP)

Persistence

T1505.003 – Bahagi ng Server Software: Web Shell (tungkol sa paggamit ng web shell at SSF upang magtatag ng access)

Pag-access sa Kredensyal

T1552.001 – Mga kredensyal mula sa mga Password Store (tungkol sa mga password file na nauugnay sa building management system (BMS))

T1558.003 – Magnakaw o Magpeke ng mga Kerberos Ticket: Kerberoasting (tungkol sa pag-atake upang makakuha ng mga kredensyal sa network)

Lateral Movement

T1021.002 – Mga Remote na Serbisyo: Mga SMB Shares (tungkol sa actor na nag-mount ng mga SMB shares mula sa maraming device)

Koleksyon

T1213 – Data mula sa mga Information Repository (tungkol sa mga manwal/dokumentasyon na matatagpuan sa BMS server)

Exfiltration

T1041 – Exfiltration Over C2 Channel (tungkol sa data exfiltration ng actor mula sa Active Directory at mounting shares)

Case study 2

Ang report na ito ay hindi nagpapakilala upang paganahin ang mas malawak na pagpapakalat. Ang naapektuhang organisasyon ay tutukuyin mula ngayon bilang 'ang organisasyon'. Inalis ang ilang partikular na detalye upang protektahan ang pagkakakilanlan ng biktima at mga pamamaraan ng pagtugon sa insidente (incident response) ng ACSC ng ASD.

Pang-ehekutibong buod (Executive summary)

Ang report na ito ay nagdedetalye ng mga natuklasan ng pagsisiyasat ng ACSC ng ASD sa matagumpay na kompromiso ng network ng organisasyon noong Abril 2022. Ibinigay ang report ng pagsisiyasat na ito sa organisasyon upang magbuod ng naobserbahang malicious activity at magbalangkas ng mga rekomendasyon sa remediation. Ang mga natuklasan ay nagpapahiwatig na ang kompromiso ay isinagawa ng APT40.

Noong Mayo 2022, inabisuhan ng ACSC ng ASD ang isang organisasyon ng pinaghihinalaang malicious activity na nakakaapekto sa network ng organisasyon mula noong Abril 2022. Kasunod nito, ipinaalam ng organisasyon sa ACSC ng ASD na nakadiskubre sila ng malicious software sa isang internet-facing server na nagbigay ng login portal para sa corporate remote access solution ng organisasyon. Gumamit ang server na ito ng remote access login at identity management product at tatawagin sa report na ito bilang 'ang nakompromisong appliance'. Ang report na ito ay nagdedetalye ng mga natuklasan sa pagsisiyasat at payo sa remediation na binuo para sa organisasyon bilang tugon sa pagsisiyasat na isinagawa ng ACSC ng ASD.

Ipinahiwatig ng ebidensya na ang bahagi ng network ng organisasyon ay nakompromiso ng (mga) malicious cyber actor sa pamamagitan ng remote access login portal ng organisasyon mula pa noong Abril 2022. Ang server na ito ay maaaring nakompromiso ng maraming actor, at malamang na naapektuhan ng isang kahinaan sa remote code execution (RCE) na malawakang naisapubliko sa panahon ng kompromiso.

Ang aktibidad ng key actor na naobserbahan ng ACSC ng ASD ay kinabibilangan ng:

- host enumeration, na nagbibigay-daan sa actor na bumuo ng sarili nitong mapa ng network;
- pagsasamantala ng mga internet-facing application at paggamit ng web shell, na nagbibigay sa actor ng pangunang pagtuntong (foothold) sa network at kakayahang mag-execute mga command;
- pagsasamantala ng mga kahinaan ng software upang magtaas ng mga pribilehiyo (escalate privileges); at
- koleksyon ng kredensyal upang paganahin ang lateral movement

Natuklasan ng ACSC ng ASD na isang malicious actor ang nag-exfiltrate ng ilang daang natatanging username at password na pares sa nakompromisong appliance noong Abril 2022, pati na rin ang ilang mga multi-factor na authentication code at teknikal na artefact na nauugnay sa mga remote access session. Sa pagsusuri ng organisasyon, napag-alamang lehitimo ang mga password. Tinatasa ng ACSC ng ASD na maaaring nakolekta ang actor ng mga teknikal na artifact na ito upang i-hijack o lumikha ng remote login session bilang isang lehitimong user, at i-access ang internal corporate network ng organisasyon gamit ang isang lehitimong user account.

Mga natuklasan sa pagsisiyasat

Buod ng pagsisiyasat

Ang ACSC ng ASD ay nagpasiya na ang actor ay nagkompromiso ng (mga) appliance na nagbibigay ng remote login session para sa mga kawani ng organisasyon at ginamit ang kompromiso na ito upang subukang magsagawa ng karagdagang aktibidad. Ang mga appliance na ito ay binubuo ng tatlong load-balanced host kung saan nakita ang pinakamaagang ebidensya ng kompromiso. Isinara ng organisasyon ang dalawa sa tatlong load-balanced host ilang sandali matapos ang unang kompromiso. Bilang resulta, naganap ang lahat ng kasunod na aktibidad sa iisang host. Ang iba pang mga server na nauugnay sa nakompromisong appliance ay na-load-balanced din sa katulad na paraan. Para madaling mabasa, ang lahat ng nakompromisong mga appliance ay tinutukoy sa karamihan ng report na ito bilang isang 'iisang appliance'.

Ang actor ay pinaniniwalaang gumamit ng mga kilalang kahinaan sa publiko para mag-deploy ng mga web shell sa nakompromisong appliance mula Abril 2022. Ang mga threat actor mula sa grupo ay sinuri na nakakuha ng mga naitaas na pribilehiyo (escalated privilege) sa appliance. Hindi matukoy ng ACSC ng ASD ang buong lawak ng aktibidad dahil sa kakulangan ng kakayahang mag-log. Gayunpaman, ang ebidensya sa device ay nagpapahiwatig na nakamit ng isang actor ang sumusunod:

- Ang koleksyon ng ilang daang tunay na pares ng username at password; at
- Ang koleksyon ng mga teknikal na artefact na maaaring nagbigay-daan sa isang malicious actor na ma-access ang isang virtual desktop infrastructure (VDI) session bilang isang lehitimong user.

Tinatasa ng ACSC ng ASD na hinahangad ng actor na palawakin pa ang kompromiso ng network ng organisasyon. Ang mga artefact na na-exfiltrate ng actor ay maaaring nagbigay-daan sa kanila na i-hijack o simulan ang mga virtual desktop session bilang isang lehitimong user, posibleng bilang isang user na kanilang pinili, kabilang ang mga administrator. Maaaring ginamit ng actor ang access vector na ito upang higit pang ikompromiso ang mga serbisyo ng organisasyon upang makamit ang persistence at iba pang mga layunin.

Ang ibang mga appliance ng organisasyon sa loob ng pinapamahalaang kapaligiran ng hosting provider ay hindi nagpakita ng ebidensya ng kompromiso.

Access

Ang host na may nakompromisong appliance ay nagbigay ng authentication sa pamamagitan ng Active Directory at isang webserver, para sa mga user na kumokonekta sa mga VDI session (T1021.001).

Lokasyon	Mga hostname ng nakompromisong appliance (load-balanced)
Datacentre 1	HOST1, HOST2, HOST3

Kasama rin sa imprastraktura ng appliance ang mga access gateway host na nagbibigay ng tunnel sa VDI para sa user, sa sandaling magkaroon sila ng authentication token na nabuo at na-download mula sa appliance.

Walang katibayan ng kompromiso ng alinman sa mga host na ito. Gayunpaman, ang mga access gateway hosts log ay nagpakita ng katibayan ng mga makabuluhang pakikipag-ugnayan sa mga kilalang malicious IP address. Malamang na ito ay sumasalamin sa aktibidad na naganap sa host na ito, o mga network connection sa imprastraktura ng threat actor na nakarating sa host na ito. Ang katangian ng aktibidad na ito ay hindi matukoy gamit ang magagamit na ebidensya ngunit nagpapahiwatig na ang grupo ay naghangad na kumilos laterally sa network ng organisasyon (TA0008).

Mga internal host

Ang ACSC ng ASD ay nag-imbestiga ng limitadong data mula sa network segment ng internal organisation. Ang pagtatangka o matagumpay na malicious activity na kilalang nakaapekto sa network segment ng internal organisation ay kinabibilangan ng pag-access ng actor sa mga artefact na nauugnay sa VDI, ang scraping ng internal na SQL server (T1505.001), at hindi maipaliwanag na trapikong naobserbahang nagmumula sa mga kilalang mga malicious IP address sa pamamagitan ng mga access gateway appliance (TA0011).

Gamit ang kanilang access sa nakompromisong appliance, nakolekta ng grupo ang mga tunay na username, password (T1003), at mga MFA token value (T1111). Nakolekta din ng grupo ang mga JSON Web Token (JWTs) (T1528), na isang authentication artefact na ginamit upang lumikha ng mga virtual desktop login session. Maaaring nagamit ng actor ang mga ito upang lumikha o mag-hijack ng mga virtual desktop session

(T1563.002) at ma-access ang network segment ng internal organisation bilang isang lehitimong user (T1078).

Gumamit din ang actor ng access sa nakompromisong appliance para i-scrape ang isang SQL server (T1505.001), na nasa internal network ng organisasyon. Malamang na may access ang actor sa data na ito.

Ang ebidensyang makukuha mula sa access gateway appliance ay nagpakita na ang trapiko sa network ay naganap sa pamamagitan o sa device na ito mula sa mga kilalang malicious IP address. Gaya ng inilarawan sa itaas, maaaring ipahiwatig nito na naapektuhan o ginamit ng mga malicious cyber actor ang device na ito, na posibleng mag-pivot sa internal network.

Timeline ng pagsisiyasat

Ang listahan sa ibaba ay nagbibigay ng timeline ng mga pangunahing aktibidad na natuklasan sa panahon ng pagsisiyasat.

Oras	Kaganapan (Event)
Abril 2022	Ang mga kilalang malicious IP address ay nakikipag-ugnayan sa host ng access gateway HOST7. Ang katangian ng mga pakikipag-ugnayan ay hindi matukoy.
Abril 2022	Lahat ng mga host, HOST1, HOST2 at HOST3, ay nakompromiso ng isang malicious actor o mga actor, at ang mga web shell ay inilagay sa mga host. Isang log file ang nilikha o binago sa HOST2. Ang file na ito ay naglalaman ng kredensyal na materyal na malamang na nakuha ng isang malicious actor. Ang mga /etc/security/opasswd at /etc/shadow file ay binago sa HOST1 at HOST3, na nagpapahiwatig na ang mga password ay binago. Ang ebidensyang available sa HOST1 ay nagmumungkahi na ang password para sa user na 'sshuser' ay binago.
Abril 2022	Ang HOST2 ay isinara ng organisasyon. Ang mga karagdagang web shell (T1505.003) ay nilikha sa HOST1 at HOST3. Nakaranas ang HOST1 ng mga pagtatangka ng SSH brute force mula sa HOST3. Isang log file ang binago (T1070) sa HOST3. Ang file na ito ay naglalaman ng kredensyal na materyal (T1078) na malamang na nakuha ng isang malicious actor. Ang mga JWT ay nakuha (T1528) at na-output sa isang file sa HOST3. Ang HOST3 ay isinara ng organisasyon. Ang lahat ng aktibidad pagkatapos ng oras na ito ay nangyayari sa HOST1.
Abril 2022	Ang mga karagdagang web shell ay nilikha sa HOST1 (T1505.003). Ang mga JWT ay nakuha at na-output sa isang file sa HOST1.
Abril 2022	Ang mga karagdagang web shell ay nilikha sa HOST1 (T1505.003), at isang kilalang malicious IP address ay nakikipag-ugnayan sa host (TA0011). Ang isang kilalang malicious IP address ay nakikipag-ugnayan sa host ng access gateway HOST7.
Mayo 2022	Nakipag-ugnayan ang isang kilalang malicious IP address sa access gateway host HOST7 (TA0011). Ang isang authentication event para sa isang user ay na-link sa isang kilalang malicious IP address sa mga log sa HOST1. Isang karagdagang web shell ang nilikha sa host na ito (T1505.003).
Mayo 2022	Ang isang script sa HOST1 ay binago ng isang actor (T1543). Naglalaman ang script na ito ng functionality na maaaring mag-scrape ng data mula sa internal SQL server.
Mayo 2022	Isang karagdagang log file sa HOST1 ang huling binago (T1070). Ang file na ito ay naglalaman ng mga pares ng username at password para sa network ng organisasyon, na pinaniniwalaang lehitimo (T1078).
Mayo 2022	Isang karagdagang log file ang huling binago (T1070). Ang file na ito ay naglalaman ng mga JWT na nakolekta mula sa HOST1.
Mayo 2022	Ang mga karagdagang web shell ay nilikha sa HOST1 (T1505.003). Sa petsang ito, inireport ng organisasyon sa ACSC ng ASD ang pagkatuklas ng isang web shell na may petsa ng paglikha noong Abril 2022
Mayo 2022	Ang ilang mga script ay nilikha sa HOST1, kabilang ang isang pinangalanang Log4jHotPatch.jar.
Mayo 2022	Ang iptables-save na command ay ginamit upang magdagdag ng dalawang open port sa access gateway host. Ang mga port ay 9998 at 9999 (T1572).

Mga taktika at teknik ng actor

Naka-highlight sa ibaba ang ilang mga taktika at teknik na natukoy sa panahon ng pagsisiyasat.

Pangunang Pag-access (Initial Access)

T1190 Pagsasamantala sa mga application na nakaharap sa publiko (public facing application)

Malamang na sinamantala ng grupo ang RCE, pagtaas ng pribilehiyo (privilege escalation), at pag-authenticate ng bypass na mga kahinaan sa remote access login at identity management product para makakuha ng pangunang pag-access sa network.

Ang pamamaraan sa pangunang pag-access na ito ay itinuturing na pinaka-malamang na dahil sa mga sumusunod:

- Ang server ay mahina sa mga CVE na ito noong panahong iyon;
- Mga pagtatangkang samantalahin ang mga kahinaang ito mula sa imprastraktura ng kilalang actor; at
- Ang unang kilalang internal malicious activity ay naganap ilang sandali matapos ang mga pagtatangkang magsamantala.

Pag-execute

T1059.004 Command at Scripting Interpreter: Unix Shell

Matagumpay na nagamit ng grupo ang mga kahinaang nabanggit sa itaas na maaaring nakapagpatakbo ng mga command sa isang Unix shell na available sa apektadong appliance. Ang mga kumpletong detalye ng mga command na pinapatakbo ng mga actor ay hindi maibibigay dahil hindi sila na-log ng appliance.

Persistence

T1505.003 Bahagi ng Software ng Server (Server Software Component): Web Shell

Nag-deploy ang mga actor ng ilang mga web shell sa apektadong appliance. Posibleng maraming natatanging actor ang nag-deploy ng mga web shell, ngunit mas maliit na bilang lamang ng mga actor ang nagsagawa ng aktibidad gamit ang mga web shell na ito. Nagbibigay-daan ang mga web shell para sa arbitrary command execution ng actor sa mga nakompromisong appliance.

Pagtaas ng pribilehiyo (privilege escalation)

T1068 Pagsasamantala para sa Pagtaas ng Pribilehiyo (Privilege Escalation)

Ang magagamit na ebidensya ay hindi naglalarawan sa antas ng pribilehiyo na nakamit ng mga actor. Gayunpaman, gamit ang mga web shell, maaaring makamit ng mga actor ang isang antas ng pribilehiyo na maihahambing sa web server sa nakompromisong appliance. Ang mga kahinaan na pinaniniwalaang naroroon sa nakompromisong appliance ay magbibigay-daan sa mga actor na makamit ang mga matatag na pribilehiyo (root privileges).

Pag-access ng kredensyal

T1056.003 Input Capture: Web Portal Capture

Ang ebidensya sa nakompromisong appliance ay nagpakita na nakuha ng actor ang ilang daang pares ng username-password, sa malinaw na text, na pinaniniwalaang lehitimo. Malamang na ang mga ito ay nakuha gamit ang ilang pagbabago sa genuine authentication process na nag-a-output ng mga kredensyal sa isang file.

T1111 Multi-Factor Authentication Interception

Nakuha rin ng actor ang value ng mga MFA token na tumutugma sa mga lehitimong login. Ang mga ito ay malamang na nakuha sa pamamagitan ng pagbabago sa genuine authentication process upang i-output ang mga halagang ito sa isang file. Walang katibayan ng kompromiso ng 'secret server' na nag-iimbak ng mga natatanging value para sa seguridad ng mga MFA token.

T1040 Network Sniffing

Pinaniniwalaang nakuha ng actor ang mga JWT sa pamamagitan ng pag-capture ng trapiko ng HTTP sa nakompromisong appliance. May ebidensya na ang utility tcpdump ay na-execute sa nakompromisong appliance, na maaaring paraan kung paano nakuha ng actor ang mga JWT na ito.

T1539 Steal Web Session Cookie

Gaya ng inilarawan sa itaas, nakunan ng actor ang mga JWT, na kahalintulad ng web session cookies. Ang mga ito ay maaaring ginamit muli ng actor upang magtatag ng karagdagang pag-access.

Pagtuklas

T1046 Pagtuklas sa Serbisyo sa Network

May katibayan na ang network scanning utility nmap ay na-execute sa nakompromisong appliance upang i-scan ang iba pang mga appliances sa parehong network segment. Ito ay malamang na ginamit ng actor upang tumuklas ng iba pang maaabot na mga serbisyo ng network na maaaring mga pagkakataon para sa lateral movement.

Koleksyon

Ang magagamit na ebidensya ay hindi naghahayag kung paano nakolekta ng mga actor ang data o kung ano mismo ang nakolekta mula sa nakompromisong appliance o mula sa iba pang mga system. Gayunpaman, malamang na may access ang mga actor sa lahat ng file sa nakompromisong appliance, kabilang ang mga nakuhang kredensyal (T1003), mga MFA token value (T1111), at mga JWT na inilarawan sa itaas.

Command and control

T1071.001 Application Layer Protocol: Mga Protocol sa Web

Gumamit ang mga actor ng mga web shell para sa command and control. Ang mga command sa web shell ay ipinasa sa HTTPS gamit ang umiiral na web server sa appliance (T1572).

T1001.003 Data Obfuscation: Protocol Impersonation

Gumamit ang mga actor ng mga nakompromisong device bilang punto ng paglulunsad ng mga pag-atake na idinisenyo upang makasabay sa lehitimong trapiko.

Mga rekomendasyon sa pagtuklas at mitigasyon

Mahigpit na inirerekomenda ng ACSC ng ASD ang pagpapatupad ng ASD Essential Eight na mga Kontrol at nauugnay na Mga Istratehiya sa Pagpapagaan (Mitigasyon) ng mga Insidente sa Cyber Security. Nasa ibaba ang mga rekomendasyon para sa mga aksyon sa seguridad ng network na dapat gawin upang matukoy at maiwasan ang mga panghihimasok ng APT40, na sinusundan ng mga partikular na mitigasyon para sa apat na mga pangunahing TTP na nakabuod sa Talahanayan 1.

Pagtuklas

Ang ilan sa mga file na tinukoy sa itaas ay ibinaba sa mga lokasyon gaya ng C:\Users\Public* at C:\Windows\Temp*. Ang mga lokasyong ito ay maaaring madaling mga lugar para sa pagsusulat ng data dahil karaniwan itong world writable, iyon ay, lahat ng user account na nakarehistro sa Windows ay may access sa mga directory na ito at sa kanilang mga subdirectory. Kadalasan, maaaring ma-access ng sinumang user ang mga file na ito, na nagbibigay-daan sa mga pagkakataon para sa lateral movement, pag-iwas sa depensa, pag-execute ng mababang pribilehiyo at paghahanda para sa exfiltration.

Ang mga sumusunod na Sigma rule ay naghahanap ng pag-execute mula sa mga kahina-hinalang lokasyon bilang isang tagapagpahiwatig ng maanomalyang aktibidad. Sa lahat ng pagkakataon, kinakailangan ang kasunod na pagsisiyasat upang kumpirmahin ang malicious activity at kung sino ang gumagawa nito (attribution).

Pamagat: World Writable Execution - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Paglalarawan: Tuklasin ang proseso ng pag-execute mula sa C:\Windows\Temp.

Background:

Ang panuntunang ito ay partikular na naghahanap ng pag-execute sa labas ng C:\Windows\Temp*. Ang Temp ay mas malawak na ginagamit ng mga benign application at sa gayon ay isang lower confidence malicious indicator kaysa sa pag-execute ng iba pang mga world writable subdirectory sa C:\Windows.

Ang pag-alis ng mga application na na-execute ng mga user ng SYSTEM o NETWORK SERVICE ay lubos na nakakabawas sa dami ng benign activity na pinili ng rule na ito.

Nangangahulugan ito na maaaring makaligtaan ng rule ang mga malicious execution sa mas mataas na antas ng pribilehiyo ngunit inirerekomendang gumamit ng iba pang mga rule upang matukoy kung sinusubukan ng isang user na itaas ang mga pribilehiyo sa SYSTEM.

Pagsisiyasat:

1. Suriin ang impormasyong direktang nauugnay sa file execution na ito, tulad ng konteksto ng user, antas ng integridad ng pag-execute, agarang follow-on na aktibidad at mga larawang na-load ng file.
2. Siyasatin ang kontekstwal na proseso, network, file at iba pang sumusuportang data sa host upang makatulong na gumawa ng pagtatasa kung ang aktibidad ay malicious.
3. Kung kinakailangan, subukang mangolekta ng isang kopya ng file para sa reverse engineering upang matukoy kung ito ay lehitimo.

Mga sanggunian:

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

May-akda: ACSC ng ASD

Petsa:2024-06-19

Status: experimental

Mga tag:

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

Log Source:

```
kategorya: process_creation
produkto: windows
```

Pagtuklas:

```
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:
    User:
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

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

kundisyon: temp at hindi (common_temp_path o system_user o dismhost o known_parent)

Mga false positive:

- Na-obserbahan ang mga Allowlist auditing application na nagpapatakbo ng mga executable mula sa Temp.
- Lehitimong maglalaman ang Temp ng isang hanay ng mga setup application at launcher, kaya mabuting isaalang-alang kung gaano kalawak ang gawi na ito sa isang sinusubaybayang network (at kung ito ay maaaring i-allowlist o hindi) bago paganahin ang rule na ito.

Antas: mababa

Pamagat: World Writable Execution - Non-Temp System Subdirectory

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

Paglalarawan Tuklasin ang pag-execute ng proseso mula sa isang world writable na lokasyon sa isang subdirectory ng Windows OS install location.

Background:

Ang rule na ito ay partikular na naghahanap ng buod mula sa mga world writable directory sa loob ng C:\ at partikular sa C:\Windows*, maliban sa C:\Windows\Temp (na mas malawak na ginagamit ng mga benign application at sa gayon ay isang lower confidence malicious indicator).

Ang mga folder ng AppData ay hindi kasama kung ang isang file ay pinapatakbo bilang SYSTEM - ito ay isang benign na paraan kung saan maraming mga temporary application file ang in-execute.

Pagkatapos makumpleto ang isang paunang network baseline at tukuyin ang mga kilalang benign execution mula sa mga lokasyong ito, ang rule na ito ay dapat bihirang gumana.

Pagsisiyasat:

1. Suriin ang impormasyong direktang nauugnay sa file execution na ito, tulad ng konteksto ng user, antas ng integridad ng pag-execute, agarang follow-on na aktibidad at mga larawang na-load ng file.
2. Siyasatin ang kontekstwal na proseso, network, file at iba pang sumusuportang data sa host upang makatulong sa pagtatasa kung ang aktibidad ay malicious.
3. Kung kinakailangan, subukang mangolekta ng isang kopya ng file para sa reverse engineering upang matukoy kung ito ay lehitimo.

Mga sanggunian:

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

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

May-akda: ACSC ng ASD

Petsa: 2024/06/19

Status: experimental

Mga tag:

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

Log source:

kategorya: process_creation

produkto: windows

Pagtuklas:

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:

Image|contains: '\\AppData\\'
User: 'SYSTEM'

kundisyon: writeable_path at hindi appdata

Mga false positive:

Ang mga Allowlist auditing application ay naobserbahang nagpapatakbo ng mga executable mula sa mga directory na ito.

Posible na ang mga script at mga administrative tool na ginagamit sa (mga) sinusubaybayang kapaligiran ay maaaring matatagpuan sa isa sa mga directory na ito at dapat na ayusin nang paisa-isa (case-by-case).

Antas: mataas

Pamagat: World Writable Execution – Mga User

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

Paglalarawan Tuklasin ang proseso ng pag-execute mula sa C:\Users\Public* at iba pang mga world writeable folder sa loob ng mga User.

Background:

Ang mga AppData folder ay hindi kasama kung ang isang file ay pinapatakbo bilang SYSTEM - ito ay isang benign na paraan kung saan maraming mga temporary application file ang ine-execute.

Pagsisiyasat:

1. Suriin ang impormasyong direktang nauugnay sa file execution na ito, tulad ng konteksto ng user, antas ng integridad ng pag-execute, agarang follow-on na aktibidad at mga larawang na-load ng file.
2. Siyasatin ang kontekstwal na proseso, network, file at iba pang sumusuportang data sa host upang makatulong sa pagtatasa kung ang aktibidad ay malicious.
3. Kung kinakailangan, subukang mangolekta ng isang kopya ng file para sa reverse engineering upang matukoy kung ito ay lehitimo.

Mga sanggunian:

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

May-akda: ASD's ACSC

Petsa: 2024-06-19

Status: experimental

Mga Tag:

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

Log source:

kategorya: process_creation
produkto: windows

Pagtuklas:

mga user:

Image|contains:

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

appdata:

Image|contains: '\\AppData\\'

User: 'SYSTEM'

kundisyon: mga user at hindi appdata

Mga false positive:

- Posible na ang mga script at mga administrative tool na ginagamit sa (mga) sinusubaybayang kapaligiran ay maaaring matatagpuan sa Pampubliko o isang subdirectory at dapat harapin nang paisa-isa (case-by-case).

Antas: medium

Mga mitigasyon

Pag-log

Sa panahon ng mga pagsisiyasat ng ACSC ng ASD, ang isang karaniwang isyu na nagpapababa sa bisa at bilis ng mga pagsisikap sa pagsisiyasat ay ang kakulangan ng komprehensibo at impormasyon sa historical logging sa maraming area kabilang ang mga request log ng web server, mga event log at internet proxy log ng Windows.

Inirerekomenda ng ACSC ng ASD na suriin at ipatupad ang kanilang patnubay sa Windows Event Logging and Forwarding kasama ang mga configuration file at script sa Windows Event Logging Repository at ang Information Security Manual's Mga Alituntunin para sa System Monitoring, upang maisama ang mga pag-sentro ng mga log at pagtatabi ng mga log nang sapat na panahon.

Pamamahala ng patch

Agad na i-patch ang lahat ng nakalantad sa internet na device at serbisyo, kabilang ang mga web server, web application, at remote access gateway. Isaalang-alang ang pagpapatupad ng isang sentralisadong sistema ng pamamahala ng patch upang i-automate at mapabilis ang proseso. Irekomenda ang pagpapatupad ng Mga Alituntunin para sa Pamamahala ng System ng ISM, partikular, ang mga kontrol ng System Patching kung saan naaangkop.

Karamihan sa mga pagsasamantalang ginamit ng actor ay kilala sa publiko at may magagamit na mga patch o mitigasyon. Dapat tiyakin ng mga organisasyon na ang mga security patch o mitigasyon ay inilalapat sa internet facing na imprastraktura sa loob ng 48 oras, at kung posible, gamitin ang mga pinakabagong bersyon ng software at mga operating system.

Pagbabaha-bahagi ng network (Network segmentation)

Maaaring pahirapan ng network segmentation ang mga kalaban na mahanap at ma-access ang mga sensitibong data ng isang organisasyon. I-segment ang mga network upang limitahan o harangan ang lateral movement sa pamamagitan ng pagpigil sa trapiko sa pagitan ng mga computer maliban kung iniuutos. Ang mga mahahalagang server tulad ng Active Directory at iba pang mga authentication server ay dapat lamang ipamahala mula sa limitadong bilang ng mga intermediary server o 'jump server'. Ang mga server na ito ay dapat masusing subaybayan, secured at limitahan kung aling mga user at device ang makakakonekta sa kanila.

Anuman ang mga pagkakataong natukoy kung saan pinipigilan ang lateral movement, ang karagdagang network segmentation ay maaaring higit pang limitahin ang dami ng data na na-access at nakuha ng mga actor.

Mga karagdagang mitigasyon

Inirerekomenda din ng mga ahensyang may-akda ang mga sumusunod na mitigasyon upang labanan ang APT40 at ang paggamit ng mga iba ng TTP sa ibaba.

- I-disable ang hindi nagamit o hindi kinakailangang mga serbisyo ng network, mga port at protocol.
- Gumamit ng maayos na mga Web application firewall (WAFs) upang protektahan ang mga web server at application.
- Magpatupad ng pinakamaliit na pribilehiyo upang limitahan ang pag-access sa mga server, file server, at iba pang mapagkukunan.
- Gumamit ng multi-factor authentication (MFA) at mga managed service account para mas mahirap mabuksan at magamit muli ang mga kredensyal. Dapat ilapat ang MFA sa lahat ng mga remote access service na naa-access sa internet, kabilang ang:
  - Web at cloud-based na email
  - Mga collaboration platform
  - Mga virtual na pribadong network connection
  - Mga serbisyong remote desktop
- Palitan ang mga malapit nang mawalan ng bisang kagamitan (end-of-life equipment).

Talahanayan 1. Mga Istratehiya/Mga Teknik sa Mitigasyon

TTP	Mahahalagang Walong Istratehiya ng Mitigasyon	Mga Kontrol ng ISM
Pangunang Pag-access T1190 Pagsasamantala sa Public-Facing Application	Mga patch application Mga patch operating system Multi-factor authentication Application control	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Pag-execute T1059 Command at Scripting Interpreter	Application control Limitahan ang mga Microsoft Office macro Limitahan ang mga pribilehiyong pang-administratibo	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Persistence T1505.003 Bahagi ng Server Software: Web Shell	Application Control Limitahan ang mga pribilehiyong pang-administratibo	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Pangunang Pag-access / Pagtaas ng Pribilehiyo (Privilege Escalation) / Persistence T1078 Mga Balidong Account	Mga patch operating system Multi-factor authentication Limitahan ang mga pribilehiyong pang-administratibo Application control User application hardening	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

Para sa karagdagang pangkalahatang payo sa pagtuklas at mitigasyon, mangyaring kumonsulta sa mga seksyong Mga Mitigasyon at Pagtuklas sa web page ng teknik ng MITER ATT&CK para sa bawat isa sa mga teknik na tinukoy sa buod ng MITER ATT&CK sa dulo ng pabatid ito.

Pagtatatwa

Ang impormasyon sa report na ito ay ibinibigay "as is" para sa mga layuning pang-impormasyon lamang. Ang mga ahensyang may-akda ay hindi nag-eendorso ng anumang komersyal na ahensya, produkto, kumpanya, o serbisyo, kabilang ang anumang mga ahensya, produkto, o serbisyong naka-link sa nilalaman ng dokumentong ito. Anumang pagtukoy sa mga partikular na komersyal na ahensya, produkto, proseso, o serbisyo sa pamamagitan ng marka ng serbisyo (service mark), trademark, tagagawa, o ano man, ay hindi bumubuo o nagpapahiwatig ng pag-endorso, rekomendasyon, o pagpapabor ng mga ahensyang may-akda.

Ang dokumentong ito ay may markang TLP:CLEAR. Ang pagsisiwalat ay hindi limitado. Maaaring gumamit ang mga source ng TLP:CLEAR kapag ang impormasyon ay may minimal o walang nakikinitang panganib ng maling paggamit, alinsunod sa mga naaangkop na panuntunan at pamamaraan para sa pampublikong pagpapalabas. Alinsunod sa mga batayang panuntunan sa karapatang-sipi (copyright), ang TLP:CLEAR na impormasyon ay maaaring ipamahagi nang walang paghihigpit. Para sa higit pang impormasyon sa Traffic Light Protocol, tingnan ang cisa.gov/tlp

MITER ATT&CK – Makasaysayang APT40 tradecraft ng interes

Reconnaissance (TA0043)	
Maghanap sa mga Website na Pag-aari ng Biktima (T1594)	Ipunin ang Impormasyon sa Pagkakakilanlan ng Biktima: Mga kredensyal (T1589.001)
Aktibong Pag-scan: Pag-scan sa Kahinaan (T1595.002)	Magtipon ng Impormasyon sa Host ng Biktima (T1592)
Mag-search sa mga Bukas na Website/Domain: Mga Search Engine (T1593.002)	Magtipon ng Impormasyon sa Network ng Biktima: Mga Domain Property (T1590.001)
Ipunin ang Impormasyon sa Pagkakakilanlan ng Biktima: Mga Email Address (T1589.002)	

Pag-unlad ng Mapagkukunan (TA0042)	
Kumuha ang Imprastraktura: Mga Domain (T1583.001)	Kunin ang Imprastrasktura (T1583)
Kunin ang Imprastraktura: DNS Server (T1583.002)	Mga Nakompromisong Account (T1586)
Bumuo ng mga Kakayahan: Mga Sertipiko ng Code Signing (T1587.002)	Nakompromisong Imprastraktura (T1584)
Bumuo ng mga Kakayahan: Mga Digital na Sertipiko (T1587.003)	Bumuo ng mga Kakayahan: Malware (T1587.001)
Kumuha ng mga Kakayahan: Mga Sertipiko ng Code Signing (T1588.003)	Magtatag ng mga Account: Mga Cloud Account (T1585.003)
Nakompromisong Imprastraktura: Mga Network Device (T1584.008)	Kumuha ng mga Kakayahan: Mga Digital na Sertipiko (T1588.004)

Pangunang Pag-access (TA0001)	
Mga Balidong Account (T1078)	Phishing (T1566)
Mga Balidong Account: Mga Default na Account (T1078.001)	Phishing: Spearphishing Attachment (T1566.001)
Mga Balidong Account: Mga Domain Account (T1078.002)	Phishing: Link ng Spearphishing (T1566.002)
Mga Panlabas na Malayuang Serbisyo (External Remote Services) (T1133)	Samantalahin ang Public-Facing Application (T1190)
Drive-by Compromise (T1189)	

Pag-execute (TA0002)	
Instrumentasyon ng Pamamahala ng Windows (T1047)	Command at Scripting Interpreter: Python (T1059.006)
Naka-iskedyul na Gawain/Trabaho: At (T1053.002)	Command at Scripting Interpreter: JavaScript (T1059.007)
Naka-iskedyul na Gawain/Trabaho: Naka-iskedyul na Gawain (T1053.005)	Native API (T1106)
Command at Scripting Interpreter (T1059)	Inter-Process Communication (T1559)
Command at Scripting Interpreter: Windows Command Shell (T1059.003)	Mga Serbisyo ng System (System Services): Pag-execute ng Serbisyo (T1569.002)
Command at Scripting Interpreter: PowerShell (T1059.001)	Pagsasamantala para sa Client Execution (T1203)
Command at Scripting Interpreter: Visual Basic (T1059.005)	User Execution: Malicious File (T1204.002)
Command at Scripting Interpreter: Unix Shell (T1059.004)	Command at Scripting Interpreter: Apple Script (T1059.002)
Naka-iskedyul na Gawain/Trabaho: Cron (T1053.003)	Mga Tool sa Pag-deploy ng Software (T1072)

Persistence (TA0003)	
Mga Balidong Account (T1078)	Bahagi ng Server Software: Web Shell (T1505.003)
Office Application Startup: Office Template Macros (T1137.001)	Lumikha o Baguhin ang Proseso ng System: Windows Service (T1543.003)
Naka-iskedyul na Gawain/Trabaho: At (T1053.002)	Boot o Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Naka-iskedyul na Gawain/Trabaho: Naka-iskedyul na Gawain (T1053.005)	Boot o Logon Autostart Execution: Pagbabago ng Shortcut (T1547.009)
Mga Panlabas na Malayuang Serbisyo (External Remote Services) (T1133)	Daloy ng Pag-execute ng Hijack: DLL Search Order Hijacking (T1574.001)
Naka-iskedyul na Gawain/Trabaho: Cron (T1053.003)	Daloy ng Pag-execute ng Hijack: DLL Side-Loading (T1574.002)
Pagmamanipula ng Account (T1098)	Mga Balidong Account: Mga Cloud Account (T1078.004)
Mga Balidong Account: Mga Domain Account (T1078.002)	

Pagtaas ng Pribilehiyo (Privilege Escalation) (TA0004)	
Naka-iskedyul na Gawain/Trabaho: At (T1053.002)	Lumikha o Baguhin ang Proseso ng System: Serbisyo ng Windows (T1543.003)
Naka-iskedyul na Gawain/Trabaho: Naka-iskedyul na Gawain (T1053.005)	Boot o Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Process Injection: Thread Execution Hijacking (T1055.003)	Boot o Logon Autostart Execution: Pagbabago ng Shortcut (T1547.009)
Process Injection: Process Hollowing (T1055.012)	Daloy ng Pag-execute ng Hijack: DLL Search Order Hijacking (T1574.001)

Pagtaas ng Pribilehiyo (Privilege Escalation) (TA0004)	
Mga Balidong Account: Mga Domain Account (T1078.002)	Pagsasamantala para sa Pagtaas ng Pribilehiyo (Privilege Escalation) (T1068)
Pagmamanipula ng Token Access: Pagpapanggap/ Pagnanakaw ng Token (T1134.001)	Na-trigger ng Event na Pag-execute (Event Triggered Execution): Pagbabago sa Configuration ng Unix Shell (T1546.004)
Process Injection: Dynamic-link Library Injection (T1055.001)	Mga Balidong Account: Mga Domain Account (T1078.002)
Mga Balidong Account: Mga Local Account (T1078.003)	

Pag-iwas sa Depensa (TA0005)	
Rootkit (T1014)	Hindi Direktang Pag-execute ng Command (T1202)
Naka-obfuscate na mga File o Impormasyon (T1027)	System Binary Proxy Execution: Mshta (T1218.005)
Naka-obfuscate na mga File o Impormasyon: Software Packing (T1027.002)	System Binary Proxy Execution: Regsvr32 (T1218.010)
Naka-obfuscate na mga File o Impormasyon: Steganography (T1027.003)	Mga Subvert Trust Control: Code Signing (T1553.002)
Naka-obfuscate na mga File o Impormasyon: Mag-compile Pagkatapos ng Paghahatid (T1027.004)	Mga Pagbabago sa mga File at Directory Permission: Mga Pagbabago ng Linux at Mac File at Directory Permission (T1222.002)
Pagbabalatkayo (Masquerading): Itugma ang Lehitimong Pangalan o Lokasyon (T1036.005)	Virtualization/Sandbox Evasion: Mga Pagsusuri ng System (System Checks) (T1497.001)
Process Injection: Thread Execution Hijacking (T1055.003)	Pagbabalatkayo (Masquerading) (T1036)
Pag-load ng Reflective Code (T1620)	Mga Impair Defense: I-disable o Baguhin ang System Firewall (T1562.004)
Process Injection: Process Hollowing (T1055.012)	Itago ang mga Artifact: Mga Nakatagong File at Directory (T1564.001)
Pag-alis ng Tagapagpahiwatig (indicator Removal): Pagtanggal ng File (T1070.004)	Itago ang mga Artifact: Nakatagong Window (T1564.003)
Pag-alis ng Tagapagpahiwatig: Timestomp (T1070.006)	Daloy ng Pag-execute ng Hijack: DLL Search Order Hijacking (T1574.001)
Pag-alis ng Tagapagpahiwatig (Indicator Removal): I-clear ang mga Windows Event Log (T1070.001)	Daloy ng Pag-execute ng Hijack: DLL Side-Loading (T1574.002)
Baguhin ang Registry (T1112)	Web Service (T1102)
I-obfuscate/I-decode ang mga File o Impormasyon (T1140)	Pagbabalatkayo (Masquerading): Masquerade na Gawain o Serbisyo (T1036.004)
Mga Pagpapahina ng Depensa (Impair Defenses) (T1562)	

Pag-access sa Kredensyal (TA0006)	
OS Credential Dumping: LSASS Memory (T1003.001)	Mga Hindi Secure na Kredensyal: Mga Kredensyal sa mga File (T1552.001)
OS Credential Dumping: NTDS (T1003.003)	Brute Force: Paghula ng Password (T1110.001)
Network Sniffing (T1040)	Forced Authentication (T1187)

Pag-access sa Kredensyal (TA0006)	
Mga Kredensyal mula sa mga Password Store: Keychain (T1555.001)	Magnakaw o Magpeke ng mga Kerberos Ticket: Kerberoasting (T1558.003)
Input Capture: Keylogging (T1056.001)	Multi-Factor Authentication Interception (T1111)
Steal Web Session Cookie (T1539)	Steal Application Access Token (T1528)
Pagsasamantala para sa Pag-access ng Kresensyal (T1212)	Brute Force: Pag-crack ng Password (T1110.002)
Input Capture: Pagkuha ng Web Portal (T1056.003)	OS Credential Dumping: DCSync (T1003.006)
Mga Kredensyal mula sa Mga Password Store (T1555)	Mga Kredensyal mula sa Mga Password Store: Mga Kredensyal mula sa Mga Web Browser (T1555.003)

Pagtuklas (TA0007)	
Pagtuklas sa System Service (T1007)	Pagtuklas sa System Information (T1082)
Application Window Discovery (T1010)	Pagtuklas sa Account: Local Account (T1087.001)
Query Registry (T1012)	System Information Discovery, Technique T1082 - Enterprise | MITER ATT&CK®
Pagtuklas sa File at Directory (T1083)	Pagtuklas sa System Time (T1124)
Pagtuklas sa Network Service(T1046)	Pagtuklas sa May-ari/User ng System (T1033)
Pagtuklas sa Remote System (T1018)	Pagtuklas sa Domain Trust (T1482)
Pagtuklas sa Account: Email Account (T1087.003)	Pagtuklas sa Account: Domain Account (T1087.002)
Pagtuklas sa Mga Koneksyon sa Network System (T1049)	Virtualisation/Sandbox Evasion: Mga System Check (T1497.001)
Pagtuklas sa Proseso (T1057)	Pagtuklas sa Software (T1518)
Pagtuklas sa mga Permission Group: Mga Domain Group (T1069.002)	Network Share Discovery, Technique T1135 - Enterprise | MITER ATT&CK®
Pagtuklas sa System Network Configuration: Pagtuklas sa Internet Connection (T1016.001)	

Lateral Movement (TA0008)	
Mga Remote Service: Remote Desktop Protocol (T1021.001)	Mga Remote Service (T1021)
Mga Remote Service: SMB/Windows Admin Shares (T1021.002)	Gumamit ng Alternate Authentication Material: Pass the Ticket (T1550.003)
Mga Remote Service: Windows Remote Management (T1021.006)	Lateral Tool Transfer (T1570)

Koleksyon (TA0009)	
Data mula sa Local System (T1005)	I-archive ang Nakolektang Data: I-archive sa pamamagitan ng Library (T1560.002)
Data mula sa Network Shared Drive (T1039)	Koleksyon ng Email: Remote Email Collection (T1114.002)

Koleksyon (TA0009)	
Input Capture: Keylogging (T1056.001)	Data ng Clipboard (T1115)
Automated Collection (T1119)	Data mula sa mga Information Repository (T1213)
Input Capture: Pagkuha ng Web Portal (T1056.003)	Data Staged: Remote Data Staging (T1074.002)
Data Staged: Local Data Staging (T1074.001)	I-archive ang Nakolektang Data (T1560)
Koleksyon ng Email (T1114)	

Exfiltration (TA0010)	
Exfiltration Sa C2 Channel (T1041)	Exfiltration Sa Alternatibong Protocol: Exfiltration Sa Asymmetric Encrypted Non-C2 Protocol (T1048.002)
Exfiltration Sa Alternatibong Protocol (T1048)	Exfiltration Sa Web Service: Exfiltration Sa Cloud Storage (T1567.002)

Command and Control (TA0011)	
Data Obfuscation: Protocol Impersonation (T1001.003)	Web Service: Dead Drop Resolver (T1102.001)
Karaniwang Ginagamit na Port (T1043)	Web Service: One-way Communication (T1102.003)
Application Layer Protocol: Mga Protocol sa Web (T1071.001)	Ingress Tool Transfer (T1105)
Application Layer Protocol: Mga File Transfer Protocol (T1071.002)	Proxy: Internal Proxy (T1090.001)
Proxy: External Proxy (T1090.002)	Non-Standard Port (T1571)
Proxy: Multi-hop Proxy (T1090.003)	Protocol Tunnelling (T1572)
Web Service: Bidirectional Communication (T1102.002)	Encrypted Channel (T1573)
Encrypted Channel: Asymmetric Cryptography (T1573.002)	Ingress Tool Transfer (T1105)
Proxy, Technique T1090 - Enterprise | MITRE ATT&CK®	

Impact (TA0040)	
Service Stop (T1489)	Disk Wipe (T1561)
System Shutdown/Reboot (T1529)	Pag-hijack ng Resource (T1496)

Mga Tala

Pagtatatwa

Ang materyal sa gabay na ito ay may pangkalahatang katangian at hindi dapat ituring bilang legal na payo o pagsalalayan para sa tulong sa anumang partikular na pangyayari o emerhensya. Sa anumang mahalagang bagay, dapat kang humingi ng naaangkop na independiyenteng propesyonal na payo kaugnay ng iyong sariling mga kalagayan.

Ang Commonwealth ay hindi tumatanggap ng responsibilidad o pananagutan para sa anumang pinsala, pagkawala o gastos na natamo bilang resulta ng pagsalalay sa impormasyong nakapaloob sa gabay na ito.

Para sa higit pang impormasyon, o para mag-report ng insidente tungkol sa cyber security, makipag-ugnayan sa amin:

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

Ang numerong ito ay magagamit lamang sa loob ng Australia.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre