Panduan Nasihat APT40

Aksi Kemahiran Dagang PRC MSS

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**

Isi Kandungan

Pengenalan

Latarbelakang

Panduan nasihat ini, yang dikarang oleh Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), the United States Cybersecurity and Infrastructure Security Agency (CISA), the United States National Security Agency (NSA), the United States Federal Bureau of Investigation (FBI), the United Kingdom National Cyber Security Centre (NCSC-UK), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), the German Federal Intelligence Service (BND) and Federal Office for the Protection of the Constitution (BfV), the Republic of Korea's National Intelligence Service (NIS) and NIS' National Cyber Security Center, and Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and National Police Agency (NPA) – dirujuk seterusnya sebagai "agensi-agensi pengarang" – menggariskan maklumat mengenai sebuah kumpulan siber yang disokong-negara oleh Republik Rakyat China (People's Republic of China) (PRC) dan ancaman semasanya ke atas jaringan-jaringan Australia. Panduan nasihat ini memanfaatkan persefahaman yang dikongsi para agensi pengarang mengenai ancaman tersebut selain siasatan respons insiden ASD ACSC.

Kumpulan siber yang disokong-negara PRC berkenaan sebelum ini telah menyasarkan organisasi-organisasi di pelbagai negara, termasuk Australia dan Amerika Syarikat, dan teknik-teknik yang digariskan di bawah kerap diguna oleh para pelaku yang disokong-negara PRC di seluruh dunia. Oleh yang demikian, pihak agensi pengarang percaya bahawa kumpulan ini, dan teknik-tekniknya yang serupa, kekal menjadi satu ancaman kepada jaringan-jaringan negara mereka juga.

Para agensi pengarang telah menilai bahawa kumpulan ini melakukan operasi siber berniat jahat bagi Kementerian Keselamatan Negara (Ministry of State Security) (MSS). PRC Aktiviti dan teknik-teknik mereka bertindih dengan kumpulan-kumpulan yang dijejaki sebagai Advanced Persistent Threat (APT) 40 (juga dikenali sebagai Kryptonite Panda, GINGHAM TYPHOON, Leviathan dan Bronze Mohawk dalam laporan industri). Kumpulan ini dahulunya pernah dilaporkan sebagai berpangkalan di Haikou, Wilayah Hainan, PRC dan menerima penugasannya daripada PRC MSS, Jabatan Keselamatan Negara Hainan.[2] Panduan nasihat berikut menyampaikan satu sampel kajian kes yang signifikan berkenaan teknik-teknik pihak seteru ini dalam tindakan mereka terhadap jaringan dua mangsa. Kajian kes ini penting bagi para pengamal keselamatan siber untuk mengenal pasti, menghalang dan memulih kembali pencerobohan APT40 terhadap jaringan mereka sendiri. Kajian kes terpilih ini mewakili kes di mana pemulihan kembali yang sewajarnya telah diambil untuk mengurangkan risiko pengeksploitasian kembali oleh pelaku ancaman ini, atau pihak lain. Oleh itu, kajian-kajian kes ini semestinya mewakili kes-kes yang sudah berlaku lama dahulu, untuk memastikan organisasi-organisasi berkaitan telah diberi tempoh masa sepatutnya untuk memulihkan diri mereka kembali.

Ringkasan Aktiviti

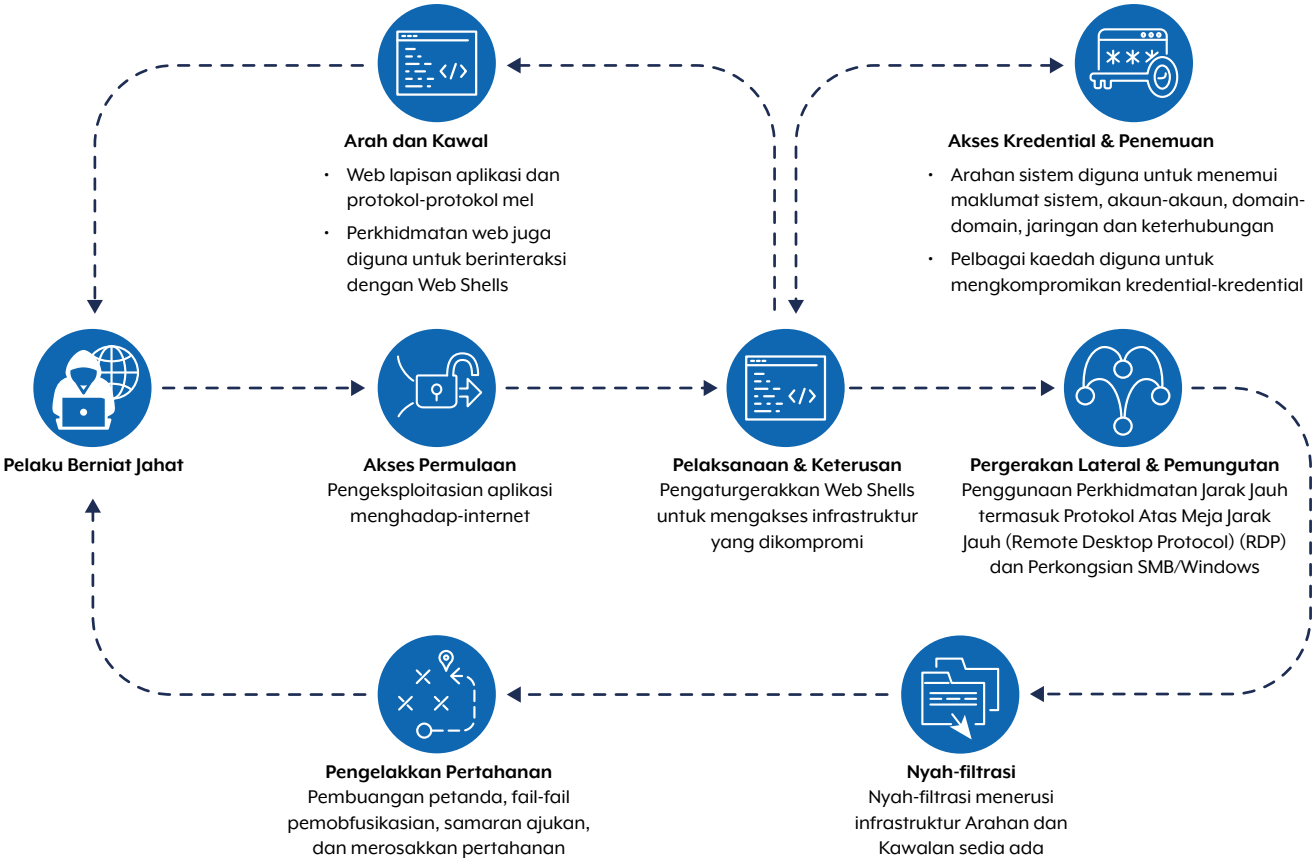
APT40 telah berkali-kali menyasarkan jaringan-jaringan Australia selain jaringan-jaringan kerajaan dan sektor swasta dalam rantau ini, dan merupakan ancaman berterusan terhadap jaringan-jaringan kami. Kemahiran Dagang yang dijelaskan dalam panduan nasihat ini sering diperhatikan berlaku terhadap jaringan-jaringan Australia.

Lebih penting lagi, APT40 memiliki keupayaan untuk mengubah dan menyesuaikan dirinya dengan pantas untuk mengeksploitasikan proof-of-concept(s) (POCs) bagi kerentanan baharu dan menggunapakaikannya dengan serta-merta terhadap jaringan-jaringan yang disasarkan yang memiliki infrastruktur kerentanan berkaitan. APT40 kerap melakukan reconnaissance terhadap jaringan-jaringan yang menarik perhatian mereka, termasuk jaringan-jaringan dalam negara-negara pihak agensi pengarang, untuk mencari peluang untuk mengkompromikan sasaran-sasarannya. Recon yang kerap berlaku ini meletakkan kumpulan ini dalam kedudukan dari mana mereka boleh mengenal pasti alat-alat peranti rentan, penghujung-hayat atau yang tidak lagi diselenggarakan pada jaringan-jaringan yang menarik perhatian mereka, dan untuk mengaturgerakkan pengekspliotasi dengan pantas. APT40 terus berjaya dalam mengeksploitasikan kerentanan dari seawal 2017 lagi.

APT40 mengeksploitasi dengan pantas kerentanan awam baharu di dalam perisian yang diguna secara meluas seperti Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) dan Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473). ASD ACSC dan para agensi pengarang menjangka bahawa kumpulan ini akan terus menggunakan POCs bagi kerentanan profil-tinggi baharu dalam tempoh hanya beberapa jam atau hari dari saat ia mula dilancarkan kepada orang ramai.

2 Jabatan Keadilan A.S. (U.S. Department of Justice.) 2021. Empat Warga Nasional China Yang Bekerja engan Kementerian Keselamatan Negara Didakwa melakukan Kempen Pencerobohan Komputer Global Yang Menyasarkan Harta Intelek dan Maklumat Perniagaan Sulit, Termasuk Penyelidikan Penyakit Berjangkit.

Rajah 1: Carta aliran TTP untuk Aktiviti APT40



Kumpulan ini nampaknya lebih suka mengeksploitasi infrastruktur rentan, dan menghadap-pihak awam daripada teknik-teknik yang memerlukan interaksi pengguna, seperti kempen-kempen pancingan, dan meletakkan keutamaan tinggi dalam pemerolehan kredential-kredential sahih untuk membolehkan pelbagai aktiviti lanjutan. APT40 kerap menggunakan web shells (T1505.003) untuk berterusan (persistence), khususnya pada tahap awal kitaran hidup sesuatu pencerobohan. Lazimnya, selepas berjaya memperolehi akses permulaan APT40 akan berfokus kepada penubuhan keterusan untuk mengekalkan akses pada persekitaran mangsa. Namun begitu, oleh kerana keterusan ini berlaku pada tahap awal sesebuah pencerobohan, ia lebih mudah diperhatikan dalam semua pencerobohan – tanpa mengira sejauh mana pengkompromian atau tindakan lanjut diambil.

Kemahiran Dagang Terpilih

Walaupun APT40 dahulunya pernah menggunakan laman-laman web Australia yang telah dikompromi sebagai hos-hos arahan dan kawalan (C2) untuk operasinya, kumpulan ini telah mengembangkan teknik ini (T1594).

APT40 telah menyambut trend global untuk menggunakan alat-alat peranti yang sudah dikompromi, termasuk alat-alat peranti pejabat-kecil/pejabat-di rumah (SOHO), sebagai infrastruktur pengoperasian dan pengarah-kembali loncatan-terakhir (T1584.008 bagi operasinya di Australia. Ini membolehkan para agensi pengarang untuk menyifatkan dan menjejaki pergerakan kumpulan ini dengan lebih baik.

Kebanyakan alat-alat peranti SOHO ini sudah mencapai akhir-hayatnya atau tidak ditampal dan menawarkan dirinya sebagai sasaran mudah bagi pengeksploitasian hari-N. Apabila ia sudah dikompromi, alat-alat peranti SOHO menawarkan batu loncatan bagi serangan yang direka untuk menyesuaikan dirinya ke dalam trafik sahih dan mencabar para pelindung jaringan (T1001.003).

Teknik ini juga kerap diguna oleh para pelaku yang dianjurkan-negara PRC di seluruh dunia, dan pihak agensi pengarang menganggap hal ini sebagai sebuah ancaman yang dikongsi. Untuk maklumat lanjut, sila rujuk panduan nasihat bersama People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices dan PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.

APT40 kadangkala menggunakan infrastruktur yang diperolehi atau disewa sebagai infrastruktur C2 yang menghadap-mangsa di dalam operasinya; namun begitu, kemahiran dagang ini nampaknya sedang agak merosot.

Pemeralatan

ASD ACSC sedang berkongsi sesetengah daripada fail-fail berniat jahat yang telah dikenal pasti semasa penyiasatan yang digariskan di bawah. Fail-fail ini telah dimuatnaik ke VirusTotal untuk membolehkan pertahanan jaringan dan komuniti-komuniti keselamatan siber yang lebih meluas untuk memahami ancaman-ancaman yang mereka perlu mempertahankan diri mereka ini dengan lebih baik.

Kajian Kes

ASD ACSC sedang berkongsi dua laporan siasatan yang telah dianonimkan untuk menyampaikan kesedaran mengenai bagaimana para pelaku menggunapakai peralatan dan kemahiran dagang mereka.

MD5	Nama fail	Maklumat tambahan
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

Kajian Kes 1

Laporan ini telah dianonimkan untuk membenarkan penyebarannya dengan lebih meluas. Organisasi yang terimpak akan dirujuk seterusnya sebagai 'organisasi'. Beberapa butiran khusus telah dikeluarkan untuk melindungi identiti mangsa dan kaedah-kaedah respons insiden ASD ACSC.

Ringkasan eksekutif

Laporan ini memperincikan hasil dapatan siasatan ASD ACSC terhadap pengkompromian yang berjaya dilakukan terhadap jaringan organisasi berkaitan antara Julai dan September 2022. Laporan penyiasatan ini telah disediakan kepada organisasi itu untuk meringkaskan aktiviti berniat jahat yang diperhatikan dan membingkaikan saranan pemulihan kembali. Hasil dapatan ini menunjukkan bahawa kompromi ini telah dilakukan oleh APT40.

Pada pertengahan-Ogos, ASD ACSC telah memberitahu organisasi berkenaan tentang interaksi berniat jahat dengan jaringan mereka daripada sebuah alat peranti yang kemungkinan besar telah dikompromi yang sedang diguna oleh kumpulan tersebut pada lewat Ogos dan, dengan izin organisasi itu, ASD ACSC telah mengaturgerakkan sensor berpangkalan pada hos ke hos yang kemungkinan besar terjejas pada jaringan organisasi itu. Sensor-sensor ini membenarkan para penganalisis respons insiden ASD ACSC untuk melakukan penyiasatan forensik digital yang menyeluruh. Dengan menggunakan data sensor sedia ada, para penganalisis ASD ACSC telah berjaya memetakan aktiviti kumpulan itu dan mewujudkan sebuah garis masa terperinci mengenai peristiwa-peristiwa yang diperhatikan.

Dari Julai ke Ogos, aktiviti pelaku utama telah diperhati oleh ASD ACSC, termasuk:

- Pembilangan hos, yang membenarkan seseorang pelaku untuk membina peta jaringan mereka sendiri:
- Penggunaan web shell, memberikan pelaku langkah pembuka pada jaringan tersebut dan keupayaan untuk melaksanakan arahan; dan
- Pengaturgerakkan peralatan lain yang dikumpil oleh pelaku berkaitan bagi tujuan berniat jahat.

Siasatan telah mendedahkan kesan bukti sejumlah besar data sensitif yang sedang diakses dan kesan bukti bahawa para pelaku ini telah bergerak secara lateral melalui jaringan itu (T1021.002). Sebahagian besar pengkompromian ini telah dipermudahkan oleh penubuhan vektor-vektor pelbagai akses oleh organisasi ini ke dalam jaringan itu, di mana jaringan itu memiliki infrastruktur rata, dan penggunaan perisian tidak teguh yang dibangunkan secara dalaman yang boleh diguna untuk memuat naik fail tanpa menimbangkan baik-buruknya dahulu. Data yang dieksfiltrasikan termasuk kredential-kredential penentusahan yang diberi laluan istimewa yang membolehkan kumpulan itu untuk mendaftar masuk, selain maklumat jaringan yang boleh membenarkan para pelaku untuk menuntut kembali akses yang tidak diluluskan jika akses vektor asal telah disekat. Tiada pemeralatan berniat jahat tambahan ditemui selain daripada apa yang ada pada mesin yang dieksploitasi pada mulanya; namun begitu, akses sesebuah kumpulan ke kredential-kredential sahih dan berlaluan istimewa mungkin akan membatalkan keperluan untuk pemeralatan tambahan. Hasil dapatan siasatan ini menunjukkan organisasi ini kemungkinan besar telah disasarkan secara sengaja oleh APT40, dan bukannya menjadi mangsa kesempatan yang diambil terhadap sebuah kerentanan yang diketahui umum.

Dapatan Siasatan

Pada pertengahan-Ogos 202, ASD ACSC telah memberitahu organisasi itu bahawa satu IP berniat jahat yang disahkan dipercayai bersekutu dengan sebuah kumpulan siber yang dianjurkan-negara telah berinteraksi dengan jaringan komputer mereka antara sekurang-kurangnya Julai dan Ogos. Alat peranti yang dikompromi itu kemungkinannya dimiliki oleh sebuah perniagaan kecil atau pengguna di rumah.

Pada lewat Ogos, ASD ACSC telah mengaturgerakkan sebuah ejen berpangkalan-hos kepada hos-hos pada jaringan organisasi itu yang menunjukkan kesan bukti ia telah mengalami impak berikutan pengkompromian itu.

Sesetengah artifak yang mungkin dapat menyokong usaha siasatan ini tidak dapat disediakan disebabkan pengkonfigurasian rekabentuk pelogan atau jaringan. Biarpun begitu, kesediaan organisasi itu untuk menyampaikan semua data yang sedia ada telah membolehkan para perespons insiden ASD ACSC untuk melakukan analisis komprehensif dan untuk membentuk sebuah pemahaman tentang aktiviti APT40 yang kemungkinan besar telah berlaku pada jaringan tersebut.

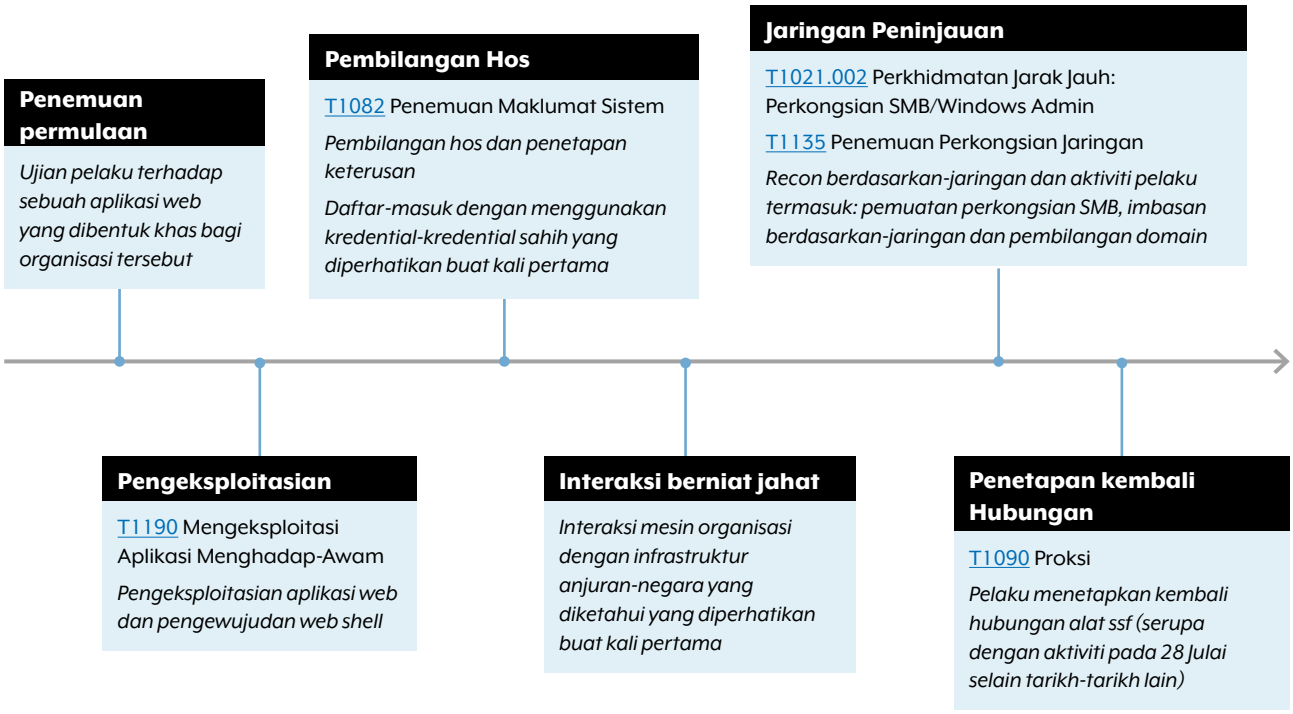
Pada September, selepas rundingan bersama ASD ACSC, organisasi itu mengambil keputusan untuk mengolah penyenaraian IP yang dikenalpasti dalam penotifikasian awalnya. Pada Oktober, organisasi itu memulakan usaha pemulihan kembali.

Butir-butir

Bermula Julai, para pelaku telah berupaya menguji dan mengeksploitasi sebuah aplikasi web yang dibentuk khas (T1190) yang berjalan pada `<webapp>2-ext`, yang membolehkan kumpulan itu untuk menetapkan langkah pembuka dalam zon nyah-militer (demilitarized zone) (DMZ) jaringan tersebut. Perkara ini telah dikumpilkan untuk membilangkan jumlah jaringan dan juga domain yang kelihatan sekali. Kredential-kredential yang telah dikompromi (T1078.002) telah diguna untuk menyoal Direktori Aktif (Active Directory) (T1018) dan mengeksfiltrasikan data dengan memuatkan perkongsian fail (T1039) daripada pelbagai mesin di dalam DMZ. Pelaku tersebut telah melakukan sebuah serangan Kerberoasting untuk memperolehi kredential-kredential jaringan sahih daripada sebuah server (T1558.003). Kumpulan berkaitan tidak diperhati memperolehi mana-mana titik keberhadiran (points of presence) tambahan dalam baik DMZ mahupun jaringan dalaman.

Garis Masa Visual

Garis masa di bawah menyampaikan gambaran meluas fasa-fasa utama dalam aktiviti pelaku berniat jahat yang diperhati dalam jaringan organisasi ini.



Garis Masa Terperinci

Julai: Para pelaku telah menetapkan sebuah aplikasi permulaan pada halaman hadapan sebuah aplikasi web yang dibentuk khas (T1190) yang dibina untuk organisasi ini (dirujuk seterusnya sebagai 'aplikasi' atau '*webapp*') menerusi sebuah hubungan keselamatan lapisan pengangkutan (transport layer security) (TLS) (T1102). Tiada kegiatan lain yang menarik perhatian diperhatikan.

Julai: Para pelaku mula membilang laman web aplikasi web itu untuk mencari titikpenghujung (endpoints) [2] untuk siasatan lanjut.

Julai: Para pelaku menumpukan perhatian ke atas cubaan untuk mengeksploitasikan satu titikpenghujung khusus.

Julai: Para pelaku berjaya `MENGHANTAR` ke server web, kemungkinan besar menerusi sebuah shell web yang diletakkan pada sebuah halaman lain. Sebuah IP kedua, kemungkinan besar dipergunakan oleh pelaku sama, juga mula membuat hantaran ke URL yang sama. Para pelaku telah mencipta dan menguji sebilangan shell web yang berpotensi.

Kaedah tepat pengeksploitasian ini tidak diketahui, tetapi ia jelas bahawa titik penghujung khusus itu telah disasarkan untuk mewujudkan fail `<webapp>2-ext`.

ASD ACSC percaya bahawa kedua-dua hubungan alamat IP ialah sebahagian daripada pencerobohan yang sama kerana minat yang dikongsi mereka bersama dan hubungan permulaan yang berlaku hanya beberapa minit antara satu sama lain.

Julai: Kumpulan itu terus melakukan pembilangan hos, untuk mencari peluang pendadakan keistimewaan, dan mengaturgerakkan sebuah web shell lain. Para pelaku melog masuk ke dalam aplikasi web itu dengan menggunakan kredential-kredential yang telah dikompromi untuk `<firstname.surname>@<organisation domain>`.

Aktiviti para pelaku ini nampaknya tidak berjaya dalam usaha mereka untuk mendadakkan keistimewaan pada `<webapp>2-ext`. Sebaliknya, para pelaku itu telah beralih kepada aktiviti berdasarkan-jaringan.

Julai: Para pelaku menguji kredential-kredential yang dikompromi untuk sebuah akaun perkhidmatan [3] yang kemungkinan besar ditemui dikodkeraskan (hardcoded) dalam binari-binari yang boleh diakses secara dalaman.

Julai: Para pelaku telah mengaturgerakkan alat sumber-terbuka Secure Socket Funnelling, yang diguna untuk berhubung keluar ke infrastruktur berniat jahat tersebut. Hubungan ini digunapakai untuk menerowongkan trafik dari mesin-mesin serangan para pelaku ke alam jaringan-jaringan dalaman organisasi itu, di mana nama mesin mereka didedahkan dalam log-log kejadian apabila mereka cuba untuk menggunakan kredential-kredential itu bagi akaun perkhidmatan tersebut.

Ogos: Para pelaku dilihat melakukan sejumlah aktiviti terhad, termasuk kegagalan untuk menetapkan hubungan melibatkan akaun perkhidmatan.

Ogos: Para pelaku melaksanakan pembilangan jaringan dan Direktori Aktif yang signifikan. Sebuah akaun yang sudah dikompromi lain kemudian digunapakai untuk memasang perkongsian[4] pada mesin-mesin Windows di dalam DMZ, yang membolehkan pengeksfiltrasian data dilakukan dengan berjaya.

Ini nampaknya satu penggunaan yang mengambil kesempatan kredential yang telah dicuri pada mesin-mesin yang sudah dipasang dalam DMZ. Penghadang api telah menyekat pelaku daripada menyasarkan jaringan dalaman dengan aktiviti serupa.

Ogos – **September:** Alat SSF telah menubuhkan kembali sebuah hubungan kepada sebuah IP berniat jahat. Kumpulan berkenaan tidak diperhati melakukan sebarang aktiviti tambahan sehingga akses mereka disekat.

September: Pihak organisasi menyekat IP berniat jahat itu dengan menafikan penyenaraiannya pada penghadang api mereka.

2 Dalam konteks ini, sesebuah titik penghujung (endpoint) merupakan satu fungsi aplikasi web tersebut.

3 Akaun-akaun perkhidmatan tidak terikat kepada pengguna individu, tetapi sebaliknya kepada perkhidmatan-perkhidmatan. Terdapat pelbagai jenis akaun dalam sebuah domain korporat Microsoft.

4 Pemasangan perkongsian ialah proses pembikinan fail-fail pada sesuatu struktur sistem fail yang boleh diakses oleh seorang pengguna atau kumpulan pengguna.

Taktik-taktik dan teknik-teknik pelaku

Kerangka kerja MITRE ATT&CK ialah satu koleksi terakam taktik-taktik dan teknik-teknik yang digunapakai oleh pelaku ancaman dalam ruang siber. Kerangka kerja ini telah dicipta oleh badan bukan-untuk-keuntungan AS, The MITRE Corporation dan berfungsi sebagai sebuah bahasa global bersama yang berlegar atas soal tingkah laku pelaku ancaman.

ASD ACSC menilai teknik-teknik dan taktik-taktik berikut sebagai relevan kepada aktiviti-aktiviti berniat jahat pihak pelaku:

Peninjauan

T1594 – Cari Laman Web Yang Dimiliki-Mangsa

Pelaku telah membilang laman web aplikasi web yang dibentuk khas untuk mengenal pasti peluang untuk mengakses jaringan tersebut.

Akses Permulaan

T1190 – Mengeksploitasikan Aplikasi Menghadap-Awam (berkenaan pengeksploitasian aplikasi web yang dibentuk khas)

T1078.002 – Akaun-Akaun Sahih: Akaun-Akaun Domain (berkenaan pelogan masuk dengan kredential-kredential yang telah dikompromi)

Pengeksploitasian aplikasi-aplikasi web yang dibentuk khas dan menghadap internet telah memberikan titik permulaan akses kepada pelaku itu. Pelaku itu kemudian berupaya menggunakan kredential-kredential yang telah dikompromi mereka untuk memperluaskan akses mereka ke dalam jaringan itu.

Pelaksanaan

T1059 – Jurutafsir Arahan dan Penskripsian (berkenaan pelaksanaan arahan melalui shell web)

T1072 – Peralatan Pengaturgerakan Perisian (berkenaan pelaku menggunakan alat sumber-terbuka Secure Socket Funnelling (SSF) untuk berhubung kepada sebuah IP)

Keterusan

T1505.003 – Komponen Perisian Server: Shell Web (berkenaan penggunaan shell web dan SSF untuk mewujudkan akses)

Akses Kredential

T1552.001 – Kredential-Kredential daripada Stor-Stor Kata Laluan (berkenaan fail-fail kata laluan berkaitan pembinaan sistem pengurusan (building management system) (BMS))

T1558.003 – Curi atau Palsukan Tiket-Tiket Kerberos: Kerberoasting (berkenaan serangan untuk memperolehi kredential-kredential jaringan)

Pergerakan Lateral

T1021.002 – Perkhidmatan-Perkhidmatan Jarak Jauh: Perkongsian SMB (berkenaan pelaku memasang perkongsian SMB daripada pelbagai alat peranti)

Pemungutan

T1213 – Data daripada Repositori-Repositori Maklumat (berkenaan buku-buku panduan/pendokumentasian yang ditemui pada server BMS)

Peneksfiltrasian

T1041 – Pengeksfiltrasian Melalui Saluran C2 (berkenaan pengeksfiltrasian data pelaku daripada Direktori Aktif dan pemasangan perkongsian)

Kajian Kes 2

Laporan ini telah dianonimkan untuk membenarkan penyebarannya dengan lebih meluas. Organisasi yang terimpak akan dirujuk seterusnya sebagai 'organisasi'. Beberapa butiran khusus telah dikeluarkan untuk melindungi identiti mangsa dan kaedah-kaedah respons insiden ASD ACSC.

Ringkasan eksekutif

Laporan ini memperincikan hasil dapatan siasatan ASD ACSC terhadap pengkompromian yang berjaya dilakukan terhadap jaringan organisasi berkaitan pada April 2022. Laporan penyiasatan ini telah disediakan kepada organisasi itu untuk meringkaskan aktiviti berniat jahat yang diperhatikan dan membingkaikan saranan pemulihan kembali. Hasil dapatan ini menunjukkan bahawa kompromi ini telah dilakukan oleh APT40.

Pada Mei 2022, ASD ACSC telah memberitahu organisasi berkenaan mengenai aktiviti berniat jahat yang disyaki yang mengimpak jaringan organisasi itu semenjak April 2022. Kemudian, organisasi itu telah memaklumkan ASD ACSC bahawa mereka telah menemui perisian berniat jahat pada sebuah server menghadap-internet yang menyediakan portal daftar-masuk bagi solusi akses jarak jauh korporat organisasi itu. Server ini menggunakan sebuah daftar masuk akses jarak jauh dan produk pengurusan identiti dan akan dirujuk dalam laporan ini sebagai 'peralatan yang dikompromi'. Laporan ini memperincikan hasil dapatan siasatan dan nasihat pemulihan kembali yang dibangunkan bagi organisasi itu sebagai respons kepada siasatan yang dilakukan oleh ASD ACSC.

Kesan bukti menunjukkan bahawa sebahagian daripada jaringan organisasi itu telah dikompromi oleh pelaku(-pelaku) siber berniat jahat menerusi portal daftar masuk akses jarak jauh organisasi itu semenjak sekurang-kurangnya April 2022. Server ini mungkin telah dikompromi pelbagai pelaku, dan kemungkinan besar dijejas oleh kerentanan pelaksanaan kod jarak jauh (remote execution code) (RCE) yang telah dihebahkan secara meluas sekitar waktu pengkompromian itu.

Aktiviti pelaku utama yang diperhati oleh ASD ACSC termasuk:

- pembilangan hos, yang membolehkan seorang pelaku untuk membina peta mereka sendiri bagi jaringan berkaitan.
- pengeksploitasian aplikasi menghadap-internet dan penggunaan web shell, yang memberi pihak pelaku langkah permulaan pada jaringan itu dan keupayaan untuk melaksanakan arahan;
- pengeksploitasian kerentanan perisian untuk mendadakkan keistimewaan; dan
- pemungutan kredential untuk membolehkan pergerakan lateral

ASD ACSC telah menemui bahawa satu pelaku berniat jahat telah mengeksfiltrasikan beratus-ratus pasangan nama pengguna dan kata laluan unik pada perkakasan yang dikompromi itu pada April 2022, selain sejumlah kod-kod penentusahan pelbagai-faktor dan artifak-artifak teknikal yang berkaitan sesi-sesi akses jarah jauh. Setelah penilaian kembali dibuat oleh organisasi itu, kata-kata laluan itu didapati adalah sahih. ASD ACSC telah menilai bahawa pelaku itu mungkin telah memungut artifak-artifak teknikal ini untuk merampas atau mewujudkan sebuah sesi daftar masuk jarak jauh sebagai seorang pengguna sahih, dan mengakses jaringan korporat dalaman organisasi itu dengan menggunakan sebuah akaun pengguna sahih.

Hasil dapatan siasatan

Ringkasan siasatan

ASD ACSC telah menentukan bahawa pelaku itu telah mengkompromikan peralatan (-peralatan) yang menyediakan sesi daftar masuk jarak jauh kepada kakitangan organisasi itu dan telah menggunakan kompromi ini untuk cuba melakukan aktiviti selanjutnya. Peralatan-peralatan ini terdiri daripada tiga hos imbangan-muatan (load-balanced) di mana kesan bukti terawal kompromi telah dikesan. Organisasi itu telah menutup dua daripada tiga hos imbangan-muatan ini tidak lama selepas kompromi permulaan berlaku. Oleh kerana itu, semua aktiviti selanjutnya telah berlaku pada satu hos tunggal sahaja. Server-server lain yang dikaitkan dengan peralatan yang dikompromi itu juga telah diimbang-muatkan dalam kaedah yang sama. Bagi memudahkan pemahaman, semua peralatan yang dikompromi ini akan dirujuk di dalam kebanyakan laporan ini sebagai 'peralatan tunggal'.

Pelaku itu dipercayai telah menggunakan kerentanan yang diketahui awam untuk mengaturgerakkan shell-shell web kepada peralatan yang dikompromi mulai April 2022. Pelaku ancaman daripada kumpulan itu dinilai dan didapati telah mencapai keistimewaan yang didadakkan pada peralatan itu. ASD ACSC tidak dapat menentukan sejauh mana aktiviti itu berlaku disebabkan kekurangan pelogan yang sedia ada. Namun begitu, kesan bukti pada alat peranti itu menunjukkan bahawa pelaku itu telah mencapai perkara-perkara berikut:

- Pemungutan ratusan pasangan nama pengguna dan kata laluan tulen; dan
- Pemungutan artifak-artifak teknikal yang mungkin telah membenarkan seorang pelaku berniat jahat untuk mengakses sesi infrastruktur atas meja virtual (virtual desktop infrastruktur) (VDI) sebagai seorang pengguna sahih.

ASD ACSC menilai bahawa pelaku mungkin telah cuba untuk melanjutkan pengkompromian jaringan organisasi ini. Artifak-artifak yang dieksfiltrasi oleh pelaku itu mungkin telah membenarkan mereka untuk merampas atau memulakan sesi-sesi atas meja virtual sebagai seorang pengguna sahih, kemungkinannya sebagai seorang pengguna pilihan mereka, termasuk pada pentadbir. Pelaku berkenaan mungkin telah menggunakan vektor akses ini untuk melanjutkan pengkompromian perkhidmatan-perkhidmatan organisasi ini untuk mencapai keterusan dan matlamat-matlamat lain.

Peralatan-peralatan organisasi lain di dalam persekitaran terurus penyedia penghosan tidak menunjukkan kesan bukti pengkompromian.

Akses

Hos dengan peralatan yang dikompromi telah menyampaikan penentusahan menerusi Direktori Aktif dan sebuah server web, bagi pengguna yang terhubung kepada sesi-sesi VDI (T1021.001).

Lokasi	Nama hos peralatan yang dikompromi (diimbang-muatan)
Pusat Data 1	HOST1, HOST2, HOST3

Infrastruktur peralatan itu juga mengandungi hos-hos pintu gerbang akses yang menyampaikan terowong kepada VDI bagi pengguna, apabila mereka mempunyai sebuah token penentusahan yang dijana dan dimuat turun daripada peralatan itu.

Tiada kesan bukti ditemui yang menunjukkan pengkompromian mana-mana hos ini. Namun begitu, log-log hos pintu gerbang akses menunjukkan kesan bukti interaksi signifikan dengan alamat-alamat IP yang berniat jahat. Kemungkinan besar hal ini mencerminkan aktiviti yang telah berlaku pada hos ini, atau hubungan jaringan dengan infrastruktur pelaku ancaman yang telah sampai ke hos ini. Sifat aktiviti ini tidak dapat ditentukan dengan menggunakan kesan bukti sedia ada tetapi ia menunjukkan bahawa kumpulan itu telah berusaha untuk bergerak secara lateral dalam jaringan organisasi ini (TA0008).

Hos-hos dalaman

ASD ACSC telah menyiasat data terhad daripada segmen jaringan dalaman organisasi ini. Aktiviti berniat jahat berbentuk cubaan atau yang berjaya diketahui telah meninggalkan impak ke atas segmen jaringan dalaman organisasi ini termasuk akses pelaku kepada artifak-artifak berkaitan-VDI, perautan server SQL dalaman (T1505.001), dan trafik yang tidak dapat dijelaskan yang diperhatikan keluar daripada alamat-alamat IP berniat jahat yang diketahui melalui peralatan-peralatan gerbang masuk akses berkaitan (TA0011).

Dengan menggunakan akses mereka kepada peralatan yang dikompromi itu, kumpulan berkenaan telah memungut nama pengguna, kata laluan (T1003), dan nilai-nilai token MFA (T1111) yang tulen. Kumpulan ini juga telah memungut JSON Web Tokens (JWT-JWT) (T1528), iaitu sebuah artifak penentusahan yang diguna untuk mewujudkan sesi daftar masuk atas meja virtual. Pelaku ini mungkin telah berupaya menggunakannya untuk mewujudkan atau merampas sesi atas meja virtual

(T1563.002) dan mengakses segmen jaringan dalaman organisasi ini sebagai seorang pengguna sahih (T1078).

Pelaku ini juga telah menggunakan akses kepada peralatan yang dikompromi untuk meraut sebuah server SQL (T1505.001), yang berada di dalam jaringan dalaman organisasi ini. Kemungkinan besar pelaku ini telah memiliki akses kepada data ini.

Kesan bukti sedia ada daripada gerbang masuk akses ini mendedahkan bahawa trafik jaringan telah berlaku melalui atau ke alat peranti ini daripada alamat-alamat IP berniat jahat yang diketahui. Seperti yang dijelaskan di atas, hal ini mungkin menunjukkan bahawa pelaku siber berniat jahat telah meninggalkan impak atau menggunapakai alat peranti ini, dengan potensi untuk memaksi ke dalam jaringan dalaman berkaitan.

Garis masa siasatan

Senarai di bawah ini menyampaikan garis masa aktiviti-aktiviti utama yang ditemui dalam siasatan ini

Masa	Peristiwa
April 2022	Alamat-alamat IP berniat jahat yang dikenali telah berinteraksi dengan hos pintu gerbang akses HOST7. Sifat interaksi-interaksi ini tidak dapat ditentukan.
April 2022	Semua hos, HOST1, HOST2 and HOST3, telah dikompromi oleh seorang pelaku atau beberapa pelaku berniat jahat, dan shell-shell web telah diletakkan pada hos-hos itu. Sebuah fail log telah diwujudkan atau dimodifikasikan pada HOST2. Fail ini mengandungi bahan kredential yang kemungkinan besar telah ditangkap oleh seorang pelaku berniat jahat. Fail-fail /etc/security/opasswd dan /etc/shadow telah dimodifikasi pada HOST1 dan HOST3, yang menunjukkan bahawa kata-kata laluan telah diubah. Kesan bukti yang ditemui pada HOST1 mencadangkan bahawa kata laluan bagi pengguna 'sshuser' telah ditukar.
April 2022	HOST2 telah ditutup oleh organisasi ini. Shell-shell web tambahan (T1505.003) telah diwujudkan pada HOST1 dan HOST3. HOST1 mengalami cubaan keganasan kasar SSH daripada HOST3. Sebuah fail log telah dimodifikasikan (T1070) pada HOST3. Fail ini mengandungi bahan kredential (T1078) yang kemungkinan besar telah ditangkap oleh seorang pelaku berniat jahat. JWT-JWT telah ditangkap (T1528) dan dikeluarkan ke sebuah fail pada HOST3. HOST3 telah ditutup oleh organisasi ini. Semua aktiviti selepas waktu ini berlaku pada HOST1.
April 2022	Shell-shell web tambahan telah diwujudkan pada HOST1 (T1505.003). JWT-JWT telah ditangkap dan dikeluarkan ke dalam sebuah fail pada HOST1.
April 2022	Shell-shell web tambahan telah diwujudkan pada HOST1 (T1505.003), dan sebuah alamat IP berniat jahat yang diketahui telah berinteraksi dengan hos (TA0011). Sebuah alamat IP berniat jahat yang diketahui telah berinteraksi dengan hos gerbang masuk akses HOST7.
Mei 2022	Sebuah alamat IP berniat jahat yang diketahui telah berinteraksi dengan hos gerbang masuk akses HOST7 (TA0011). Sebuah peristiwa penentusahan bagi seorang pengguna dikaitkan kepada sebuah alamat IP berniat jahat yang diketahui dalam log-log pada HOST1. Sebuah shell web tambahan telah diwujudkan pada hos ini (T1505.003).
Mei 2022	Sebuah skrip pada HOST1 telah dimodifikasi oleh seorang pelaku (T1543). Skrip ini mengandungi kefungsian yang berupaya meraut data daripada sebuah server SQL dalam.
Mei 2022	Sebuah fail log tambahan HOST1 telah dimodifikasi (T1070). Fail ini mengandungi nama pasangan nama pengguna dan kata laluan bagi jaringan organisasi ini, yang dipercayai adalah sahih (T1078).
Mei 2022	Sebuah fail log tambahan telah dimodifikasi (T1070). Fail ini mengandungi JWT-JWT yang dipungut daripada HOST1.
Mei 2022	Shell-shell web tambahan telah diwujudkan pada HOST1 (T1505.003). Pada tarikh ini, organisasi ini telah melaporkan penemuan sebuah shell web dengan tarikh pengewujudan pada April 2022 kepada ASD's ACSC
Mei 2022	Sejumlah skrip telah diwujudkan pada HOST1, termasuk satu yang dinamakan Log4jHotPatch.jar.
Mei 2022	Arahan iptables-save telah diguna untuk menambah dua port terbuka kepada hos pintu gerbang akses. Port-portnya ialah 9998 dan 9999 (T1572).

Taktik-taktik dan teknik-teknik pelaku

Di bawah ini diketengahkan beberapa taktik dan teknik yang telah dikenal pasti dalam siasatan ini.

Akses Permulaan

T1190 Mengeksploitasikan Aplikasi Menghadap Awam

Kumpulan ini kemungkinan besar telah mengeksploitasikan RCE, pendadakan keistimewaan, dan penentusahan kerentanan pemintasan dalam daftar masuk akses jarak jauh dan produk pengurusan identiti untuk mendapatkan akses permulaan ke dalam jaringan itu.

Kaedah akses permulaan ini dianggap kemungkinan besar telah berlaku disebabkan perkara-perkara berikut:

- Pada ketika itu, server berkenaan telah mengalami kerentanan kepada CVE-CVE ini;
- Cubaan untuk mengeksploitasikan kerentanan ini daripada seorang pelaku infrastruktur yang dikenali; dan
- Aktiviti berniat jahat dalaman yang pertama diketahui telah berlaku tidak lama selepas percubaan cubaan pengeksploitasian telah dibuat.

Pelaksanaan

T1059.004 Jurutafsir Arahan dan Penskripsian: Shell Unix

Kumpulan yang berjaya mengeksploitasikan kerentanan-kerentanan di atas mungkin telah berupaya menjalankan arahan di dalam shell Unix yang sedia ada pada peralatan yang terjejas itu. Butir-butir penuh arahan-arahan yang dijalankan oleh para pelaku tidak boleh disediakan kerana ia tidak dilogkan oleh peralatan tersebut.

Keterusan

T1505.003 Komponen Perisian Server: Shell Web

Para pelaku mengaturgerakkan beberapa shell web pada peralatan yang terjejas itu. Satu kemungkinan ialah bahawa pelbagai pelaku berbeza telah mengaturgerakkan shell-shell web itu, tetapi hanya sebilangan kecil pelaku telah melakukan aktiviti dengan menggunakan shell-shell web ini. Shell web mungkin akan membenarkan pelaksanaan arahan arbitari oleh pelaku pada peralatan yang dikompromi itu.

Pendadakan Keistimewaan

T1068 Pengeksploitasian untuk Pendadakan Keistimewaan

Kesan bukti sedia ada tidak menjelaskan tahap keistimewaan yang telah dicapai oleh para pelaku itu. Namun begitu, dengan menggunakan shell-shell web, pelaku itu agaknya berjaya mencapai tahap keistimewaan seganding dengan server web berkaitan pada peralatan yang dikompromi itu. Kerentanan yang dipercayai sudah pun sedia hadir pada peralatan yang dikompromi itu telah membenarkan para pelaku itu untuk mencapai keistimewaan akar (root privileges).

Akses Kredential

T1056.003 Tangkapan Masukan (Input): Tangkapan Portal Web

Kesan bukti pada peralatan yang dikompromi itu menunjukkan bahawa pelaku telah menangkap beratus pasangan nama pengguna-kata laluan, dalam teks jelas, yang dipercayai adalah sahih. Kemungkinan besar ia telah ditangkap dengan menggunakan sedikit pemodifikasian kepada proses penentusahan tulen yang mengeluarkan kredential-kredential kepada sebuah fail.

T1111 Pemintasan Penentusahan Pelbagai-Faktor

Pelaku itu juga telah menangkap nilai token-token MFA yang dikaitkan bersama kepada daftar-daftar masuk sahih. Ia kemungkinan besar telah ditangkap dengan memodifikasian proses penentusahan tulen untuk mengeluarkan nilai-nilai ini kepada sebuah fail. Tiada kesan bukti pengkompromian 'server rahsia' yang menyimpan nilai-nilai unik yang menyediakan keselamatan bagi token-token MFA ini.

T1040 Penghiduan (Sniffing) Jaringan

Pelaku dipercayai telah menangkap JWT-JWT dengan menangkap trafik HTTP pada peralatan yang dikompromi itu. Terdapat kesan bukti bahawa utiliti tcpdump telah dilaksanakan pada peralatan yang dikompromi itu, iaitu kemungkinan besar cara bagaimana pelaku itu telah menangkap JWT-JWT ini.

T1539 Mencuri Cookie Sesi Web

Seperti yang dijelaskan di atas, pelaku ini telah menangkap JWT-JWT, yang serupa dengan cookie sesi web. Ia kemudian mungkin telah diguna kembali oleh pelaku untuk mewujudkan akses lebih lanjut.

Penemuan

T1046 Penemuan Perkhidmatan Jaringan

Terdapat kesan bukti yang menunjukkan bahawa nmap utili imbasan jaringan telah dilaksanakan pada peralatan yang dikompromi untuk mengimbas peralatan lain dalam segmen jaringan yang sama. Ini kemungkinan besar diguna oleh pelaku untuk menemui perkhidmatan-perkhidmatan jaringan lain yang boleh dicapai yang mungkin menyampaikan peluang untuk pergerakan lateral.

Pemungutan

Kesan bukti sedia ada tidak mendedahkan cara bagaimana para pelaku ini memungut data atau apa yang sebenarnya telah dipungut daripada peralatan yang dikompromi atau daripada sistem-sistem lain. Namun begitu, kemungkinan besar para pelaku telah memiliki akses kepada semua fail pada peralatan yang dikompromi itu, termasuk kredential-kredential yang ditangkap (T1003), nilai-nilai token MFA (T1111), serta JWT-JWT yang dijelaskan di atas.

Arah dan Kawal

T1071.001 Protokol Lapisan Aplikasi: Protokol-Protokol Web

Para pelaku menggunakan shell-shell web untuk arahan dan kawalan. Arahan-arahan shell web kemungkinannya telah melewati HTTPS dengan menggunakan server web sedia ada pada peralatan tersebut (T1572).

T1001.003 Pengobfusikasian Data: Penyamaran ajukan Protokol

Para pelaku menggunakan alat-alat peranti yang dikompromi sebagai batu loncatan untuk serangan yang direka untuk menyelinapkan diri ke dalam trafik sahih.

Saranan-Saranan Pengesanan dan Pemitigasian

ASD ACSC menyarankan dengan tegas pelaksanaan Kawalan-Kawalan Essential Eight ASD dan Strategies to Mitigate Cyber Security Incidents berkaitan. Di bawah ini ialah saranan bagi tindakan-tindakan keselamatan jaringan yang patut diambil untuk mengesan dan menghalang pencerobohan oleh APT40, diikuti pemitigasian khusus untuk empat TTP utama yang diringkaskan dalam Rajah 1.

Pengesanan

Sesetengah fail yang dikenal pasti di atas telah diletakkan ke dalam lokasi-lokasi seperti C:\Users\Public* and C:\Windows\Temp*. Lokasi-lokasi ini mungkin menjadi tempat mudah untuk menulis data kerana ia biasanya boleh ditulis dunia, iaitu, semua akaun pengguna yang didaftar dalam Windows akan mempunyai akses kepada direktori-direktori ini serta direktori-direktori kecil mereka sekali. Mana-mana pengguna sering berupaya untuk mengakses fail-fail ini kemudian daripada itu, yang membenarkan peluang bagi pergerakan lateral, pengelakan pertahanan, pelaksanaan keistimewaan-rendah dan untuk pementasan pengeksfiltrasian.

Syarat-syarat Sigma berikut cuba untuk mencari pelaksanaan daripada lokasi-lokasi yang mencurigakan sebagai petanda aktiviti tidak biasa. Dalam semua contoh ini, siasatan lanjutan diperlukan untuk mengesahkan aktiviti berniat jahat dan penentumilikan.

Tajuk: Pelaksanaan Boleh Tulis Dunia (World Writable Execution) - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Keterangan Mengesan proses pelaksanaan daripada from C:\Windows\Temp.

Latarbelakang

Syarat ini melihat khusus untuk pelaksanaan yang keluar dari C:\Windows\Temp*. Temp ini diguna dengan lebih meluas oleh aplikasi-aplikasi yang tidak berniat jahat dan oleh yang demikian merupakan satu penunjuk keyakinan berniat jahat yang lebih rendah daripada pelaksanaan yang keluar daripada direktori-direktori kecil boleh tulis dunia (world writable subdirectories) dalam C:\\Windows.

Mengeluarkan aplikasi-aplikasi yang dilaksanakan pengguna SYSTEM atau NETWORK SERVICE mengurangkan sebahagian besar jumlah aktiviti tidak berniat jahat yang dipilih dengan syarat ini.

Ini bererti bahawa syarat ini mungkin akan terlepas pandang pelaksanaan berniat jahat pada tahap keistimewaan yang lebih tinggi tetapi penggunaan syarat-syarat lain adalah disarankan untuk menentukan jika seseorang pengguna sedang cuba untuk meningkatkan keistimewaan kepada SYSTEM.

Siasatan:

1. Periksa maklumat yang dikaitkan secara langsung dengan pelaksanaan fail ini, misalnya konteks pengguna, tahap integriti pelaksanaan, aktiviti lanjutan yang berlaku serta-merta dan imej-imej yang dimuat naik oleh fail itu.
2. Siasat proses kontekstual, jaringan, fail dan data sokongan lain pada hos untuk membantu membuat penilaian sama ada aktiviti berkaitan berniat jahat.
3. Jika perlu, cuba untuk memungut satu salinan fail itu untuk dijuruterakan balik untuk menentukan sama ada ia sahih atau tidak.

Rujukan-Rujukan:

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

Pengarang: ASD's ACSC

Tarikh: 2024/06/19

Status: eksperimental

Tags:

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

Sumber Log:

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

Pengesanan:

```
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'

keadaan: temp dan tidak (common_temp_path or system_user or dismhost or known_parent)

Positif-Positif Palsu:

- Aplikasi-aplikasi pengoditan senarai yang dibenar telah diperhati menjalankan pembolehlaksana daripada Temp.
- Temp akan secara sahih mengandungi sejumlah aplikasi pemasangan (setup) dan pelepasan, jadi ia mungkin berbaloi untuk menimbangkan sejauh manakah tingkah laku ini meleluasa dalam sesebuah jaringan yang dipantau (dan sama ada ia boleh disenaraibenarkan atau tidak) sebelum syarat ini diaturgerakkan.

Tahap: rendah

Tajuk: Pelaksanaan Boleh Tulis Dunia - Non-Direktori-kecil Sistem Temp

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

Keterangan: Mengesan pelaksanaan proses daripada sebuah lokasi boleh tulis dunia di dalam sebuah direktori kecil lokasi pemasangan Windows OS.

Latarbelakang

Syarat ini melihat khusus untuk pelaksanaan yang keluar dari direktori-direktori boleh tulis dunia di dalam C:\ dan khususnya C:\Windows\T*, kecuali bagi C:\\Windows\Temp (yang diguna secara lebih meluas oleh aplikasi-aplikasi yang tidak berniat jahat dan oleh yang demikian merupakan satu penunjuk keyakinan berniat jahat yang lebih rendah).

Folder-folder AppData dikecualikan jika sebuah fail dijalankan sebagai SYSTEM – ini merupakan sebuah cara tidak berniat jahat di mana kebanyakan fail-fail aplikasi sementara dilaksanakan.

Selepas melengkapkan sebuah garis dasar jaringan permulaan dan mengenal pasti pelaksanaan tidak berniat jahat yang diketahui daripada lokasi-lokasi ini, syarat ini sepatutnya jarang terbakar.

Siasatan:

1. Periksa maklumat yang dikaitkan secara langsung dengan pelaksanaan fail ini, misalnya konteks pengguna, tahap integriti pelaksanaan, aktiviti lanjutan yang berlaku serta-merta dan imej-imej yang dimuat naik oleh fail itu.
2. Siasat proses kontekstual, jaringan, fail dan data sokongan lain pada hos untuk membantu membuat penilaian sama ada aktiviti berkaitan berniat jahat.
3. Jika perlu, cuba untuk memungut satu salinan fail itu untuk dijuruterakan balik untuk menentukan sama ada ia sahih atau tidak.

Rujukan-Rujukan:

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

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

Pengarang: ASD ACSC

Tarikh: 2024/06/19
Status: tahap eksperimental

Tag-tag:

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

Sumber log:

category: process_creation
product: windows

Pengesanan:

writable_path:

Imej|mengandungi:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'

- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Imej|mengandungi: '\\AppData\\'
Pengguna: 'SISTEM'

keadaan: writable_path and not appdata

Positif-positif palsu:

Aplikasi-aplikasi pengoditan senarai dibenarkan telah diperhati menjalankan pembolehlaksana (executables) daripada direktori-direktori ini.

Ia adalah munasabah bagi skrip-skrip dan alat-alat pentadbiran yang diguna dalam persekitaran(-persekitaran) yang dipantau mungkin ditemui di dalam salah-satu direktori-direktori ini dan patut ditangani atas dasar kes-demi-kes.

Tahap: tinggi

Tajuk: Pelaksaan Boleh Tulis Dunia – Pengguna

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

Keterangan Mengesan proses pelaksanaan daripada C:\Users\Public* dan folder boleh tulis dunia lain di dalam Users.

Latarbelakang:

Folder-folder AppData dikecualikan jika sesebuah fail dijalankan sebagai SYSTEM – ini merupakan satu cara selamat bagaimana kebanyakan fail-fail aplikasi sementara dilaksanakan:

Siasatan:

1. Periksa maklumat yang dikaitkan secara langsung dengan pelaksanaan fail ini, misalnya konteks pengguna, tahap integriti pelaksanaan, aktiviti lanjutan yang berlaku serta-merta dan imej-imej yang dimuat naik oleh fail itu.
2. Siasat proses kontekstual, jaringan, fail dan data sokongan lain pada hos untuk membantu membuat penilaian sama ada aktiviti berkaitan berniat jahat.
3. Jika perlu, cuba untuk memungut satu salinan fail itu untuk dijuruterakan balik untuk menentukan sama ada ia sahih atau tidak.

Rujukan-Rujukan:

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

Pengarang: ASD's ACSC

Tarikh: 2024/06/19

Status: eksperimental

Tags:

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

Sumber log:

kategori: process_creation
produk: windows

Pengesanan:

pengguna:

Imej|mengandungi:

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

appdata:

Imej|mengandungi: '\\AppData\\'
Pengguna: 'SYSTEM'

syarat: pengguna dan bukan appdata

Positif-positif palsu:

- Ia menjadi satu kemungkinan bahawa skrip-skrip dan peralatan pentadbiran yang diguna di dalam persekitaran(-persekitaran) yang dipantau mungkin berada di dalam khalayak awam atau direktori-kecil dan sepatutnya ditangani atas dasar kes-demi-kes.

Tahap: sederhana

Pemitigasian

Pelogan

Dalam penyiasatan ASD ACSC, satu isu lazim yang mengurangkan keberkesanan dan kepantasan usaha-usaha siasatan ini ialah ketiadaan maklumat pelogan lampau dan yang menyeluruh merentasi sejumlah kawasan termasuk log permintaan server web, log kejadian Windows dan log proksi internet.

ASD ACSC menyarankan penilaian kembali dan penerapan nasihat panduan mereka ke atas Windows Event Logging and Forwarding termasuk fail-fail pengkonfigurasian dan skrip-skrip di dalam Windows Event Logging Repository dan Buku Panduan Keselamatan Maklumat (Information Security Manual) Guidelines for System Monitoring, untuk meliputi pemusatan log dan penyimpanan log bagi satu tempoh masa yang wajar.

Pengurusan penampalan

Menampal semua alat-alat peranti dan perkhidmatan yang terdedah kepada internet dengan kadar segera, termasuk server-server web, aplikasi-aplikasi web, dan gerbang masuk akses jarak jauh. Pertimbangkan pelaksanaan sebuah sistem pengurusan penampalan secara berpusat untuk mengotomasi dan mempercepatkan proses berkaitan. ASD ACSC menyarankan pelaksanaan Guidelines for System Management ISM, khususnya, kawalan Sistem Penampalan (System Patching) di mana ia berpatutan.

Kebanyakan eksploitasi yang diguna pakai oleh pelaku diketahui secara umum dan mempunyai penampalan dan pemitigasian sedia ada. Organisasi-organisasi patut memasikan bahawa penampalan keselamatan atau pemitigasian diterapkan ke atas infrastruktur menghadap internet dalam tempoh masa 48 jam, dan sejauh mana yang boleh, menggunakan versi terkini perisian dan sistem-sistem.

Pensegmentasian jaringan

Pensegmentasian jaringan boleh menjadikannya jauh lebih sukar bagi para seteru untuk mencari dan mendapatkan akses kepada data sensitif sesebuah organisasi. Segmen jaringan untuk mengehadkan atau menyekat gerakan lateral dengan menafikan trafik antara komputer-komputer kecuali jika diperlukan. Server-server penting seperti Direktori Aktif dan server penentusahan lain sepatutnya hanya boleh ditadbir daripada sejumlah server pengantara atau 'server lompatan' ('jump servers') yang terhad. Server-server in patut dipantau dengan lebih dekat, diteguhkan dengan baik dan mengehadkan pengguna dan alat peranti mana yang boleh dihubungkan kepada mereka.

Tanpa mengira contoh-contoh yang dikenal pasti di mana pergerakan lateral adalah dihalang, pensegmentasian jaringan tambahan mungkin telah mengehadkan jumlah data yang boleh diakses dan dikeluarkan oleh para pelaku.

Pemitigasian tambahan

Pihak agensi pengarang juga menyarankan pemitigasian berikut untuk memerangi APT40 dan penggunaan pihak lain bagi TTP di bawah.

- Nyahbolehkan perkhidmatan jaringan, port-port dan protokol-protokol yang tidak diguna atau tidak diperlukan.
- Gunakan penghadang api aplikasi Web (Web application firewalls) (WAFs) yang sudah diperhalusi untuk melindungi server-server web dan aplikasi-aplikasi.
- Menguatkuasakan laluan keistimewaan yang paling rendah untuk mengehadkan akses kepada server-server, perkongsian fail, dan sumber-sumber lain.
- Gunakan penentusahan pelbagai-faktor (multi-factor authentication) (MFA) dan akaun-akaun perkhidmatan terurus untuk menjadikan kredential lebih sukar untuk diretak dan diguna kembali. MFA sepatutnya diterapkan ke atas semua perkhidmatan akses jarak jauh internet yang boleh diakses, termasuk:
  - E-mel web dan berdasarkan awan
  - Platform-platform kolaborasi
  - Hubungan jaringan maya peribadi
  - Perkhidmatan-perkhidmatan desktop jarak jauh
- Gantikan kelengkapan akhir-hayat

Rajah 1: Strategi/Teknik Pemitigasian

TTP	Lapan Strategi Pemitigasian Wajib	Kawalan-kawalan ISM
Akses Permulaan T1190 Pengeksploitasian Aplikasi Menghadap-Awam	Aplikasi penampalan Menampal sistem-sistem pengoperasian Penentusahan Pelbagai-Faktor Kawalan aplikasi	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Pelaksanaan T1059 Penafsir Arahan dan Penskripsian	Kawalan Aplikasi Hadkan makro-makro Microsoft Office Hadkan keistimewaan pentadbiran	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Keterusan T1505.003 Komponen Perisian Server: Shell Web	Kawalan aplikasi Hadkan keistimewaan pentadbiran	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Akses Permulaan / Mengistimewakan Pendadakan / Keterusan T1078 Akaun-akaun Sah	Penampalan sistem-sistem pengoperasian Penentusahan Pelbagai-Faktor Hadkan keistimewaan pentadbiran Kawalan aplikasi Pengerasan aplikasi pengguna	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

Bagi nasihat pengesanan dan pemitigasian umum tambahan, sila rujuk seksyen-seksyen Mitigations and Detection pada laman web teknik MITRE ATT&CK bagi setiap teknik yang dikenal pasti dalam ringkasan MITRE ATT&CK pada penghujung panduan nasihat ini.

Penafian

Maklumat yang terkandung di dalam laporan ini disediakan "seadanya" untuk tujuan pemberian maklumat sahaja. Agensi-agensi pengarang tidak mengendors mana-mana entiti komersial, produk, syarikat, atau perkhidmatan, termasuk mana-mana entiti, produk, atau perkhidmatan yang dipautkan di dalam dokumen ini. Sebarang rujukan kepada entiti-entiti komersil, produk-produk, proses-proses, atau perkhidmatan-perkhidmatan khusus dengan tanda perkhidmatan, tanda dagang, pengeluar, atau sebaliknya, tidak bererti atau menunjukkan pengendorsan, saranan, atau sokongan kelebihan oleh pihak agensi pengarang.

Dokumen ini ditanda TLP:CLEAR. Pendedahan tidak dihadkan. Sumber-sumber boleh menggunakan TLP:CLEAR bila maklumat berkaitan membawa risiko minimum atau tidak akan dijangka, bertepatan dengan peraturan-peraturan yang terpakai dan prosedur-prosedur bagi edaran awam. Tertakluk kepada peraturan-peraturan hakcipta standard, maklumat TLP:CLEAR mungkin boleh diedar tanpa had. Untuk maklumat lanjut mengenai Traffic Light Protocol, lihat cisa.gov/tlp

MITRE ATT&CK – Kemahiran Dagang Lampau Terpilih APT40

Peninjauan (TA0043)	
Cari Laman Web Yang Dimiliki-Mangsa (T1594)	Kumpulan Maklumat Identiti Mangsa: Kredential-kredential (T1589.001)
Pengimbasan Aktif: Pengimbasan Kerentanan (T1595.002)	Kumpulkan Maklumat Hos Mangsa (T1592)
Mencari Laman Web/Domain-domain Terbuka: Enjin Carian (T1593.002)	Kumpulkan Maklumat Jaringan Mangsa: Sifat-Sifat Domain (T1590.001)
Kumpulkan Maklumat Identiti Mangsa: Alamat-alamat e-Mel (T1589.002)	

Pembangunan Sumber (TA0042)	
Perolehi Infrastruktur: Domain-domain (T1583.001)	Perolehi Infrastruktur (T1583)
Perolehi Infrastruktur: Server DNS (T1583.002)	Kompromikan Akaun-Akaun (T1586)
Membangunkan Keupayaan: Sijil-Sijil Penandaan Kod (T1587.002)	Kompromikan Infrastruktur (T1584)
Membangunkan keupayaan: Sijil-Sijil Digital (T1587.003)	Membangunkan Keupayaan: Malware (T1587.001)
Perolehi Keupayaan: Sijil-Sijil Penandaan Kod (T1588.003)	Menubuhkan Akaun-akaun: Akaun-Akaun Awan (T1585.003)
Kompromikan Infrastruktur: Alat-Alat Peranti Jaringan (T1584.008)	Perolehi Keupayaan: Sijil-Sijil Digital (T1588.004)

Akses Permulaan (TA0001)	
Akaun-Akaun Sahih (T1078)	Pancingan (T1566)
Akaun-Akaun Sahih: Akaun-Akaun Lalai (T1078.001)	Pancingan: Lampiran Pancingan Serampang (T1566.001)
Akaun-Akaun Sahih: Akaun-Akaun Domain (T1078.002)	Pancingan: Pautan Pancingan Serampang (T1566.002)
Perkhidmatan-Perkhidmatan Jarak Jauh Luaran (T1133)	Eksploitasikan Aplikasi Menghadap-Awam (T1190)
Kompromi Pandu-Lalu (T1189)	

Pelaksanaan (TA0002)	
Penginstrumentasian Pengurusan Windows (T1047)	Jurutafsir Arahan dan Penskripsian: Python (T1059.006)
Tugas/Kerja Terjadual: At (T1053.002)	Jurutafsir Arahan dan Penskripsian: JavaScript (T1059.007)
Tugas/Kerja Terjadual: Tugas Terjadual: (T1053.005)	API Asal (T1106)
Jurutafsir Arahan dan Penskripsian (T1059)	Komunikasi Inter-Proses (T1559)
Jurutafsir Arahan dan Penskripsian: Shell Arahan Windows (T1059.003)	Perkhidmatan-Perkhidmatan Sistem: Pelaksanaan Perkhidmatan (T1569.002)
Jurutafsir Arahan dan Penskripsian: ShellKuasa (T1059.001)	Pengeksploitasian untuk Pelaksanaan Pelanggan (T1203)
Jurutafsir Arahan dan Penskripsian: Dasar Visual (T1059.005)	Pelaksanaan oleh Pengguna: Fail Berniat Jahat (T1204.002)
Jurutafsir Arahan dan Penskripsian:: Shell Unix (T1059.004)	Jurutafsir Arahan dan Penskripsian: Skrip Apple(T1059.002)
Tugas/Kerja Terjadual: Cron (T1053.003)	Peralatan Peraturgerakkan Perisian (T1072)

Keterusan (TA0003)	
Akaun-Akaun Sahih (T1078)	Komponen Perisian Server: Shell Web (T1505.003)
Pemula Aplikasi Office: Makro-Makro Templat Office (T1137.001)	Proses Sistem Cipta atau Gubah: Perkhidmatan Windows (T1543.003)
Tugas/Kerja Terjadual: At (T1053.002)	Pelaksanaan Pemula-Auto Boot atau Daftar Masuk: Kekunci Untuk Menjalankan Daftar / Folder Pemula (T1547.001)
Tugas/Kerja Terjadual: Tugas Terjadual (T1053.005)	Pelaksanaan Pemula-Auto Boot atau Daftar Masuk: Pemodifikasian Jalan Pintas (T1547.009)
Perkhidmatan-Perkhidmatan Jarak Jauh Luaran (T1133)	Aliran Pelaksanaan Rampasan: Rampasan Arahan Carian DLL (T1574.001)
Tugas/Kerja Terjadual: Cron (T1053.003)	Aliran Pelaksanaan Perampasan: Pemuatan-Sisi DLL (T1574.002)
Manipulasi Akaun (T1098)	Akaun-Akaun Sahih: Akaun-Akaun Awan (T1078.004)
Akaun-Akaun Sahih: Akaun-Akaun Domain (T1078.002)	

Pendadakan Keistimewaan (TA0004)	
Tugas/Kerja Terjadual: At (T1053.002)	Proses Wujud atau Modifikasi Sistem: Perkhidmatan Windows (T1543.003)
Tugas/Kerja Terjadual: Tugas Terjadual (T1053.005)	Boot or Logon Autostart Execution: Kekunci Untuk Menjalankan Daftar / Folder Pemula (T1547.001)
Suntikan Proses: Rampasan Pelaksanaan Bebenang (T1055.003)	Pelaksanaan Pemula-Auto Boot atau Daftar Masuk: Pemodifikasian Jalan Pintas (T1547.009)
Suntikan Proses: Pengosongan Proses (T1055.012)	Aliran Pelaksanaan Rampasan: Rampasan Arahan Carian DLL (T1574.001)

Pendadakan Keistimewaan (TA0004)	
Akaun-Akaun Sahih: Akaun-Akaun Domain (T1078.002)	Pengeksploitasian untuk Pendadakan Keistimewaan (T1068)
Pemanipulasian Token Akses: Kecurian/Penyamaran Ajukan Token (T1134.001)	Pelaksanaan Cetusan Peristiwa: Pemodifikasian Pengkonfigurasian Shell Unix (T1546.004)
Suntikan Proses: Suntikan Perpustakaan Pautan-Dinamik (T1055.001)	Akaun-Akaun Sahih: Akaun-Akaun Domain (T1078.002)
Akaun-Akaun Sahih: Akaun-Akaun Lokal (T1078.003)	

Pengelakkan Pertahanan (TA0005)	
Rootkit (T1014)	Pelaksanaan Arahan Tidak Langsung (T1202)
Fail-Fail atau Maklumat Yang Diobfusikasikan (T1027)	Pelaksanaan Proksi Binari Sistem: Mshta (T1218.005)
Fail-fail atau Maklumat yang Diobfusikasikan: Pembungkusan Perisian (T1027.002)	Pelaksanaan Proksi Sistem Binari: Regsvr32 (T1218.010)
Fail-fail atau Maklumat yang Diobfusikasikan: Steganografi (T1027.003)	Melemahkan Kawalan Keyakinan: Penandaan Kod (T1553.002)
Fail-fail atau Maklumat yang Diobfusikasikan: Pengumpulan Selepas Penghantaran (T1027.004)	Pemodifikasian Kebenaran Fail dan Direktori: Pemodifikasian Kebenaran Fail dan Direktori Linux dan Fail Mac (T1222.002)
Penyamaran Ajukan: Padanan Nama atau Lokasi Sahih (T1036.005)	Pengelakkan Pemvisualisasian/Sandbox: Pemeriksaan Sistem (T1497.001)
Suntikan Proses: Perampasan Pelaksanaan Bebenang (T1055.003)	Penyamaran Ajukan (T1036)
Memuatkan Kod Pembalikan (T1620)	Merosakkan Pertahanan: Menyahbolehkan atau Merubah Sistem Penghadang Api (T1562.004)
Suntikan Proses: Pengosongan Proses (T1055.012)	Menyembunyi Artifak: Fail-Fail dan Direktori-Direktori Tersembunyi (T1564.001)
Pembuangan Petunjuk: Pemadaman Fail (T1070.004)	Menyembunyi Artifak: Tingkap Tersembunyi (T1564.003)
Pembuangan Petunjuk: Timestomp (T1070.006)	Merampas Aliran Pelaksanaan: Perampasan Arahan Carian DLL (T1574.001)
Pembuangan Petunjuk: Padamkan Log-Log Kejadian Windows (T1070.001)	Merampas Aliran Pelaksanaan: Muat naik-sisian DLL (T1574.002)
Merubah Daftar (T1112)	Perkhidmatan Web (T1102)
Menyahobfukasi/Nyahkod Fail-Fail atau Maklumat (T1140)	Penyamaran Ajukan: Tugas Penyamaran Ajukan atau Perkhidmatan (T1036.004)
Menggugat Pertahanan (T1562)	

Credential Access (TA0006)	
OS Credential Dumping: Memori LSASS (T1003.001)	Kredential-kredential Tidak Teguh: Kredential-kredential dalam Fail-Fail (T1552.001)
Pembuangan Kredential OS: NTDS (T1003.003)	Kuasa Ganas: Meneka Kata Laluan (T1110.001)
Penghiduan Jaringan (T1040)	Penentusahan Yang Dipaksa (T1187)

Credential Access (TA0006)	
Kredential-kredential daripada Stor-Stor Kata Laluan: Rantaiankunci (T1555.001)	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
Tangkapan Masukan: Pelogan kekunci (T1056.001)	Pemintasan Penentusahan Pelbagai-Faktor (T1111)
Mencuri Cookie Sesi Web (T1539)	Mencuri Token Akses Aplikasi (T1528)
Pengeksplotasian untuk Akses Kredential (T1212)	Kuasa Ganas: Pemecahan Kata Laluan (T1110.002)
Penangkapan Masukan: Penangkapan Portal Web (T1056.003)	Pembuangan Kredential OS: DCSync (T1003.006)
Kredential-kredential daripada Stor-Stor Kata Laluan (T1555)	Kredential-kredential daripada Stor-Stor Kata Laluan: Kredential-kredential daripada Pelayar-Pelayar Web (T1555.003)

Penemuan (TA0007)	
Penemuan Perkhidmatan Sistem (T1007)	Penemuan Perkhidmatan Sistem (T1082)
Penemuan Aplikasi Window (T1010)	Penemuan akaun: Akaun lokal (T1087.001)
Daftar Pertanyaan (T1012)	System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®
Penemuan Fail dan Direktori (T1083)	Penemuan Masa Sistem (T1124)
Penemuan Perkhidmatan Jaringan (T1046)	Penemuan Pemilik/Pengguna Sistem (T1033)
Penemuan Sistem Jarak Jauh (T1018)	Penemuan Amanah Domain (T1482)
Penemuan Akaun: Akaun e-Mel (T1087.003)	Penemuan Akaun: Akaun Domain (T1087.002)
Penemuan Hubungan Jaringan Sistem (T1049)	Pengelakkan Pemayaan (Virtualisation)/Sandbox: Pemeriksaan Sistem (T1497.001)
Penemuan Proses (T1057)	Penemuan Perisian (T1518)
Penemuan Kebenaran Kumpulan: Kumpulan Domain (T1069.002)	Network Share Discovery, Technique T1135 - Enterprise | MITRE ATT&CK®
Penemuan Pengkonfigurasian Jaringan Sistem: Penemuan Hubungan Internet (T1016.001)	

Pergerakan Lateral (TA0008)	
Perkhidmatan Jarak Jauh: Protokol Atas Meja Jarak Jauh (T1021.001)	Perkhidmatan Jarak Jauh (T1021)
Perkhidmatan Jarak Jauh: Perkongisan SMB/Windows Admin (T1021.002)	Gunakan Bahan Penentusahan Alternat: Pass the Ticket (T1550.003)
Perkhidmatan Jarak Jauh: Pengurusan Jarak Jauh Windows (T1021.006)	Penghantaran Alat Lateral (T1570)

Pengumpulan (TA0009)	
Data daripada Sistem Lokal (T1005)	Data Arkib Terkumpul: Perpustakaan menerusi Arkib (T1560.002)
Data daripada Drive Jaringan Berkongsi (T1039)	Pengumpulan e-Mel: Pengumpulan e-Mel Jarak Jauh (T1114.002)

Pengumpulan (TA0009)	
Tangkapan Masukan: Pelogan kunci (T1056.001)	Data Papan Klip (T1115)
Koleksi Yang Diotomasi (T1119)	Data daripada Repositori Maklumat (T1213)
Tangkapan Masukan: Tangkapan Portal Web (T1056.003)	Data Dipentaskan: Pementasan Data Jarak Jauh (T1074.002)
Data Dipentaskan: Pementasan Data Lokal (T1074.001)	Pengarkiban Data Terkumpul (T1560)
Pengumpulan e-Mel (T1114)	

Pengeksfiltrasian (TA0010)	
Pengekfiltrasian Melalui Saluran C2 (T1041)	Pengekfiltrasian Melalui Protokol Alternatif: Pengekfiltrasian Melalui Protokol Bukan-CS Yang Dienkripsi dan Tidak Sepadan (T1048.002)
Pengekfiltrasian Melalui Protokol Alternatif (T1048)	Pengekfiltrasian Melalui Perkhidmatan Web: Pengekfiltrasian ke Penyimpanan Awan (T1567.002)

Arahan dan Kawalan (TA0011)	
Pengobfusikasian Data: Penyamaran Protokol (T1001.003)	Perkhidmatan Web: Dead Drop Resolver (T1102.001)
Port Yang Lazim Diguna (T1043)	Perkhidmatan Web: Komunikasi Sehala (T1102.003)
Protokol Lapisan Aplikasi: Protokol-Protokol Web (T1071.001)	Penghantaran Alat Ingres (T1105)
Protokol Lapisan Aplikasi: Protokol Penghantaran Fail (T1071.002)	Proksi: Proksi Dalaman (T1090.001)
Proksi: Proksi Luaran (T1090.002)	Port Bukan-Standard (T1571)
Proksi: Proksi pelbagai-loncatan (T1090.003)	Penerowongan Protokol (T1572)
Web Service: Komunikasi dwi-arah (T1102.002)	Saluran Yang Dienkripsikan (T1573)
Saluran Yang Dienkripsikan: Kriptografi Tidak Sepadan (T1573.002)	Penghantaran Alat Kemasukan (T1105)
Proksi, Teknik T1090 - Perusahaan | MITRE ATT&CK®	

Impak (TA0040)	
Hentian Perkhidmatan (T1489)	Pemadaman Cakera (T1561)
Penutupan Sistem/Reboot (T1529)	Rampasan Sumber (T1496)

Nota

Penafian

Bahan di dalam panduan ini adalah bersifat umum dan tidak harus dianggap sebagai nasihat perundangan atau digantung sebagai bantuan dalam apa-apa keadaan atau kecemasan tertentu. Dalam sebarang hal mustahak, anda harus mendapatkan nasihat profesional bebas tentang apa yang anda sedang alami sendiri.

Pihak Komanwel tidak menerima tanggungjawab atau tanggungan ke atas sebarang kerosakan, kerugian atau perbelanjaan yang ditanggung akibat daripada pergantungan kepada maklumat yang terkandung dalam panduan ini.

Untuk maklumat lanjut, atau untuk melaporkan sebuah kejadian keselamatan siber, sila hubungi kami:

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

Nombor ini tersedia untuk digunakan di dalam Australia sahaja.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre