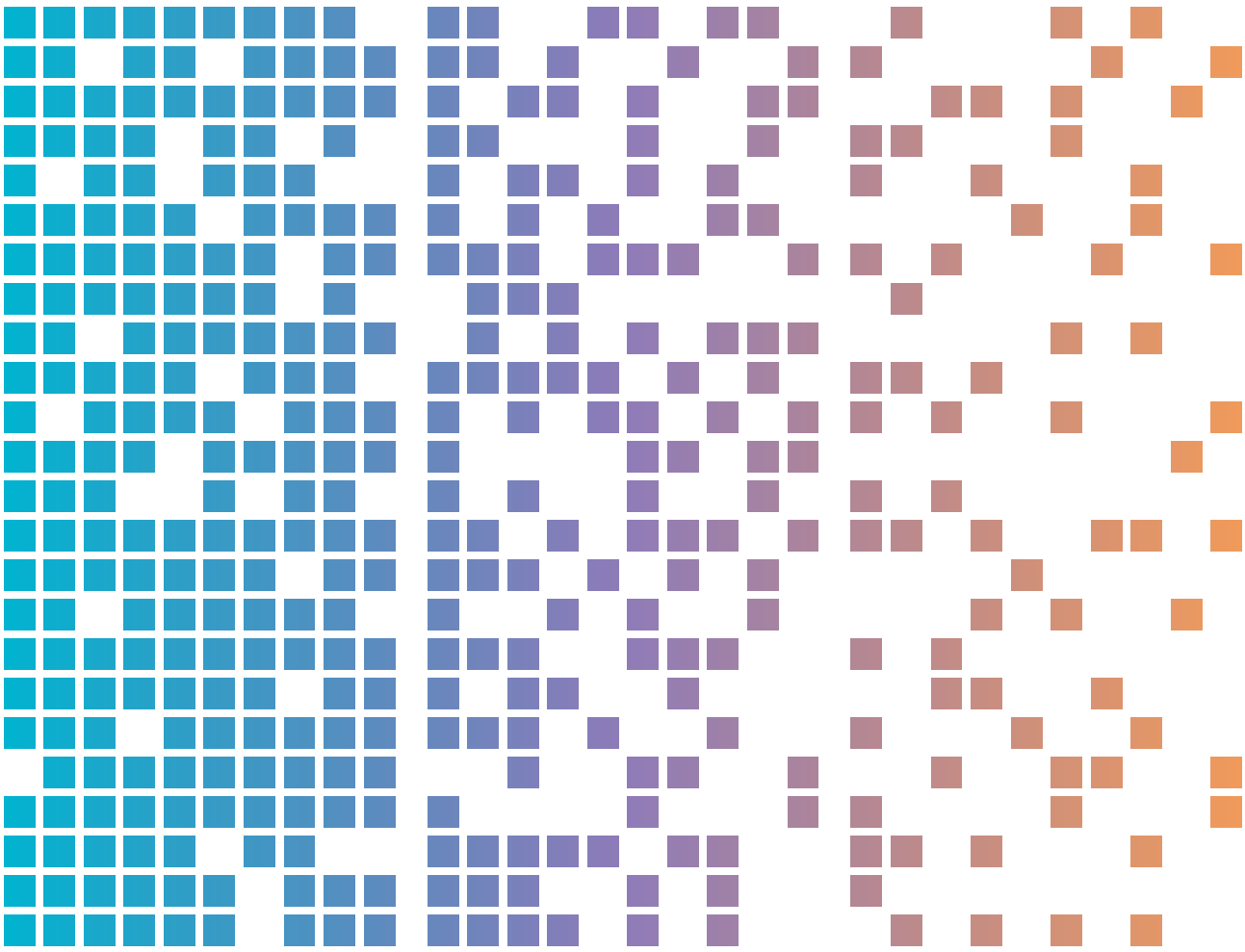
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Rompakan sepi: penjenayah siber menggunakan malware pencuri maklumat untuk mengkompromikan jaringan-jaringan korporat



Kerumitan kandungan
SEDERHANA

Isi Kandungan

Konteks

Malware pencuri maklumat mencuri kredential pengguna dan maklumat sistem yang dieksploitasi penjenayah siber, khususnya untuk meraut keuntungan kewangan. Pencuri maklumat telah diperhati dalam serangan penjenayah siber terhadap pelbagai organisasi dan sektor di seluruh dunia, termasuk Australia. Penerbitan ini memberikan para pembaca panduan keselamatan siber mengenai malware pencuri maklumat, termasuk aktiviti ancaman dan nasihat pemitigasian bagi organisasi-organisasi dan para pekerja mereka.

Perkara utama

- Malware pencuri maklumat, yang juga dikenali sebagai pencuri info, ialah sejenis malware yang direkabentuk untuk mengumpulkan maklumat daripada alat peranti seseorang mangsa. Ini boleh meliputi nama dan kata laluan pengguna, butir-butir kad kredit, dompet matawang kripto, fail-fail lokal, dan data pelayar termasuk cookies, sejarah pengguna dan butir-butir pengisian auto borang.
- Penjenayah mungkin akan berusaha untuk membeli dan menggunakan kredential pengguna yang telah dicuri yang berkaitan dengan akaun-akaun korporat untuk mendapatkan akses awal kepada alat-alat peranti majikan mangsa, para pelanggan mereka selain sistem-sistem perusahaan yang lain. Impak selanjutnya ke atas organisasi-organisasi ini boleh meliputi ransomware, peras ugut, pengkompromian e-mel perniagaan dan kecurian harta intelek.
- Pusat Keselamatan Siber Australia Direktorat Semboyan Australia (The Australian Signals Directorate's Australian Cyber Security Centre (ASD ACSC) telah mengenalpasti pencerobohan jaringan korporat yang disebabkan para pekerjanya mengakses sumber-sumber kerja daripada alat-alat peranti peribadi yang telah dikompromi. Dalam pelbagai contoh berganda, penjenayah siber telah mendapat akses awal kepada jaringan korporat dengan menggunakan kredential pengguna sah yang telah dicuri. Siasatan kami menunjukkan bahawa pengkompromian yang meleluasa biasanya terjadi selepas penjenayah siber berjaya mengakses akaun-akaun pengguna yang diberi laluan istimewa.
- Organisasi yang menyelaraskan para pekerja, kontraktor, penyedia perkhidmatan terurus atau entiti-entiti lain untuk mengakses jaringan mereka dari jarak jauh, termasuk perkakasan Bring Your Own Device (BYOD), perlu berwaspada akan risiko pencuri info dan melindungi diri mereka sendiri daripada ancaman ini. Penjenayah siber mengaturgerakkan pencuri info ke alat-alat peranti mangsa dengan menggunakan pelbagai teknik, termasuk e-mel pancingan (phishing), perisian cetak rompak yang dimuat turun, teknik-teknik pengoptimasian enjin carian (SEO), iklan berniat jahat atau pautan berniat jaha yang dihantar pada platform-platform media sosial. Pada umumnya, alat-alat peranti yang diguna buat kedua-dua tujuan kerja dan peribadi berisiko lebih tinggi untuk dijangkiti melalui teknik-teknik ini disebabkan tingkah laku pengguna dan kawalan keselamatan yang direndahkan.
- Pencuri info menawarkan model menarik kepada penjenayah siber untuk penjanaan wang daripada aktiviti jenayah siber, khususnya bagi penjenayah tahap-mula masuk dan mereka yang mempunyai kecekapan teknikal yang terhad. Sesetengah penjenayah siber akan memasarkan produk-produk pencuri info di bawah sebuah program bergaya Malware-as-a-service (MaaS), dengan mengenakan yuran langganan bulanan bagi kegunaannya.

Latarbelakang

Penggunaan pencuri info oleh penjenayah siber merupakan sebuah ancaman kepada keselamatan dan kesejahteraan organisasi-organisasi Australia. Jangkitan pencuri info biasanya muncul sebagai aktiviti langkah pemula kepada insiden-insiden keselamatan siber besar, kerana penjenayah siber menggunakan mereka untuk memungut kredential-kredential pengguna. Kredential-kredential pengguna ini, khususnya yang menyampaikan akses kepada perkhidmatan jarak jauh yang menghadap-internet atau akaun-akaun dengan laluan istimewa, kemudian dieksploitasi untuk membenarkan akses pemula kepada sistem-sistem dan data korporat.

Nota: Para broker akses pemula memainkan peranan khas di dalam sistem-eko jenayah siber dengan membeli dan menentusahkan kredential-kredential pengguna yang telah dicuri. Mereka kemudian akan melelong kredential-kredential pengguna yang bermutu tinggi, bagi persekitaran korporat yang sangat dicari, kepada penjenayah siber yang akan menggunakan kredential-kredential pengguna itu untuk mengeksploitasikan jaringan korporat organisasi tersebut.

Kredential-kredential pengguna sah yang dicuri sangat berharga kepada penjenayah siber, kerana ia akan mempercepatkan akses pemula kepada jaringan-jaringan korporat dan sistem-sistem perusahaan. Dengan kredential-kredential pengguna sah yang dicuri, penjenayah siber boleh memintas lalu beberapa taktik dan teknik lazim, termasuk:

- mengenal pasti dan menyelidik sesuatu sasaran
- memperhalusi jaringan sasaran untuk kelemahan
- membangunkan vektor-vektor untuk akses pemula, misalnya:
  - material pancingan
  - pengeksploitasian kelemahan-kelemahan perisian
  - menyasarkan perkhidmatan jarak jauh, termasuk Remote Desktop Protocol (RDP) atau perkhidmatan virtual private network (VPN).
  - serangan keras dan ganas terhadap kredential pengguna (meneka kata laluan)

Langkah-langkah ini memerlukan pelaburan masa dan tahap kecekapan teknikal yang merupakan halangan bagi sesetengah penjenayah siber. Khususnya, penjenayah siber yang tidak berupaya untuk menembusi pertahanan jaringan korporat boleh memanfaatkan secara langsung daripada jangkitan pencuri info, kerana jangkitan ini boleh menyampaikan akses kredential pengguna pantas dan mudah kepada jaringan-jaringan korporat yang diingini.

Dalam pengesetan kerja jarak jauh, sesetengah pengguna menggunakan alat peranti peribadi bagi bagi melayari internet buat tujuan kerja dan peribadi. Dengan berbuat demikian, para pekerja mungkin memilih untuk menyimpan kredential-kredential pengguna mereka di dalam stor kata laluan pelayar web atau sambungannya (extensions), atau mereka mungkin akan menggunakan ciri-ciri pengisian auto dalam pelayar web. Pencuri info akan menyasarkan stor-stor kata laluan, beserta cookies penentusahan dan data peribadi lain di dalam pelayar web tersebut.

Berbeza daripada alat-alat peranti korporat, alat-alat peranti peribadi tidak senantiasa memiliki dasar-dasar keselamatan perusahaan yang dikuatkuasakan, yang menyampaikan risiko lebih tinggi kepada organisasi-organisasi. Contohnya, para pekerja mungkin terlibat dalam aktiviti-aktiviti, seperti memuat turunkan perisian cetak rompak dan melayari dalam talian secara berisiko-tinggi, yang meningkatkan pendedahan mereka kepada ancaman siber dan jangkitan malware.

Pencuri info, pengedar, broker akses awal and rakan sekutu ransomware kini membentuk bahagian teras sistem-eko jenayah siber yang dipacu keuntungan kewangan. Sistem-eko ini akan membangun dengan lebih cekap apabila penjenayah siber mengkhusus dan membangunkan keupayaan yang menyasarkan tahap-tahap tertentu bagi sesuatu serangan, dan kemudian menjual keupayaan itu sebagai satu perkhidmatan kepada para rakan sekutu penjenayah lain.

Aktiviti ancaman

ASD ACSC sedang menjejak dan memantau peningkatan dalam aktiviti pencuri info secara global, yang merupakan sebuah ancaman yang semakin membesar kepada jaringan-jaringan Australia. Laporan industri menunjukkan bahawa pencuri info merupakan varian malware paling popular daripada keseluruhan aktiviti jenayah siber sepanjangan 2023. Jumlah data dicuri untuk jualan yang semakin meningkat dalam tempat pasaran web haram, dan satu peningkatan dalam aktiviti broker akses pemula yang mengumpilkan (leveraging) data ini, mencerminkan trend yang meningkat ini, yang telah dipercepatkan dalam 2024.

Sistem-eko pencuri maklumat

Tahap 1: Memperolehi malware

Pencuri info biasanya ditawarkan, dalam tempat pasaran penjenayah siber, sebagai MaaS atau Stealer-as-a-Service, atau dijual sebagai kod sumber (source code). MaaS merujuk kepada sebuah model perniagaan di mana seseorang pembangun malware menjual langganan kepada perisian berniat jahat mereka kepada para individu melalui sebuah platform berdasarkan-web, serupa dengan penawaran Software-as-a-Service yang sahih. Model MaaS telah menurunkan halangan kemasukan bagi penjenayah siber, kerana ia membenarkan para individu yang tidak memiliki kemahiran teknikal meluas untuk mengedar malware dan memungut maklumat yang dicuri untuk digunakan dalam serangan siber.

Pencuri info yang ditawarkan sebagai MaaS umumnya diiklankan dengan kadar yuran bulanan yang agak murah, dan menyampaikan penjenayah siber dengan akses kepada dashboard seseorang pencuri info. Dashboard tersebut memudahkan penciptaan malware pencuri info, menyusun data yang dicuri dan menjejaki bilangan sistem yang telah dikompromi. Pengusaha MaaS menawarkan ciri-ciri pengemaskinian, peralatan dan sokongan teknikal untuk mengelakkan pengesanan oleh perisian anti-virus dan untuk menarik dan mengekalkan minat pelanggan. Ramai pencuri info mempunyai keupayaan untuk memadamkan diri mereka sendiri daripada alat peranti mangsa selepas pengeksfiltrasi data dilakukan.

Tahap 2: Pengedaran

Penjenayah siber yang mengedarkan pencuri info dan memungut maklumat daripada alat-alat peranti yang dikompromi adalah dikenali sebagai ‘Traffers’ (pengedar trafik). Traffers mengarahkan mangsa ke pautan berniat jahat, yang memudahkan penyebaran pencuri info sebagai sebahagian daripada kempen yang lebih meluas. Kebanyakan kempen tidak mendiskriminasi, dan bergantung kepada jangkitan yang mengambil kesempatan. Namun begitu, sesetengah kempen dibentuk khusus bagi industri-industri tertentu dan melibatkan pancingan-serampang (spear-phishing) tersasar terhadap mangsa-mangsa tertentu. Traffers melaksanakan kempen-kempen lebih tersasar ini sebagai respons kepada permintaan pelanggan; contohnya, di mana pembeli sedang mencari akses kepada organisasi-organisasi atau sektor-sektor bernilai tinggi yang khusus.

Traffers akan mengaturgerakkan pencuri info ke alat-alat peranti mangsa dengan menggunakan pelbagai rupa teknik, termasuk:

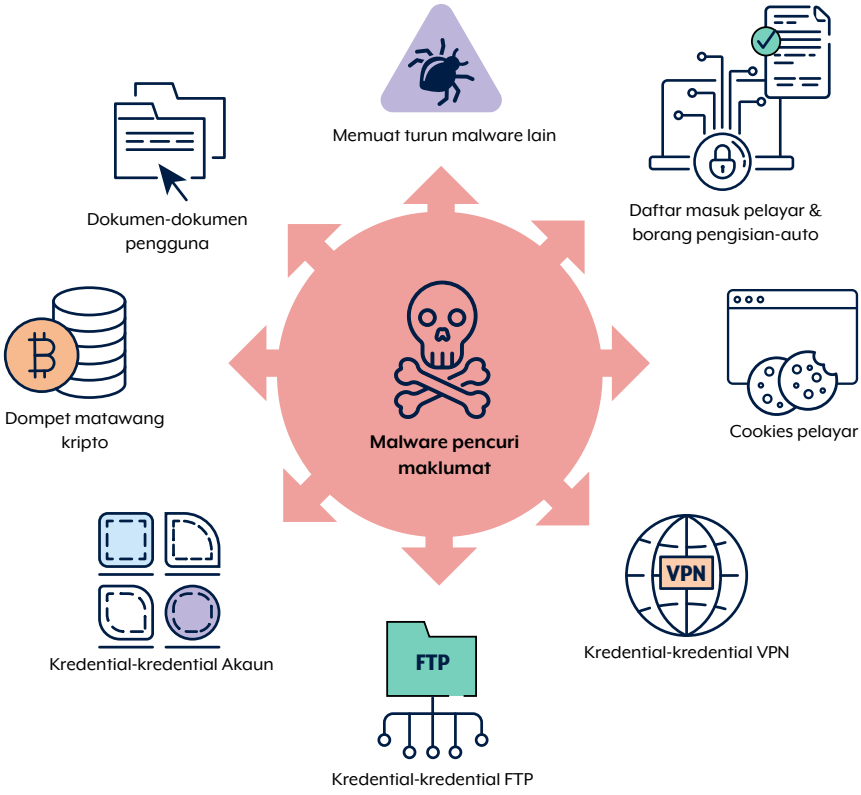
- **botnet**: jaringan sistem-sistem komputer yang telah dikompromi yang dikawal oleh penjenayah siber untuk menjalankan tindakan berniat jahat yang terbuka, misalnya menghantar pesanan pancingan atau malware

- **pancingan (phishing)**: cubaan untuk mendapatkan maklumat sensitif melalui penipuan, termasuk menerusi e-mel atau pesanan terus pada media sosial, forum-forum dan app-app pesanan, yang merupakan kaedah pengedaran biasa yang telah menurunkan halangan bagi kemasukan untuk penjenayah siber:
  - Pesanan-pesanan ini biasanya mengandungi pautan berniat jahat, dan bukannya dengan melampirkan fail-fail berniat jahat kepada e-mel itu sendiri.
- **hasil carian berniat jahat** : disampaikan menerusi teknik-teknik pengoptimasian enjin carian (SEO) yang mengarahkan sasaran ke laman-laman web yang melayani malware yang disamarkan sebagai perisian sahih atau kandungan lain
- **malvertising**: penggunaan kod yang memudaratkan, yang disuntik ke dalam iklan-iklan dalam talian sahih, untuk mengedar malware
- **perisian yang telah retak atau dicetak rompak**: bahan yang dimuat turun, termasuk permainan video, yang dikongsi menerusi video-video YouTube, dengan pautan berniat jahat ke dalam deskripsi atau komen-komen video tersebut, atau daripada laman-laman muat turun yang tidak boleh dipercayai**.**
- **iklan dan hantaran media sosial**: mengarahkan sasaran kepada fail-fail malware yang disamarkan
- **pengemaskinian perisian berniat jahat**: biasanya disamarkan sebagai pengemaskinian pelayar web

Tahap 3: Penuaian data

Setelah seseorang pencuri info melaksanakan kegiatannya pada alat peranti mangsa, ia akan mula memungut data sensitif daripada mesin yang dikompromi. Selain mencuri kredential-kredential pengguna, dalam kes di mana pencuri info ialah sebahagian daripada sebuah botnet, penjenayah siber boleh mengawal alat peranti yang dikompromi secara jarak jauh dengan menghantar arahan penkonfigurasian untuk mengaktifkan keupayaan tambahan atau untuk mengirim malware lain. Umumnya, pencuri info berupaya mencuri:

- nama dan kata laluan pengguna, khususnya yang disimpan dalam sesi / token penentusahan pelbagai-faktor (multi-factor authentication) (MFA) pelayar web pengguna.
- cookies penentusahan
- maklumat borang pengisian auto pelayar web
- kredential-kredential e-mel, kandungan atau kontak
- sejarah layaran web
- dokumen-dokumen pengguna
- butir-butir kad kredit
- log-log perbualan daripada app-app pesanan desktop
- maklumat sistem
- dompet-dompet matawang kripto
- Kredential-kredential VPN atau File Transfer Protocol (FTP).



Rajah 1. Keupayaan pencuri info

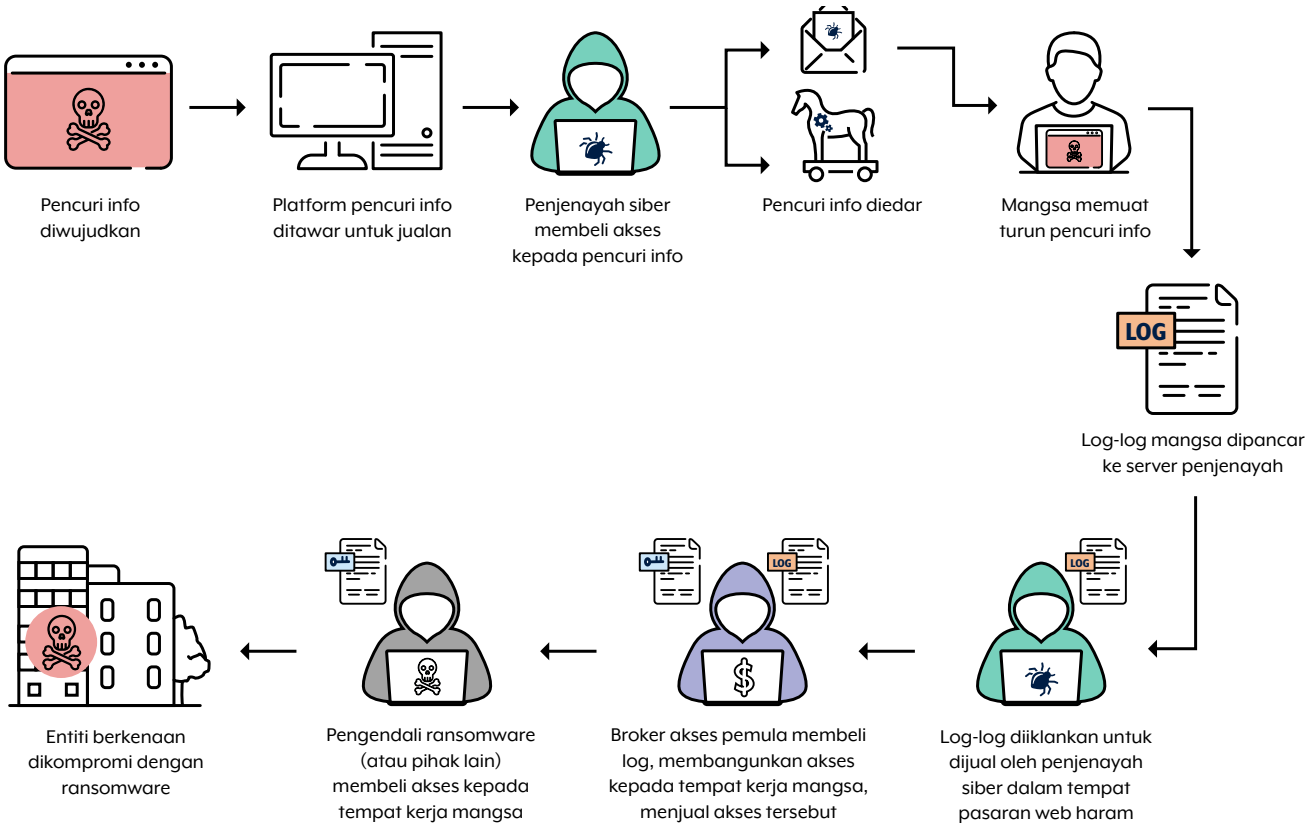
Sesetengah cookies penentusahan pelayar web akan memastikan seorang pengguna kekal berdaftar masuk ke dalam sesebuah akaun atau perkhidmatan bagi tempoh masa selama berhari-hari lamanya setiap kali, supaya pengguna tersebut tidak perlu ditentusahkan kembali. Jika ia dicuri, cookies penentusahan ini boleh memintas keperluan MFA secara efektif dan menyampaikan penjenayah siber akses ke dalam akaun-akaun mangsa, jaringan-jaringan korporat dan sistem-sistem perusahaan.

Tahap 4: Pengaggretan dan pengewangan data

Pencuri info dikonfigurasi untuk mengeksfiltrasikan maklumat mangsa, yang dikenali sebagai 'log', ke server-server arah-dan-kawal (command-and-control) berniat jahat. Umumnya, pencuri info akan mengumpilkan app-app pesanan popular, misalnya Telegram dan Discord, untuk mengongsi suapan log dengan penjenayah siber.

Tempat pasaran khusus wujud pada Telegram dan di seluruh web haram bagi penjualan dan dagangan log. Penjenayah siber mengewangkan log dalam pelbagai cara, termasuk:

- Menjual log dalam tempat pasaran jenayah, termasuk kepada broker akses pemula.
- mengeksploitasikan mangsa secara langsung, menerusi pencurian identiti dan pemerasan
- Pengumpilan maklumat bagi akses pemula ke jaringan-jaringan korporat bagi aktiviti ransomware.



Rajah 2. Sistem-eko pencuri info dan kemungkinan kesannya ke atas sebuah organisasi

Implikasi

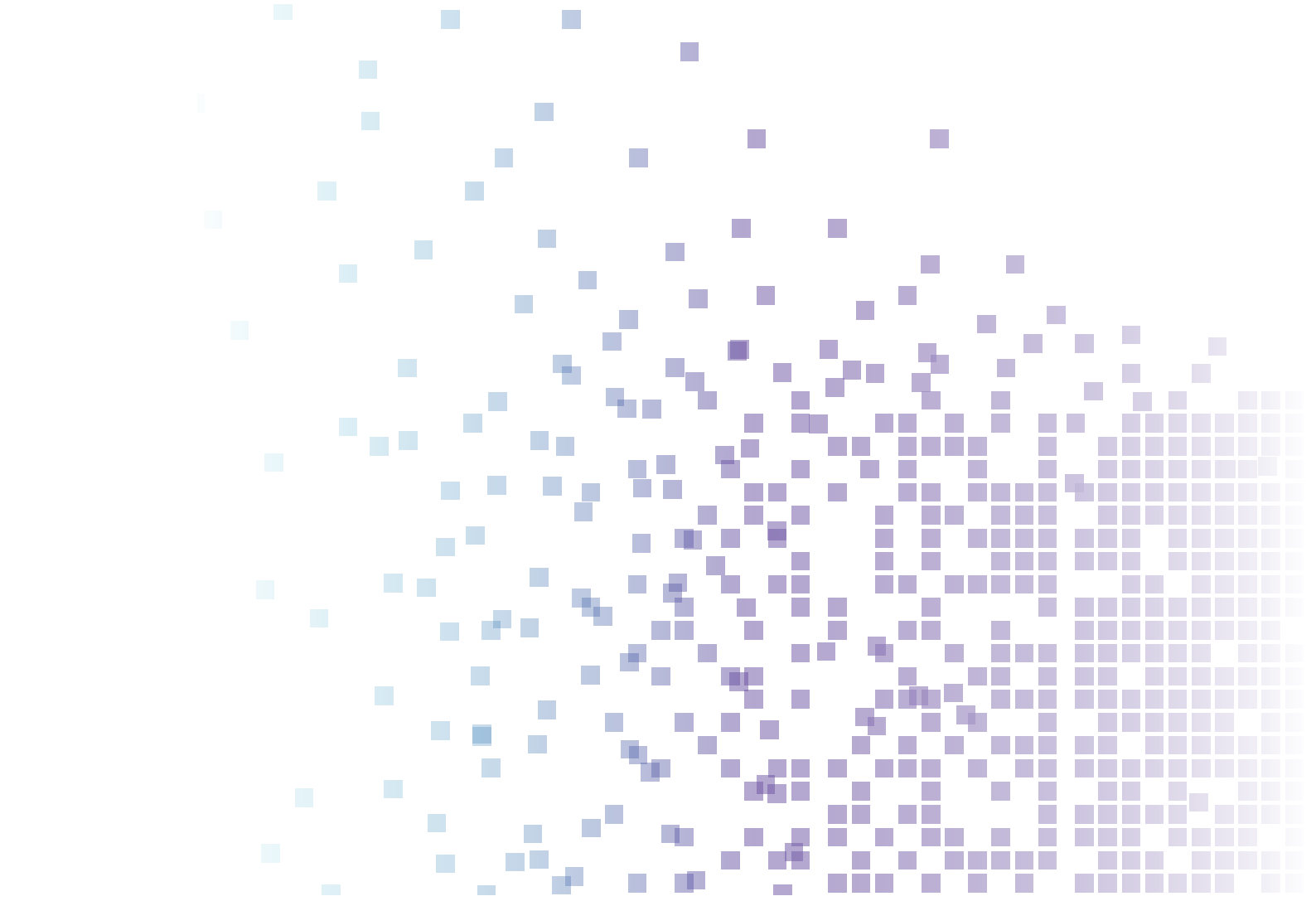
Pencuri info boleh mengenakan implikasi buruk ke atas kedua-dua pihak individu dan organisasi. Jikalau pencuri info memungut kredential-kredential pengguna, penjenayah siber pula mungkin akan menggunakan kredential-kredential pengguna ini untuk mengakses jaringan-jaringan korporat atau sistem-sistem perusahaan dengan akaun-akaun pengguna sahih, yang sering melambatkan pengesanan oleh pemilik sistem.

Bagi **organisasi-organisasi** yang dijejas oleh pencuri info, akibatnya mungkin termasuk:

- ransomware
- pencerobohan data
- pengkompromian e-mel perniagaan
- pencurian harta intelek
- pencurian maklumat sensitif.

Bagi seseorang **individu** yang dijejas oleh pencuri info, akibatnya mungkin termasuk:

- akses yang tidak dibenarkan kepada akaun-akaun e-mel atau media sosial peribadi
- peningkatan risiko pencurian identiti
- peningkatan risiko serangan pancingan
- kerugian kewangan atau akses yang tidak dibenarkan kepada akaun-akaun kewangan
- kehilangan privasi.



Kajian Kes:

Kajian kes ini telah dianonimkan untuk membenarkan penyebarannya kepada khalayak ramai. Ia dibina daripada pelbagai inside keselamatan siber yang telah meninggalkan impak ke atas entiti-entiti Australia yang telah dilaporkan kepada ASD ACSC. Entiti yang diimpak ini akan dirujuk selepas ini sebagai 'organisasi'. Nama-nama para individu dalam kajian kes ini adalah rekaan semata-mata dan butir-butir berkaitan telah dikeluarkan untuk melindungi identiti para mangsa.

Organisasi yang dimaksudkan ialah sebuah perniagaan Australia yang membenarkan kakitangannya untuk mengakses sistem-sistem korporat mereka daripada alat-alat peranti peribadi. Alice ialah seorang pekerja organisasi tersebut yang bekerja secara jarak jauh.

Sewaktu beliau bekerja dari rumah, Alice mengakses jaringan korporat organisasi beliau secara jarak jauh dengan menggunakan komputer riba peribadi beliau. Alice **memuat turunkan**, ke dalam **komputer riba peribadi** beliau, sebuah versi Notepad++ (sejenis perisian pengambilan nota) daripada sebuah laman web yang beliau percaya adalah sahih. Sebuah **pencuri info** telah disembunyikan sebagai alat pemasang bagi perisian Notepad++.

Apabila Alice cuba untuk memasang perisian tersebut, pencuri info pun diaktifkan dan mula **menuai kredential-kredential pengguna** daripada komputer riba beliau. Ini termasuk nama pengguna dan kata laluan kerja beliau, yang beliau telah simpankan ke dalam ciri daftar masuk yang disimpan dalam pelayar web beliau. Pencuri info itu kemudian menghantar kredential-kredential pengguna itu kepada sebuah server arah-dan-kawal jarak jauh yang dikawal oleh satu kumpulan penjenayah siber.

Log-log yang dicuri telah dipakejkan dengan log-log lain dan kemudian **dijual kepada penjenayah siber** menerusi tempat pasaran web haram.

Seorang penjenayah siber bernama Bob telah membeli kredential-kredential pengguna Alice, dan mengenal pasti kredential-kredential pengguna kepada perkhidmatan dalam jaringan organisasi beliau. Organisasi Alice **tidak mengkonfigurasikan MFA** bagi perkhidmatan-perkhidmatan ini, yang bererti Bob boleh menggunakan kredential-kredential pengguna yang dicuri tersebut dengan sendirinya untuk **menentusahkan dan mengakses** jaringan korporat itu dengan berjaya.

Bob mengakses jaringan korporat organisasi Alice tanpa dikesan dengan menggunakan **kredential-kredential pengguna sah** yang dicuri itu. Bob kemudian berupaya untuk berpaksi secara lateral melalui jaringan korporat itu, mengenal pasti data sensitif yang dimiliki organisasi itu dan mengeksfiltrasikannya untuk memeras ugut syarikat tersebut.

Setelah mencuri data sensitif itu, Bob **mengenkriptasikan pangkalan data dan sistem-sistem fail** organisasi itu untuk menjadikannya tidak boleh diakses.

Pemitigasian

Organisasi-organisasi mungkin tidak akan berupaya untuk menguatkuasakan kawalan ke atas alat-alat peranti yang terhubung kepada jaringan korporat mereka, khususnya pada alat-alat peranti peribadi yang diguna oleh pekerja yang bekerja secara jarak jauh. ASD ACSC menyarankan agar organisasi berfokus ke arah menerapkan kawalan untuk melindungi diri mereka sendiri daripada risiko pencuri info menyasarkan kredential-kredential pengguna. Pemitigasian ini termasuk:

Menyampaikan latihan kesedaran keselamatan siber kepada para kakitangan

- Menghalang penjuruteraan sosial tersasar yang berjaya dan pemuat turunan fail berniat jahat dengan menyampaikan latihan berkesan kepada para kakitangan
- Meningkatkan kesedaran tentang pencuri info, kaedah penyampaian mereka dan ancaman pancingan terhadap organisasi anda.

Teguhkan akaun-akaun korporat

- Laksanakan MFA:
- Laksanakan MFA ke seluruh pelusuk perkhidmatan luaran dan dalaman, repositori-repositori sistem dan data sensitif, khususnya bagi webmail, VPN, dan akaun-akaun pengguna yang diberi laluan istimewa yang mengakses sistem-sistem kritikal. Amalan terbaik ialah untuk menerapkan MFA tahan-pancingan pada semua akaun.
- Nyahbolehkan akaun pengguna apabila ia tidak diperlukan lagi.
- Mengehadkan keistimewaan pentadbir:
- Lakukan pentadbiran jaringan dan tugas-tugas laluan istimewa lain dengan menggunakan sebuah stesenkerja tunggal yang telah dikunciketat sahaja (iaitu sebuah stesenkerja admin yang teguh).
- Turuti amalan terbaik laluan keistimewaan-paling kurang dengan mengehendaki para pentadbir untuk menggunakan akaun-akaun penggguna dengan laluan istimewa bagi mengurus sistem dan akaun-akaun pengguna standard untuk tugas-tugas bukan berunsur pentadbiran.
- Menghalang akaun-akaun pengguna dengan laluan istimewa (kecuali mereka yang dibenarkan secara nyata untuk mengakses perkhidmatan dalam talian) daripada mengakses internet, e-mel dan perkhidmatan web.
- Timbangkan pelaksanaan pentadbiran sesempat-masa (just-in-time) bagi sistem-sistem dan aplikasi-aplikasi.
- Menguatkuasakan pengurusan dan pengoditan akaun-akau pengguna berlaluan istimewa.
- Mengemaskinikan kata laluan secara berkala, khususnya bagi akaun-akaun yang menghadap akses jarak jauh.
- Menguatkuasakan tempoh hayat pembatalan masa (time outs) dan dasar-dasar senja (sunset policies) bagi token-token sesi dan cookies.

Perkuatkan mobiliti perusahaan.

- Lakukan penilaian risiko mobiliti perusahaan dan laksanakan garis panduan penguatan mobiliti perusahaan.
- Laksanakan sebuah dasar Bring Your Own Device (BYOD) jika anda membenarkan para pekerja untuk menggunakan alat-alat peranti peribadi unuk kerja, kerana alat-alat peranti yang diurus secara korporat adalah lebih teguh daripada alat-alat peranti peribadi yang tidak diurus.

Menilai kembali dan mengakses risiko rantaian bekalan daripada vendor-vendor yang mengakses jaringan-jaringan anda, termasuk vendor-vendor Software-as-a-Service (Saas) dan Manager Service Providers. Bagaimana Untuk Mengurus Keselamatan Anda Sewaktu Berurusan dengan Sebuah Penyedia Perkhidmatan Terurus.

Lindungi jaringan korporat anda

- Pastikan aplikasi-aplikasi dan sistem-sistem pengendalian dikemaskini.
- Terapkan dasar-dasar keselamatan lokal untuk menguatkuasakan kawalan aplikasi dengan sebuah senarai kebenaran yang ketat.
- Laksanakan pensegmentasian jaringan untuk mengasingkan segmen-segmen jaringan berdasarkan peranan dan kefungsian.
- Odit dan pantau aktiviti-aktiviti pengguna, khususnya bagi para pekerja jarak jauh.
- Memantau akaun-akaun berlaluan istimewa boleh mendedahkan akses yang tidak dibenarkan kepada data sensitif atau aktiviti-aktiviti penghantaran data luarbiasa, misalnya jumlah bilangan besar data yang dimuat naik kepada sesuatu jaringan luaran.
- Melaksanakan dasar dan peralatan penghalangan kehilangan-data untuk menghalang penghantaran data yang tidak dibenarkan.

Menjadi seorang Rakan Kongsi Jaringan Keselamatan Siber ASD (ASD Cyber Security Network Partner) dan menyertai perkhidmatan Perkongsian Risikan Ancaman Siber ASD (Cyber Threat Intelligence Sharing) (CTIS).

- CTIS ialah sebuah platform perkongsian dua-hala yang membolehkan rakan kongsi kerajaan dan industri untuk menerima dan berkongsi maklumat mengenai aktiviti siber berniat jahat.
- ASD ACSC sedang menjejaki aktiviti pencuri info dan berkongsi butir-butir mengenai infrastruktur arahan dan kawalan yang aktif melalui platform CTIS.
- Daftarkan diri anda untuk menjadi seorang rakan kongsi dan lindungi organisasi anda dan data pelanggan anda daripada ancaman penjenayah siber.

Bersiapsiaga untuk dikompromi

- Bangunkan sebuah pelan respons insiden keselamatan siber untuk diguna sewaktu berlakunya sebuah kompromi pencuri info. Pastikan bahawa para pekerja sedar tentang apa yang perlu dibuat dan siapa untuk dihubungi jika mereka mengesyaki mereka telah memuat turun sebuah fail yang mencurigakan.

Laksanakan Lapan Perkara Wajib (Essential Eight) ASD ACSC

- Selain pemitigasian yang disebut di atas, ASD ACSC menyarankan dengan tegas pelaksanaan Lapan Perkara Wajib (Essential Eight) ASD ACSC yang selanjutnya.

Nasihat bagi para pekerja anda sewaktu mereka bekerja secara jarak jauh

- Lindungi maklumat anda pada alat peranti peribadi anda
  - Bangunkan sikap kebersihan siber yang baik dan jangan klik pada pautan yang mencurigakan atau pop-up, atau memuat turunkan fail-fail atau perisian daripada sumber-sumber yang tidak diketahui atau tidak dipercayai.
  - Gunakan kata laluan tersendiri bagi akaun-akaun kerja dan peribadi. Gunakan MFA sejauh mungkin bagi akaun-akaun peribadi.
  - Jangan simpankan kredential-kredential kerja anda dalam sebuah pengurus kata laluan peribadi kecuali jika ia telah diluluskan secara nyata oleh majikan anda. Ini termasuk pengurus kata laluan pelayar web anda.**Jika anda tidak pasti, mintak majikan anda untuk menyediakan sebuah pengurus kata laluan yang disokong secara korporat.**
  - Jangan daftar masuk ke dalam akaun-akaun kerja anda daripada stesen-stesen kerja yang dikongsi atau komunal.
  - Sentiasa berwaspada tentang apa yang disimpan dalam ciri pengisian auto pelayar web anda. Pencuri info menyasarkan data yang disimpan pelayar untuk mengisi autokan borang. Sewaktu mengisi borang sesawang, timbangkan kemasukan data sensitif secara manual, misalnya nombor-nombor kad kredit, daripada menyimpannya ke dalam ciri pengisian auto pelayar web anda.
  - Daftar keluar daripada semua perkhidmatan dalam talian dan padamkan semua cookies pelayar web selepas selesainya sesi layaran untuk menguragnkan maklumat yang tersedia kepada pencuri info.
  - Pastikan solusi anti-virus yang terbina di dalam sistem pengendalian anda dibolehkan. Jika anda menggunakan solusi anti-virus pihak ketiga, pastikan ia dikemaskini dan ialah daripada sebuah vendor yang berwibawa.

Bantuan

Organisasi-organisasi Australia yang telah diimpak atau memerlukan bantuan mengenai sesuatu kompromi pencuri info boleh menghubungi ASD ACSC menerusi **1300 CYBER1 (1300 292 371)** atau dengan menghantarkan sebuah laporan di cyber.gov.au/report.

ASD ACSC menggalakkan entiti-entiti untuk melaporkan aktiviti jaringan yang mencurigakan dan petanda-petanda kompromi yang dikaitkan dengan pencuri info, biarpuan insiden tersebut dianggap telah diselesai. Kami menggunakan maklumat yang anda sediakan untuk memperbaiki pemahaman kami tentang taktik-taktik, teknik-teknik dan prosedur-prosedur pelaku ancaman siber, yang menolong kami untuk memberi amaran kepada organisasi-organisasi Australia lain yang telah dijadikan sasaran dalam cara yang sama.

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