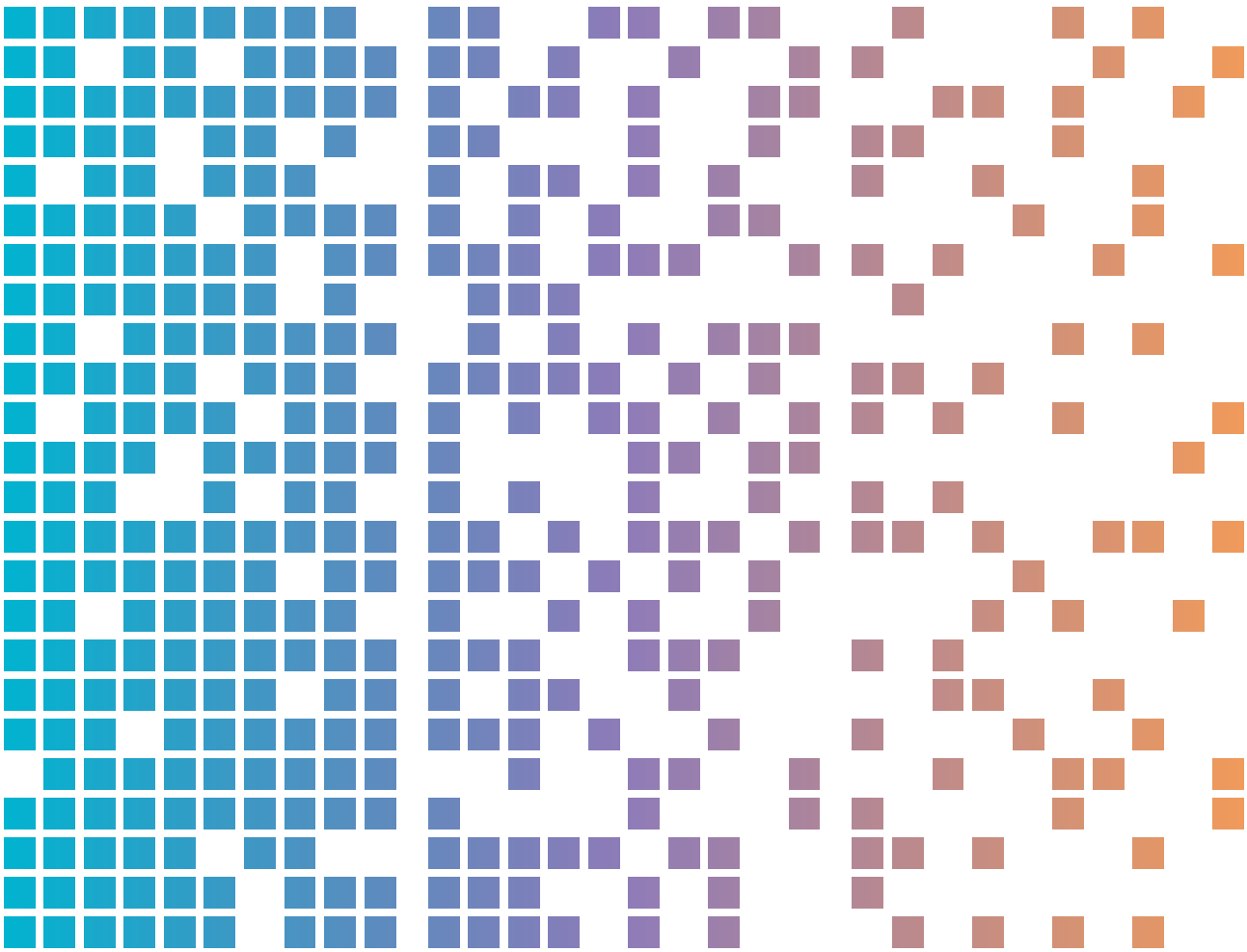
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Pencurian diam-diam: penjahat siber menggunakan malware pencuri informasi untuk menyusupi jaringan perusahaan



Kompleksitas konten
SEDANG

Daftar isi

Konteks

Information stealer malware mencuri kredensial pengguna dan informasi sistem yang dieksploitasi oleh penjahat siber, terutama untuk keuntungan finansial. Pencuri informasi telah diamati dalam serangan kejahatan siber terhadap berbagai organisasi dan sektor di seluruh dunia, termasuk Australia. Publikasi ini memberikan panduan keamanan siber kepada pembaca tentang malware pencuri informasi, termasuk aktivitas ancaman dan saran mitigasi bagi organisasi dan karyawannya.

Poin-Poin Penting

- Malware pencuri informasi, juga dikenal sebagai pencuri informasi, adalah jenis malware yang dirancang untuk mengumpulkan informasi dari perangkat korban. Ini dapat mencakup nama pengguna dan kata sandi, detail kartu kredit, dompet mata uang kripto, berkas lokal, dan data peramban termasuk kuki, riwayat pengguna, dan detail formulir isi otomatis.
- Penjahat siber dapat berupaya membeli dan menggunakan kredensial pengguna curian yang terkait dengan akun perusahaan untuk mendapatkan akses awal ke perangkat perusahaan korban, klien mereka, dan sistem perusahaan lainnya. Dampak selanjutnya bagi organisasi-organisasi ini dapat mencakup ransomware, pemerasan, penyusupan sur-el bisnis, dan pencurian kekayaan intelektual.
- Pusat Keamanan Siber Australia (ACSC) di Australian Signals Directorate (ASD) telah mengidentifikasi pelanggaran jaringan perusahaan yang berawal dari karyawan yang mengakses sumber daya kerja dari perangkat pribadi yang telah disusupi. Dalam beberapa kasus, penjahat siber mendapatkan akses awal ke jaringan perusahaan dengan menggunakan kredensial pengguna sah yang dicuri. Investigasi kami menunjukkan bahwa penyusupan ekstensif biasanya terjadi setelah penjahat siber berhasil mengakses akun pengguna istimewa.
- Organisasi yang memfasilitasi karyawan, kontraktor, penyedia layanan terkelola, atau entitas lain untuk mengakses jaringan mereka dari jarak jauh, termasuk dengan perangkat keras Bring Your Own Device (BYOD), perlu mewaspadai risiko pencuri informasi dan melindungi diri dari ancaman ini. Penjahat siber menyebarkan pencuri informasi ke perangkat korban menggunakan berbagai teknik, termasuk sur-el phishing, unduhan perangkat lunak bajakan, teknik search engine optimisation (SEO), iklan berbahaya, atau tautan berbahaya yang diposting di platform media sosial. Secara umum, perangkat yang digunakan untuk keperluan kerja dan pribadi berisiko lebih tinggi terinfeksi melalui teknik-teknik ini karena perilaku pengguna dan kontrol keamanan yang terbatas.
- Pencuri informasi menawarkan model yang menarik bagi penjahat siber untuk memonetisasi aktivitas kejahatan siber, terutama bagi penjahat siber tingkat pemula dan mereka yang memiliki kemampuan teknis terbatas. Beberapa penjahat siber akan memasarkan produk pencuri informasi dengan program bergaya Malware-as-a-Service (MaaS), dengan mengenakan biaya berlangganan bulanan untuk penggunaannya.

Latar Belakang

Penggunaan pencuri informasi oleh penjahat siber menghadirkan ancaman bagi keamanan dan kesejahteraan organisasi-organisasi di Australia. Infeksi pencuri info umumnya muncul sebagai aktivitas pendahuluan untuk insiden keamanan siber besar, karena penjahat siber menggunakannya untuk mengumpulkan kredensial pengguna. Kredensial pengguna ini, terutama yang menyediakan akses ke layanan jarak jauh yang terhubung ke internet atau akun istimewa, kemudian dieksploitasi untuk memungkinkan akses awal ke sistem dan data perusahaan.

Catatan: Broker akses awal memainkan peran khusus dalam ekosistem kejahatan siber dengan membeli dan memvalidasi kredensial pengguna yang dicuri. Mereka kemudian melelang kredensial pengguna berkualitas tinggi, untuk lingkungan korporat yang diminati, kepada penjahat siber yang akan menggunakan kredensial pengguna tersebut untuk mengeksploitasi jaringan korporat organisasi.

Kredensial pengguna valid yang dicuri sangat berharga bagi penjahat siber, karena mempercepat akses awal ke jaringan korporat dan sistem perusahaan. Dengan kredensial pengguna valid yang dicuri, penjahat siber dapat melewati beberapa taktik dan teknik umum, termasuk:

- mengidentifikasi dan meneliti target
- mencari kerentanan pada jaringan target
- mengembangkan vektor untuk akses awal, seperti:
  - materi phishing
  - eksploitasi kerentanan perangkat lunak
  - menargetkan layanan jarak jauh, termasuk RemoteDesktop Protocol (RDP) atau layanan Virtual Private Network (VPN)
  - serangan brute force terhadap kredensial pengguna (tebakan kata sandi).

Langkah-langkah ini membutuhkan investasi waktu dan tingkat kecakapan teknis yang menjadi penghalang bagi beberapa penjahat siber. Khususnya, penjahat siber yang tidak mampu menembus pertahanan jaringan perusahaan dapat langsung diuntungkan oleh infeksi pencuri informasi, karena infeksi ini dapat memberikan akses kredensial pengguna yang cepat dan mudah ke jaringan perusahaan yang diinginkan.

Dalam pengaturan kerja jarak jauh, beberapa karyawan menggunakan perangkat pribadi untuk bekerja dan menjelajah internet pribadi. Dengan demikian, karyawan dapat memilih untuk menyimpan kredensial pengguna mereka di penyimpanan kata sandi dan ekstensi peramban web mereka, atau mereka dapat memanfaatkan fitur isi otomatis peramban web. Pencuri informasi menargetkan penyimpanan kata sandi ini, beserta kuki autentikasi dan data pribadi lainnya di dalam peramban web.

Tidak seperti perangkat perusahaan, perangkat pribadi tidak selalu memiliki kebijakan keamanan perusahaan yang diberlakukan, yang menimbulkan risiko lebih tinggi bagi organisasi. Misalnya, karyawan dapat terlibat dalam aktivitas, seperti mengunduh perangkat lunak bajakan dan menjelajah daring berisiko tinggi, yang meningkatkan paparan mereka terhadap ancaman siber dan infeksi malware.

Pencuri informasi, distributor, broker akses awal, dan afiliasi ransomware kini membentuk bagian inti dari ekosistem kejahatan siber yang didorong oleh keuntungan finansial. Ekosistem tumbuh lebih efisien ketika penjahat siber mengkhususkan diri dan mengembangkan kemampuan yang menargetkan tahap serangan tertentu, lalu menjual kemampuan itu sebagai layanan kepada afiliasi kriminal lainnya.

Aktivitas ancaman

ACSC ASD melacak dan memantau peningkatan aktivitas pencurian informasi secara global, yang menghadirkan ancaman yang semakin besar bagi jaringan Australia. Laporan industri menunjukkan bahwa pencuri informasi merupakan varian malware paling populer dalam aktivitas kejahatan siber sepanjang tahun 2023. Meningkatnya volume data curian yang dijual di pasar web gelap, dan peningkatan aktivitas broker akses awal yang memanfaatkan data ini, mencerminkan tren yang meningkat ini, yang semakin cepat hingga tahun 2024.

Ekosistem Pencuri Informasi

Tahap 1: Dapatkan malware

Pencuri informasi biasanya ditawarkan di pasar kejahatan siber sebagai MaaS atau Stealer-as-a-Service, atau dijual sebagai kode sumber. MaaS mengacu kepada model bisnis di mana pengembang malware menjual langganan perangkat lunak berbahaya mereka kepada individu melalui platform berbasis web, mirip dengan penawaran Perangkat Lunak sebagai Layanan yang sah. Model MaaS telah menurunkan hambatan masuk bagi penjahat siber, karena memungkinkan individu tanpa keterampilan teknis yang luas untuk mendistribusikan malware dan mengumpulkan informasi curian untuk digunakan dalam serangan siber.

Pencuri informasi yang ditawarkan sebagai MaaS umumnya diiklankan dengan biaya bulanan yang relatif murah, dan memberi penjahat siber akses ke dasbor pencuri informasi. Dasbor ini memfasilitasi pembuatan malware pencuri informasi, mengelola data yang dicuri, dan melacak jumlah sistem yang disusupi. Operator MaaS menawarkan pembaruan fitur, alat, dan dukungan teknis untuk menghindari deteksi perangkat lunak antivirus serta untuk menarik dan mempertahankan pelanggan. Banyak pencuri informasi memiliki kemampuan untuk menghapus diri mereka sendiri dari perangkat korban setelah melakukan eksfiltrasi data.

Tahap 2: Distribusi

Penjahat siber yang mendistribusikan pencuri informasi dan mengumpulkan informasi dari perangkat yang disusupi dikenal sebagai 'Traffer' (distributor lalu lintas). Traffer mengarahkan korban ke tautan berbahaya, memfasilitasi penyebaran pencuri informasi sebagai bagian dari kampanye yang luas. Sebagian besar kampanye bersifat acak, mengandalkan infeksi oportunistik. Namun, beberapa kampanye dirancang khusus untuk industri tertentu dan melibatkan spear-phishing yang ditargetkan terhadap korban tertentu. Traffer melakukan kampanye yang lebih tertarget ini sebagai respons terhadap permintaan pelanggan; misalnya, ketika pembeli mencari akses ke organisasi atau sektor bernilai tinggi tertentu.

Traffer akan menyebarkan pencuri informasi ke perangkat korban menggunakan berbagai teknik, termasuk:

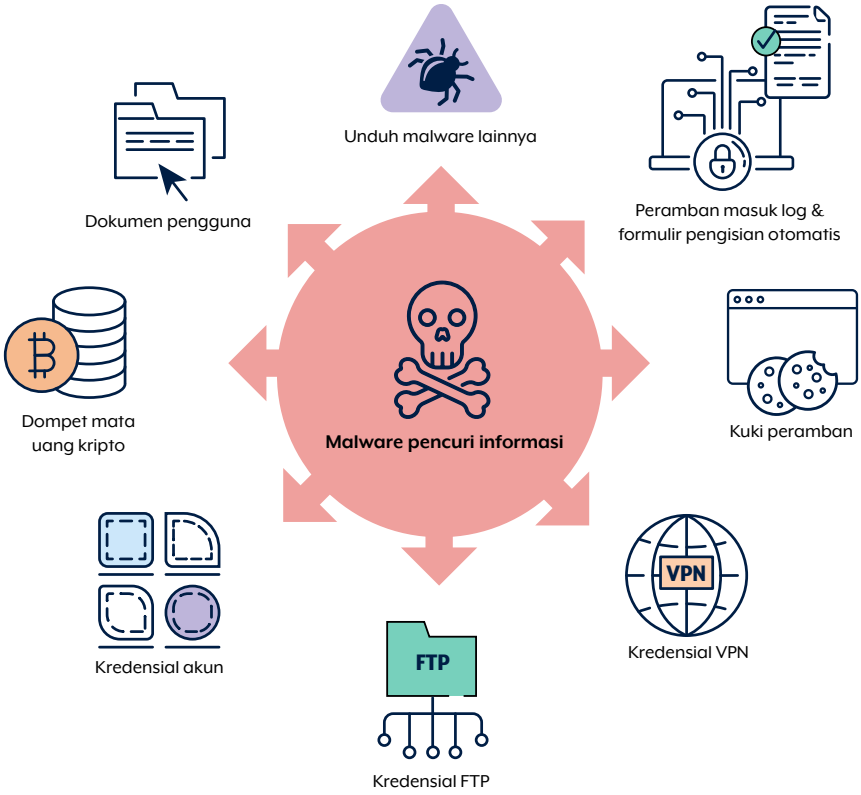
- **botnet**: jaringan sistem komputer yang disusupi yang dikendalikan oleh penjahat siber untuk melakukan tindakan jahat, seperti mengirimkan pesan phishing atau malware

- **phishing**: upaya untuk mendapatkan informasi sensitif melalui penipuan, termasuk melalui sur-el atau pesan langsung di media sosial, forum, dan aplikasi perpesanan, yang merupakan metode distribusi umum yang telah menurunkan hambatan masuk bagi penjahat siber:
  - Pesan-pesan ini umumnya berisi tautan berbahaya, alih-alih melampirkan berkas berbahaya ke dalam sur-el itu sendiri.
- **hasil pencarian berbahaya**: dikirimkan melalui teknik search engine optimisation (SEO) yang mengarahkan target ke situs web yang menyajikan malware yang disamarkan sebagai perangkat lunak atau konten sah lainnya
- **malvertising**: penggunaan kode berbahaya, yang disuntikkan ke dalam iklan daring yang sah, untuk mendistribusikan malware
- **perangkat lunak hasil retasan atau bajakan**: unduhan, termasuk gim video, yang dibagikan melalui video YouTube, dengan tautan berbahaya dalam deskripsi video atau komentar, atau dari situs unduhan yang tidak tepercaya
- **iklan dan unggahan media sosial**: mengarahkan target ke berkas malware yang disamarkan
- **pembaruan perangkat lunak berbahaya**: umumnya disamarkan sebagai pembaruan peramban web

Tahap 3: Data Harvesting

Setelah pencuri informasi mengeksekusi perangkat korban, ia mulai mengumpulkan data sensitif dari mesin yang disusupi. Selain mencuri kredensial pengguna, dalam kasus di mana pencuri informasi merupakan bagian dari botnet, penjahat siber dapat mengendalikan perangkat yang disusupi dari jarak jauh dengan mengirimkan perintah konfigurasi untuk mengaktifkan kemampuan tambahan atau mengirimkan malware lainnya. Secara umum, pencuri informasi mampu mencuri:

- nama pengguna dan kata sandi, terutama yang tersimpan dalam sesi/token pengguna autentikasi multi-faktor (MFA) peramban web
- kuki autentikasi
- informasi formulir isi otomatis peramban web
- kredensial sur-el, konten, dan kontak
- riwayat penelusuran web
- dokumen pengguna
- detail kartu kredit
- log obrolan dari aplikasi perpesanan desktop
- informasi sistem
- dompet mata uang kripto
- kredensial VPN atau File Transfer Protocol (FTP).



Gambar 1. Kemampuan pencuri informasi

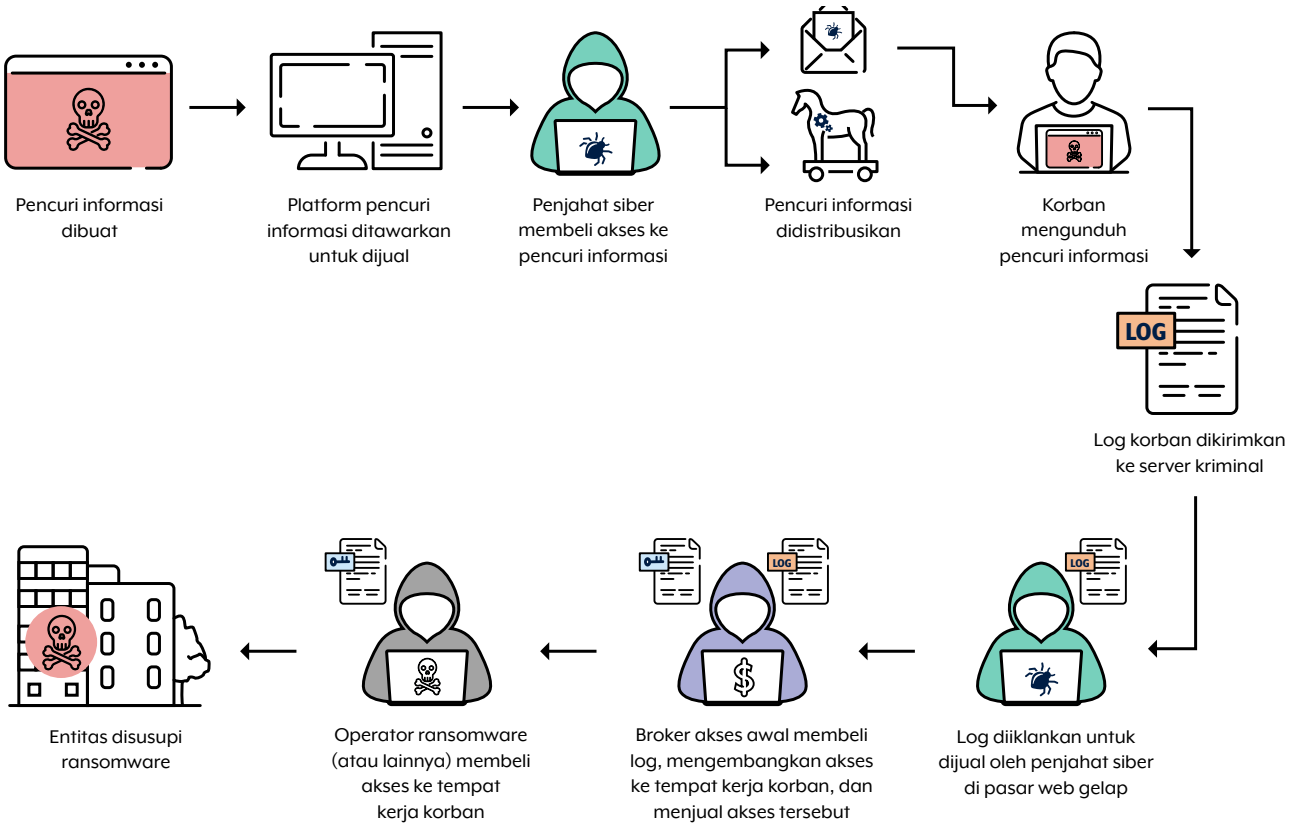
Beberapa kuki autentikasi peramban web membuat pengguna tetap masuk ke suatu akun atau layanan selama beberapa hari, sehingga pengguna tidak perlu melakukan autentikasi ulang. Jika dicuri, kuki autentikasi ini dapat secara efektif melewati persyaratan MFA dan memberikan akses kepada penjahat siber ke akun korban, jaringan perusahaan, dan sistem perusahaan.

Tahap 4: Agregasi dan Monetisasi Data

Pencuri informasi dikonfigurasi untuk mencuri informasi korban, yang dikenal sebagai 'log', ke server perintah dan kontrol berbahaya. Pada umumnya, pencuri informasi memanfaatkan aplikasi perpesanan (messaging app) populer, seperti Telegram dan Discord, untuk berbagi umpan log dengan penjahat siber.

Terdapat pasar khusus di Telegram dan di seluruh dark web untuk penjualan dan perdagangan log. Penjahat siber memonetisasi log dengan berbagai cara, termasuk:

- menjual log di pasar kriminal, termasuk kepada broker akses awal
- mengeksploitasi korban secara langsung, melalui pencurian identitas dan pemerasan
- memanfaatkan informasi untuk akses awal ke jaringan perusahaan untuk aktivitas ransomware.



Gambar 2. Ekosistem pencuri informasi dan dampak yang mungkin terjadi pada suatu organisasi.

Implikasi

Ekosistem pencuri informasi dan kemungkinan dampaknya terhadap individu dan organisasi. Ketika pencuri informasi mengumpulkan kredensial pengguna, penjahat siber dapat menggunakan kredensial pengguna ini untuk mengakses jaringan perusahaan atau sistem perusahaan dengan akun pengguna yang valid, yang seringkali menunda deteksi oleh pemilik sistem.

Bagi **organisasi** yang terdampak oleh pencuri informasi, konsekuensinya dapat meliputi:

- ransomware
- pelanggaran data
- sur-el bisnis yang disusupi
- pencurian kekayaan intelektual
- pencurian informasi sensitif.

Bagi **individu** yang terdampak pencurian informasi, konsekuensinya dapat meliputi:

- akses tidak sah ke sur-el pribadi atau akun media sosial
- peningkatan risiko pencurian identitas
- peningkatan risiko serangan phishing
- kerugian finansial atau akses tidak sah ke rekening keuangan
- kehilangan privasi.

Studi kasus

Studi kasus ini telah dianonimkan agar dapat disebarluaskan kepada publik. Studi kasus ini didasarkan pada beberapa insiden keamanan siber yang telah berdampak kepada entitas Australia yang telah melapor ke ACSC ASD. Entitas yang terdampak selanjutnya disebut sebagai 'organisasi'. Nama-nama individu dalam studi kasus ini fiktif dan detailnya telah dihapus untuk melindungi identitas korban.

Organisasi ini adalah bisnis Australia yang memungkinkan staf mengakses sistem perusahaan dari perangkat pribadi. Alice adalah seorang karyawati organisasi yang bekerja jarak jauh.

Saat bekerja dari rumah, Alice mengakses jaringan perusahaan organisasinya dari jarak jauh menggunakan laptop pribadinya. Alice **mengunduh**, ke **laptop pribadinya**, sebuah versi Notepad++ (yang merupakan sejenis perangkat lunak pencatat) dari situs web yang ia yakini sah. Seorang **pencuri informasi** menyamar sebagai penginstal perangkat lunak Notepad++.

Ketika Alice mencoba memasang perangkat lunak tersebut, pencuri informasi tersebut aktif dan mulai **memanen kredensial pengguna** dari laptopnya. Ini termasuk nama pengguna dan kata sandi kantornya, yang telah ia simpan di fitur login tersimpan pada peramban web-nya. Pencuri informasi kemudian mengirimkan kredensial pengguna tersebut ke server perintah dan kendali jarak jauh yang dikendalikan oleh kelompok penjahat siber.

Log yang dicuri dikemas bersama dengan yang lain dan kemudian **dijual kepada penjahat siber** melalui pasar web gelap.

Seorang penjahat siber bernama Bob membeli kredensial pengguna Alice, mengidentifikasi kredensial pengguna untuk layanan di jaringan organisasinya. Organisasi Alice **belum mengonfigurasi MFA** untuk layanan ini, yang berarti Bob dapat menggunakan kredensial pengguna yang dicuri itu sendiri untuk berhasil **mengautentikasi dan mengakses** jaringan perusahaan.

Bob mengakses jaringan perusahaan organisasi Alice tanpa terdeteksi menggunakan **kredensial pengguna yang valid** hasil curian. Bob dapat melakukan pivot lateral melalui jaringan perusahaan, mengidentifikasi data sensitif milik organisasi dan mengekstraknya untuk memeras perusahaan.

Setelah mencuri data sensitif tersebut, Bob **mengenkripsi basis data dan sistem berkas** organisasi agar tidak dapat diakses.

Mitigasi

Organisasi mungkin tidak dapat menerapkan kontrol pada perangkat yang terhubung ke jaringan perusahaan mereka, terutama pada perangkat pribadi yang digunakan oleh karyawan yang bekerja jarak jauh. ACSC ASD merekomendasikan agar organisasi berfokus pada penerapan kontrol untuk melindungi diri dari risiko pencuri informasi yang menargetkan kredensial pengguna. Mitigasi ini meliputi:

Memberikan pelatihan kesadaran keamanan siber bagi staf

- Mencegah rekayasa sosial tertarget dan pengunduhan berkas berbahaya dengan memberikan pelatihan yang efektif kepada staf.
- Meningkatkan kewaspadaan terhadap pencuri informasi, metode pengirimannya, dan ancaman phishing terhadap organisasi Anda.

Mengamankan akun perusahaan

- Menerapkan MFA:
- Menerapkan MFA di seluruh layanan eksternal dan internal, sistem, dan repositori data sensitif, terutama untuk webmail, VPN, dan akun pengguna istimewa yang mengakses sistem penting. Praktik terbaik adalah menerapkan MFA yang tahan phishing di semua akun.
- Menonaktifkan akun pengguna jika tidak lagi diperlukan.
- Batasi hak akses administratif:
- Lakukan administrasi jaringan dan tugas istimewa lainnya hanya menggunakan stasiun kerja khusus yang terkunci (yaitu stasiun kerja admin yang aman).
- Ikuti praktik terbaik dengan hak istimewa paling rendah dengan mewajibkan administrator menggunakan akun pengguna istimewa untuk mengelola sistem dan akun pengguna standar untuk tugas non-administratif.
- Cegah akun pengguna istimewa (kecuali yang secara eksplisit diizinkan untuk mengakses layanan daring) mengakses internet, sur-el, dan layanan web.
- Pertimbangkan penerapan administrasi tepat waktu untuk sistem dan aplikasi.
- Terapkan pengelolaan dan audit akun pengguna istimewa.
- Perbarui kata sandi secara berkala, terutama akun akses jarak jauh yang terhubung ke eksternal.
- Terapkan kebijakan batas waktu masa berlaku dan kebijakan penghentian sementara pada token sesi dan kuki.

Perkuat mobilitas perusahaan

- Lakukan penilaian risiko mobilitas perusahaan dan terapkan pedoman penguatan mobilitas perusahaan.
- Terapkan kebijakan Bring Your Own Device (BYOD) jika Anda mengizinkan karyawan menggunakan perangkat pribadi untuk bekerja, karena perangkat yang dikelola perusahaan lebih aman daripada perangkat pribadi yang tidak dikelola.

Tinjau dan nilai risiko rantai pasokan dari vendor yang mengakses jaringan Anda, termasuk vendor Perangkat Lunak sebagai Layanan (SaaS) dan Penyedia Layanan Terkelola. Cara Mengelola Keamanan Anda Saat Menggunakan Penyedia Layanan Terkelola.

Lindungi jaringan perusahaan Anda

- Pastikan aplikasi dan sistem operasi selalu diperbarui.
- Terapkan kebijakan keamanan lokal untuk menegakkan kontrol aplikasi dengan daftar izin yang ketat.
- Terapkan segmentasi jaringan untuk memisahkan segmen jaringan berdasarkan peran dan fungsionalitas.
- Audit dan pantau aktivitas pengguna, terutama untuk karyawan jarak jauh.
- Pemantauan akun istimewa dapat mengungkap akses tidak sah ke data sensitif atau aktivitas transfer data yang tidak biasa, seperti data bervolume besar yang diunggah ke jaringan eksternal.
- Terapkan kebijakan dan alat pencegahan kehilangan data untuk mencegah transfer data tidak sah.

Jadilah Mitra Jaringan Keamanan Siber ASD dan bergabunglah dengan layanan Cyber Threat Intelligence Sharing (CTIS) ASD

- CTIS adalah platform berbagi dua arah yang memungkinkan mitra pemerintah dan industri menerima dan berbagi informasi tentang aktivitas siber berbahaya.
- ACSC ASD melacak aktivitas pencuri informasi dan membagikan detail infrastruktur komando dan kendali aktif melalui platform CTIS.
- Daftar untuk menjadi mitra dan lindungi data organisasi dan pelanggan Anda dari ancaman kejahatan siber.

Bersiaplah untuk menghadapi penyusupan

- Kembangkan rencana respons insiden keamanan siber untuk digunakan jika terjadi penyusupan oleh pencuri informasi. Pastikan karyawan mengetahui apa yang harus dilakukan dan siapa yang harus dihubungi jika mereka mencurigai telah mengunduh berkas yang mencurigakan.

Terapkan Delapan Esensial ACSC ASD

- Selain mitigasi yang disebutkan di atas, ACSC ASD sangat menyarankan untuk menerapkan sisa dari Delapan Esensial ACSC ASD.

Saran untuk karyawan Anda saat bekerja jarak jauh

- Lindungi informasi Anda di perangkat pribadi
  - Jaga kebersihan siber yang baik dan jangan klik tautan atau pop-up yang mencurigakan, atau unduh berkas atau perangkat lunak dari sumber yang tidak dikenal atau tidak tepercaya.
  - Gunakan kata sandi yang berbeda untuk akun kerja dan pribadi. Gunakan MFA untuk akun pribadi jika memungkinkan.
  - Jangan simpan kredensial kerja Anda di pengelola kata sandi pribadi kecuali disetujui secara tegas oleh perusahaan Anda. Ini termasuk pengelola kata sandi peramban web Anda. **Jika ragu, mintalah perusahaan Anda untuk menyediakan pengelola kata sandi yang didukung perusahaan.**
  - Jangan masuk ke akun kerja Anda dari stasiun kerja bersama atau komunal.
  - Waspadai apa yang disimpan dalam fitur isi otomatis peramban web Anda. Pencuri informasi menargetkan data yang disimpan peramban untuk mengisi otomatis formulir. Saat mengisi formulir web, pertimbangkan untuk memasukkan data sensitif secara manual, seperti nomor kartu kredit, daripada menyimpannya ke fitur isi otomatis peramban web Anda.
  - Keluar dari semua layanan daring dan hapus kuki peramban web setelah menyelesaikan sesi penelusuran untuk mengurangi akses informasi kepada pencuri informasi.
  - Pastikan solusi antivirus bawaan sistem operasi Anda diaktifkan. Jika Anda menggunakan solusi antivirus pihak ketiga, pastikan antivirus tersebut selalu diperbarui dan berasal dari vendor yang tepercaya.

Bantuan

Organisasi Australia yang terkena dampak atau memerlukan bantuan terkait pencurian informasi dapat menghubungi ACSC ASD melalui **1300 CYBER1 (1300 292 371)** atau dengan mengirimkan laporan di cyber.gov.au/report.

ACSC ASD mendorong entitas untuk melaporkan aktivitas jaringan yang mencurigakan dan indikator penyusupan yang terkait dengan pencuri informasi, meskipun suatu insiden dianggap terkendali. Kami menggunakan informasi yang Anda berikan untuk meningkatkan pemahaman kami tentang taktik, teknik, dan prosedur pelaku ancaman siber, yang membantu kami memperingatkan organisasi Australia lainnya yang telah menjadi sasaran dengan cara yang sama.

Penafian

Materi dalam panduan ini bersifat umum dan tidak boleh dianggap sebagai nasihat hukum atau diandalkan untuk bantuan dalam keadaan tertentu atau situasi darurat. Dalam masalah penting apa pun, Anda harus mencari nasihat profesional independen yang sesuai sehubungan dengan keadaan Anda sendiri.

Persemakmuran tidak bertanggung jawab atau berkewajiban atas kerusakan, kerugian, atau biaya apa pun yang ditimbulkan sebagai akibat mengandalkan informasi yang terkandung dalam panduan ini.

Hak Cipta

Penggunaan lambang Coat of Arms

Persyaratan penggunaan Lambang Coat of Arms diperinci di situs web Department of the Prime Minister and Cabinet Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

Untuk informasi lebih lanjut, atau untuk melaporkan insiden keamanan siber, hubungi kami:

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

Nomor ini hanya dapat digunakan di Australia.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre