



LAPORAN INTELIGENSI KEAMANAN MICROSOFT

VOLUME 24
JANUARI – DESEMBER 2018



Daftar isi

Dokumen ini dibuat hanya untuk tujuan informasi. MICROSOFT TIDAK MEMBERIKAN JAMINAN, BAIK SECARA TERSURAT, TERSIRAT, MAUPUN HUKUM, MENGENAI INFORMASI DI DALAM DOKUMEN INI.

Dokumen ini disediakan "sebagaimana adanya". Informasi dan pendapat yang disampaikan dalam dokumen ini, termasuk URL dan referensi situs web internet lainnya, dapat berubah tanpa pemberitahuan. Anda menanggung risiko dalam menggunakannya.

Hak Cipta © 2019 Microsoft Corporation. Semua hak dilindungi oleh undang-undang.

Nama asli perusahaan dan produk yang disebutkan di sini mungkin merupakan merek dagang dari pemiliknya masing-masing.

Penulis dan kontributor

Abhishek Agrawal

Perlindungan Informasi

David Fantham

Perlindungan Informasi

Debraj Ghosh

Pemasaran Microsoft Security

Diana Kelley

Grup Solusi Keamanan Siber

Elia Florio

Windows Active Defense

Eric Avena

Tim Peneliti Windows Defender

Eric Douglas

Tim Peneliti Windows Defender

Francis Tan Seng

Tim Peneliti Windows Defender

Jonathan Trull

Grup Solusi Keamanan Siber

Joram Borenstein

Grup Solusi Keamanan Siber

Karthik Selvaraj

Tim Peneliti Windows Defender

Kasia Kaplinska

Pemasaran Microsoft Security

Kristina Laidler

Respons Insiden Keamanan

Matt Duncan

Teknik dan Analitik Data Windows Active Defense

Mark Simos

Grup Solusi Keamanan Siber

Paul Henry

Wadeware LLC

Pragya Pandey

Pemasaran Microsoft Security

Ram Pliskin

Azure Security

Ryan McGee

Pemasaran Microsoft Security

Seema Kathuria

Grup Solusi Keamanan Siber

Steve Wacker

Wadeware LLC

Tanmay Ganacharya

Tim Peneliti Windows Defender

Volv Grebennikov

Bing

Yaniv Zohar

Azure Security

Prakata

Halo dan selamat datang di Laporan Inteligensi Keamanan (SIR) Microsoft edisi ke-24. Sebagai seorang praktisi dan arsitek keamanan, saya membaca laporan seperti ini dengan harapan dapat lebih memahami lanskap serta poin-poin penting terkait tips praktis tentang bagaimana menggunakan pengetahuan tersebut untuk pertahanan dan perlindungan organisasi yang lebih efektif.

Tim SIR menghadirkan semangat edukasi peningkatan ketahanan siber ke dalam laporan ini dan selama satu tahun telah memilah-milah data untuk menyaring pelajaran-pelajaran paling penting.

Apa yang Anda baca ini merupakan wawasan yang terkumpul dari analisis data keamanan selama satu tahun dan pelajaran praktis yang telah diseleksi. Data yang dianalisis meliputi 6,5 triliun sinyal ancaman yang masuk ke cloud Microsoft setiap hari dan penelitian serta pengalaman di dunia nyata dari ribuan peneliti dan responden kami di seluruh dunia. Pada 2018, para pelaku serangan menggunakan berbagai trik kotor, baik yang baru (seperti penambangan koin) maupun lama (seperti phishing), dengan upaya mencuri data dan sumber daya dari pelanggan dan organisasi. Serangan hibrid, seperti kampanye Ursnif, menggabungkan pendekatan sosial dengan teknis. Ketika defender semakin cerdas menangkal ransomware, yakni jenis serangan secara terbuka dan disruptif, para pelaku kejahatan beralih ke metode yang lebih "senyap", tapi tetap menguntungkan, yakni penambangan koin.

"Peralihan" ini bisa terasa sangat memusingkan, seolah-olah para pelaku serangan selalu selangkah lebih maju. Tetapi, dari sudut pandang yang berbeda, ini dapat dianggap sebagai sesuatu yang positif. Defender dan ahli keamanan siber seperti Anda telah menerapkan teknik-teknik pertahanan yang memaksa pelaku serangan mengubah muatan kesukaan mereka dan beralih dari ransomware.

Area lain di mana para pelaku kejahatan siber meningkatkan kegiatannya adalah rantai pasokan. Salah satu kejadian paling diingat, yakni wabah penambang koin Dofail, yang terjadi pada 6 Maret 2018, dihalau oleh aplikasi peer-to-peer yang telah "diracuni". Masalah-masalah rantai pasokan ditemukan tidak hanya di aplikasi tetapi juga di cloud dan meliputi ekstensi browser jahat, repositori Linux yang rentan, dan berbagai modul yang telah dipasang back door. Untuk menangani ancaman ini, organisasi beralih ke model rantai pasokan yang transparan dan tepercaya.

Data sangat berguna, tetapi terkadang data juga membantu mengetahui apa yang benar-benar terjadi di sebuah organisasi. Itulah alasan kami memasukkan pelajaran-pelajaran yang diperoleh di lapangan dari Tim Deteksi dan Respons (DART) kami. Termasuk di dalamnya adalah bagaimana sebuah perusahaan produksi besar mampu menerapkan kontrol untuk memblokir kampanye phishing multi-fase yang sudah menjangkiti mereka selama berbulan-bulan, dan organisasi-organisasi layanan keuangan yang akhirnya mampu memusnahkan pelaku ancaman dari sistem mereka menggunakan alat investigasi dan pemantauan endpoint canggih.

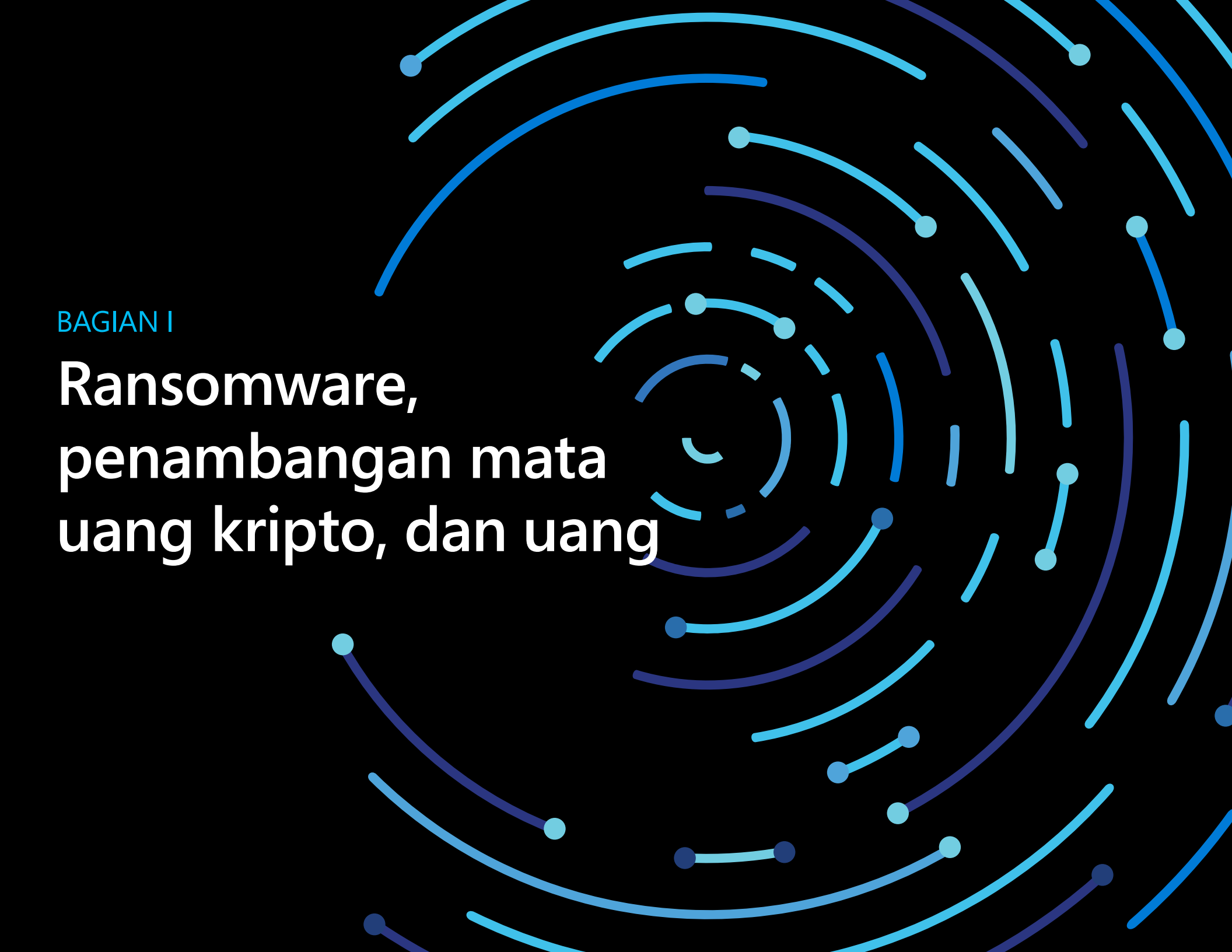
Terakhir tapi tidak kalah penting, korban phishing semakin banyak – tetapi model-model pembelajaran mesin semakin baik dalam mendeteksi tipuan sebelum mencapai data pengguna dan mencegah bahaya jika mereka mengkliknya. Berita baik lainnya? Semakin banyak perusahaan yang menerapkan solusi multi-faktor untuk membatasi keberhasilan email-email phishing pencuri sandi.

Pelaku serangan terus mencari kesempatan, sehingga semakin kita memahami teknik dan metode mereka, maka kita akan semakin siap dalam membangun pertahanan dan merespons dengan cepat. Langkah-langkah kecil yang penting dapat menciptakan perbedaan yang besar dalam keamanan siber sebuah organisasi. Oleh karena itu, selain wawasan mendalam tentang pergeseran lanskap malware dan serangan, Anda juga akan menemukan langkah-langkah yang disarankan dan pedoman praktik terbaik lain dalam laporan ini. Karena ketika dulu saya menjadi praktisi, itulah yang saya perlukan untuk melawan para pelaku kejahatan. Kami harap itu juga yang Anda perlukan.

Diana Kelley

CTO Lapangan Keamanan Siber Microsoft

N.B. Kami selalu ingin meningkatkan kualitas SIR. Jika Anda ingin memberikan masukan, silakan hubungi kami dan sampaikan masukan Anda.



BAGIAN I

Ransomware, penambangan mata uang kripto, dan uang

Kisah penting tentang keamanan di tahun 2017 sebagian besar melibatkan ransomware. Wabah utama ransomware thrust WannaCrypt dan Petya yang terjadi di seluruh dunia — jenis malware yang mengunci atau mengenkripsi komputer, kemudian meminta tebusan uang untuk memulihkan akses — menjadi kewaspadaan publik, dan banyak yang berspekulasi bahwa masalah ini akan semakin banyak terjadi di masa depan. Sebaliknya, menurun secara signifikan pada tahun 2018.

Penurunan insiden ransomware ini sebagian disebabkan karena meningkatnya deteksi dan edukasi sehingga pelaku penyerangan lebih sulit mengambil keuntungan dari insiden ini. Akibatnya, penyerang mulai mengalihkan upaya mereka menjauhi aksi ransomware ke pendekatan seperti penambangan mata uang kripto yang menggunakan sumber daya komputasi korban untuk membuat uang digital bagi para penyerang. Pergeseran ini menunjukkan sifat oportunistik fundamental kebanyakan penjahat siber yang berorientasi pada profit: mereka cenderung mengejar keuntungan termudah yang tersedia, dan ketika situasi ekonomi kejahatan siber berubah, mereka dengan cepat juga mengikutinya.

SERANGAN RANSOMWARE SEMAKIN MENURUN

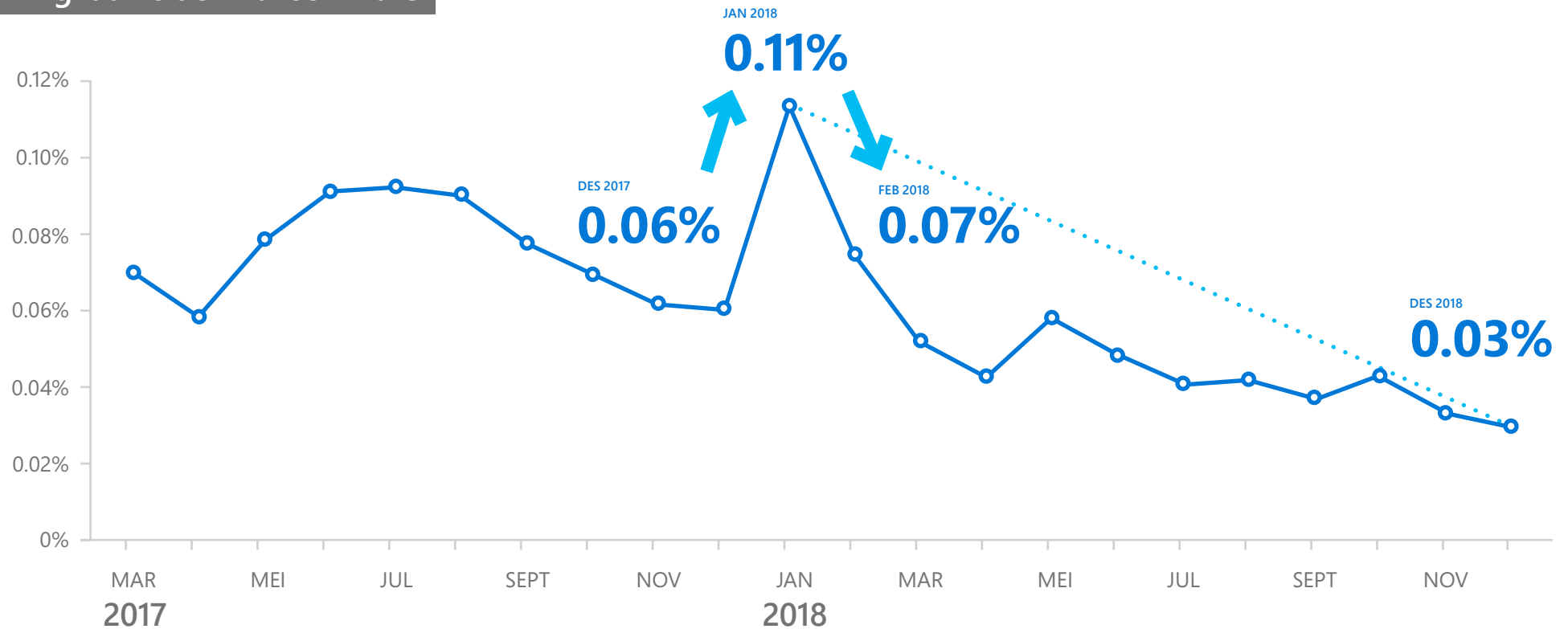
Lebih dari satu dekade lalu, para peretas dan pelaku prank yang mendominasi awal-awal malware gelap digantikan oleh kejahatan terorganisir dan kepentingan lain yang berorientasi pada profit. Apabila wabah malware pada awalnya seringkali terlihat mencolok dan jelas, malware yang berorientasi profit lebih cenderung beroperasi diam-diam dan tidak ingin menarik perhatian, agar terus dapat menjalankan fungsinya — mengirim spam, mencuri informasi sensitif, melakukan serangan penolakan layanan, dan aktivitas berbahaya lainnya — selama mungkin.

Ransomware berlawanan dengan tren ini. Bukannya mencoba untuk tetap tidak terdeteksi, ransomware secara terbuka menolak akses korban ke komputer mereka

dan file penting sampai korban membayar tebusan (dan bahkan sesudahnya; seringkali penyerang tidak serta-merta melepaskan kontrol mereka atas komputer tersebut, bahkan setelah tebusan dibayar).

Ketika ransomware memuncak pada tahun 2017, nampak seolah-olah gaya serangan terbuka ini mungkin mewakili fase baru dalam teknik penyerangan. Tetapi data yang lebih baru menunjukkan bahwa frekuensi ransomware mengalami penurunan, dan para penyerang banyak yang kembali ke modus operandi yang telah mereka gunakan di masa lalu, bersembunyi dari radar agar dapat melakukan serangan lebih efektif seperti dengan penambangan mata uang kripto. Meskipun telah terjadi penurunan frekuensi insiden ransomware, ini tidak berarti bahwa tingkat keparahan serangan juga menurun.

Tingkat Insiden Ransomware

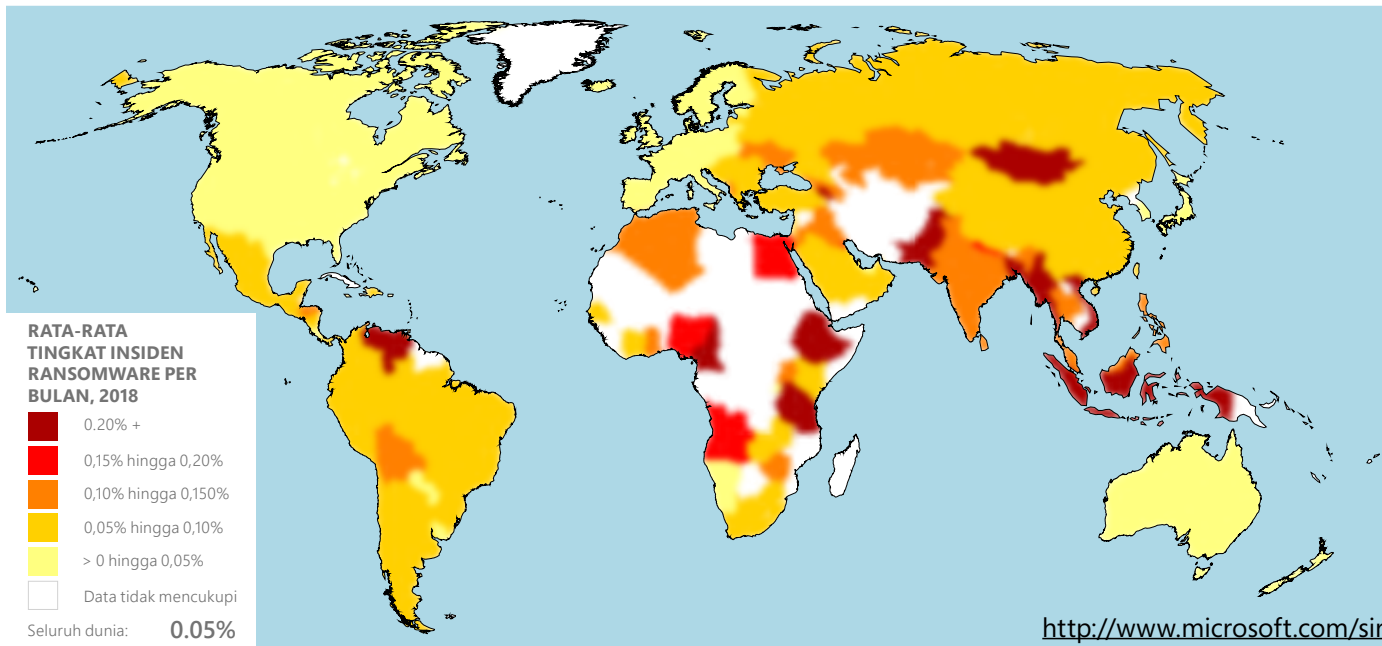


Tingkat insiden ransomware **menurun sekitar 60 persen** antara Maret 2017 hingga Desember 2018, dengan fase naik-turun sepanjang periode tersebut.

▲ **GAMBAR 1.**

Insiden ransomware dari Maret 2017 hingga Desember 2018

Mungkin ada banyak penyebab atas penurunan menyeluruh ini, meskipun para peneliti keamanan Microsoft menduga bahwa faktor utamanya adalah pengguna akhir maupun organisasi menjadi lebih waspada dan semakin cerdas dengan ancaman ransomware, termasuk lebih awas dan juga mencadangkan file penting sehingga dapat dipulihkan jika dienkrupsi oleh ransomware. Selain itu, seperti yang telah dijelaskan sebelumnya, penjahat siber bersifat oportunis.



◀ GAMBAR 2.

Rata-rata tingkat insiden ransomware per bulan di seluruh dunia berdasarkan negara/wilayah pada tahun 2018

NEGARA YANG PALING BANYAK TERSERANG RANSOMWARE: ETIOPIA



Rata-rata tingkat insiden per bulan: **0.77%**

Lima lokasi dengan rerata tingkat insiden ransomware bulanan tertinggi tahun 2018 adalah Etiopia (rerata tingkat insiden ransomware bulanan 0,77 persen), Mongolia (0,46), Kamerun (0,41), Myanmar (0,33), dan Venezuela (0,31), yang masing-masing memiliki rerata tingkat insiden ransomware bulanan 0,31 persen atau lebih besar selama periode tersebut.¹ Beberapa tahun lalu, insiden ransomware cenderung terjadi di negara dan wilayah makmur di Eropa dan Amerika Utara, tetapi karena ransomware mulai tidak menguntungkan para penyerang, pola insiden berubah menjadi lebih mirip dengan malware secara keseluruhan.

Lokasi dengan tingkat insiden ransomware terendah di tahun 2018 adalah Irlandia (0,01), Jepang (0,01), Amerika Serikat (0,02), Inggris (0,02), dan Swedia (0,02 persen), masing-masing memiliki rerata tingkat insiden ransomware bulanan 0,02 persen atau lebih kecil dalam periode yang sama. Lokasi dengan tingkat insiden yang rendah cenderung memiliki infrastruktur keamanan siber yang matang dan program yang mapan untuk melindungi infrastruktur penting dan menyampaikan komunikasi tentang keamanan dasar kepada warga negara mereka.

CATATAN KAKI

¹ Tingkat insiden adalah persentase komputer yang menjalankan produk keamanan real-time Microsoft yang melaporkan insiden malware. Mendeteksi ancaman bukan berarti komputer telah terinfeksi. Hanya komputer yang penggunaannya telah bersedia memberikan data ke Microsoft yang dipertimbangkan ketika menghitung tingkat temuan.

PENAMBANGAN MATA UANG KRIPTO SEMAKIN MENINGKAT

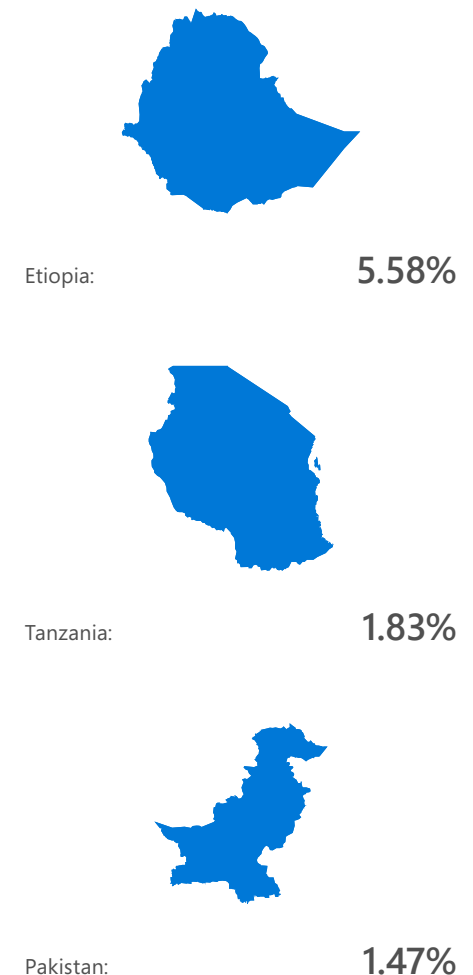
Mata uang kripto adalah uang virtual yang dapat digunakan untuk membeli dan menjual barang dan jasa secara anonim, baik secara online maupun di dunia nyata. Ada banyak jenis mata uang kripto, tetapi semuanya didasarkan pada teknologi blockchain, di mana setiap transaksi dicatat dalam buku besar terdistribusi yang dipelihara oleh ribuan atau jutaan komputer di seluruh dunia. Koin baru dibuat atau "ditambang" oleh komputer yang melakukan penghitungan kompleks yang juga berfungsi untuk memverifikasi transaksi blockchain.

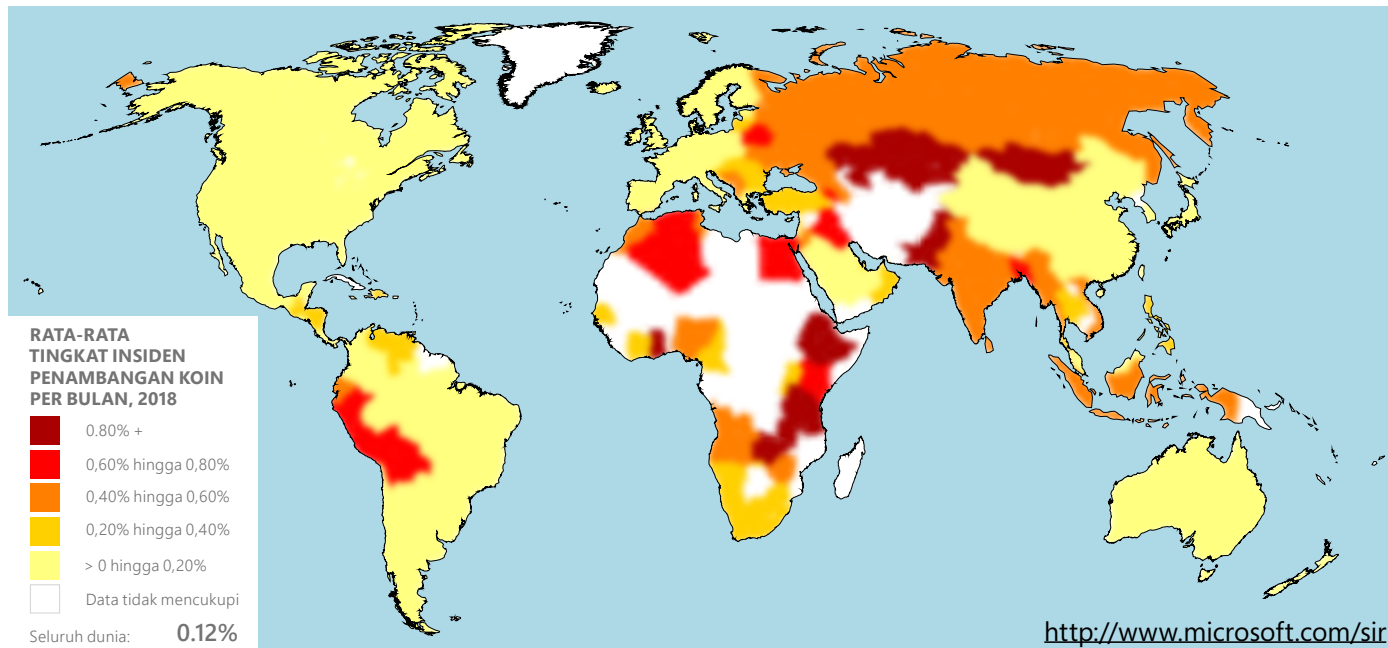
Menambang koin bisa sangat menguntungkan—pada tahun 2018, satu koin Bitcoin, mata uang kripto tertua dan paling populer, bernilai beberapa ribu dolar AS—tetapi melakukan perhitungan yang diperlukan bisa jadi memerlukan sumber daya intensif dan akan lebih meningkat ketika koin baru ditambang. Untuk mata uang populer seperti Bitcoin, keuntungan menambang koin hampir mustahil tanpa akses ke sumber daya komputasi yang sangat besar dan baik, dan biasanya ini di luar jangkauan bagi sebagian besar individu dan kelompok kecil. Karena alasan ini, penyerang yang mencari keuntungan gelap kini semakin berpaling ke malware yang memungkinkan mereka menggunakan komputer korban untuk membantu menambang koin mata uang kripto. Pendekatan ini memungkinkan mereka memanfaatkan kekuatan pemrosesan dari ratusan ribu komputer, bukan hanya satu atau dua. Bahkan ketika infeksi kecil ditemukan, sifat mata uang kripto yang anonim mempersulit upaya untuk melacak pihak yang bertanggung jawab.

Pada tahun 2018, rerata biaya bulanan penambangan koin mata uang kripto di seluruh dunia adalah 0,12 persen, dibandingkan dengan hanya 0,05 persen untuk ransomware. Banyak faktor yang berkontribusi terhadap meningkatnya popularitas penambangan sebagai muatan untuk malware. Tidak seperti ransomware, penambangan mata uang kripto tidak memerlukan input pengguna: karena bekerja di latar belakang, sementara pengguna melakukan tugas lain atau saat jauh dari komputer, dan mungkin sama sekali tidak akan mendeteksinya kecuali jika kinerja komputer menurun cukup signifikan. Akibatnya, pengguna cenderung tidak mengambil tindakan apa pun untuk menghapus ancaman, dan mungkin penambangan akan terus dilakukan untuk kepentingan penyerang dalam jangka waktu lama.

Ketersediaan produk "gelap" untuk penambangan rahasia banyak mata uang kripto adalah penggerak tren lainnya. Penghalangnya untuk masuk sangat kecil, ini karena luasnya ketersediaan perangkat lunak penambangan koin, yang dikemas ulang oleh para penjahat siber sebagai malware untuk dikirim ke komputer pengguna yang tidak menaruh curiga. Berbekal ini, para penambang kemudian mendistribusikannya kepada korban menggunakan banyak teknik yang sama yang umumnya digunakan penyerang untuk mengirim ancaman, seperti rekayasa sosial, eksploitasi, dan unduhan drive. Setelah perangkat lunak penambang diinstal, maka akan berjalan di latar belakang komputer korban untuk melakukan komputasi blockchain, dan penyerang akan mulai menuai hasilnya.

RATA-RATA TINGKAT INSIDEN PER BULAN DI NEGARA YANG PALING BANYAK TERSERANG PENAMBANGAN MATA UANG KRIPTO





GAMBAR 3.

Rata-rata tingkat insiden penambangan koin per bulan di seluruh dunia berdasarkan negara/wilayah pada tahun 2018

RATA-RATA TINGKAT INSIDEN PER BULAN DI NEGARA YANG PALING SEDIKIT TERSEERANG PENAMBANGAN MATA UANG KRIPTO



Irlandia:

0.02%



Jepang:

0.02%



Amerika Serikat:

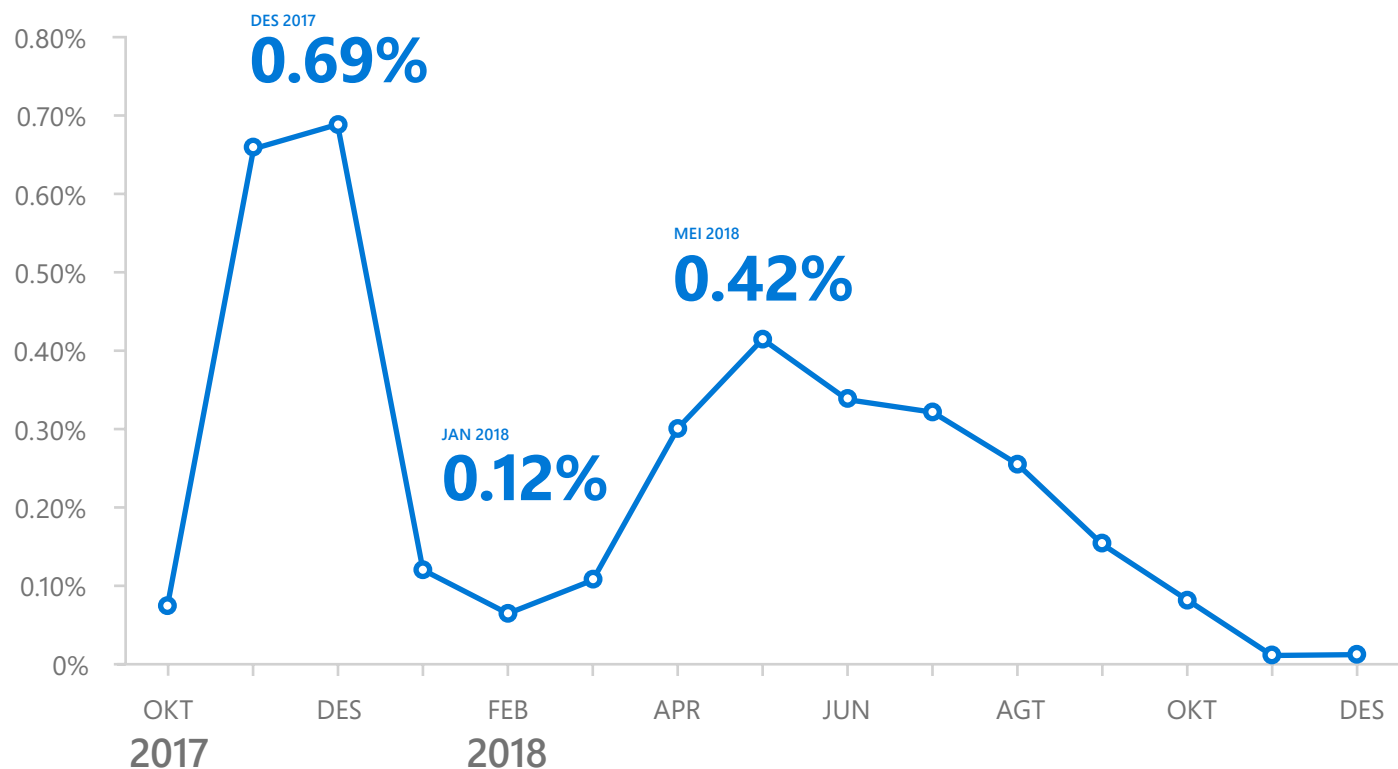
0.02%

Lima lokasi dengan tingkat insiden penambangan mata uang kripto tertinggi di tahun 2018 adalah Etiopia (5,58), Tanzania (1,83), Pakistan (1,47), Kazakhstan (1,24), dan Zambia (1,13), yang masing-masing memiliki rerata tingkat insiden penambangan koin per bulan sekitar 1,13 persen atau lebih besar selama periode tersebut. Lokasi dengan tingkat insiden penambangan koin terendah di tahun 2018 adalah Irlandia, Jepang, Amerika Serikat, dan Cina, yang masing-masing memiliki rerata tingkat insiden penambangan koin per bulan sekitar 0,02 persen selama periode tersebut.

PENAMBANG MATA UANG KRIPTO BERBASIS BROWSER: JENIS ANCAMAN BARU

Statistik yang disajikan dalam bagian ini melibatkan penambang mata uang kripto berbahaya yang dirancang untuk diinstal pada komputer korban sebagai malware. Namun, beberapa ancaman penambangan mata uang kripto yang paling signifikan sepenuhnya didasarkan pada browser web dan sama sekali tidak perlu diinstal. Sejumlah layanan mengiklankan penambangan mata uang kripto berbasis browser sebagai cara bagi pemilik situs web untuk memonetisasi lalu lintas ke situs mereka tanpa bergantung pada iklan. Pemilik situs harus menambahkan kode JavaScript ke halaman yang menambang mata uang kripto di latar belakang saat pengguna mengunjungi situs, dengan performa hasil dibagi antara pemilik situs dan layanan. Sayangnya, penyerang dengan cepat mengambil keuntungan

Tingkat Insiden Brocoiner



dari layanan ini untuk menambang mata uang kripto tanpa persetujuan dari pengguna akhir, seringkali dengan cara mengorbankan situs web yang sah dan menyisipkan kode pertambangan berbahaya ke kode sumber mereka. Penambang berbasis browser ini tidak perlu mengorbankan komputer pengguna akhir sama sekali, dan akan berjalan di platform apa pun dengan browser web berkemampuan JavaScript. Seperti trojan penambang mata uang kripto, penambang berbasis browser dapat menurunkan kinerja komputer secara signifikan dan memboroskan biaya listrik saat pengguna mengunjungi halaman web yang terpengaruh.

◀ GAMBAR 4.

Tingkat insiden Brocoiner, penambang mata uang kripto berbasis browser yang paling lazim

DAMPAK PENAMBANGAN MATA UANG KRIPTO YANG TIDAK DIHARAPKAN

Ancaman paling nyata yang dihadapi korban dari pertambangan mata uang kripto berbahaya adalah konsumsi sumber daya komputasi, yang dapat memboroskan listrik dan kinerja komputer menurun secara signifikan. Pengguna dan organisasi juga menghadapi risiko lain dari penambangan koin ini, termasuk:

- !** Sebagai batu loncatan untuk melakukan kerusakan yang lebih besar di masa depan.

Seperti bentuk malware lainnya, penambangan mata uang kripto dapat menjadi titik masuk bagi penyerang. Sementara komputer sedang menambang mata uang kripto di latar belakang, penjahat siber dapat belajar tentang lingkungan dan bisa saja menemukan celah dalam keamanan untuk mengeksploitasi dengan tujuan lain.
- !** Perangkat yang tersambung ke internet dapat diinfeksi dan diubah menjadi bot untuk penambangan mata uang kripto.

Banyak perangkat dengan fitur keamanan internal yang kurang memadai seperti deteksi ancaman malware, dapat menjadi sasaran empuk untuk penyerang.
- !** Mesin yang berbahaya.

Perangkat lunak pertambangan mata uang kripto yang berjalan terus-menerus selama berbulan-bulan atau lebih dapat mengganggu kinerja, dan panas yang dihasilkan oleh konsumsi daya yang berlebihan dan penggunaan CPU dapat merusak komputer.

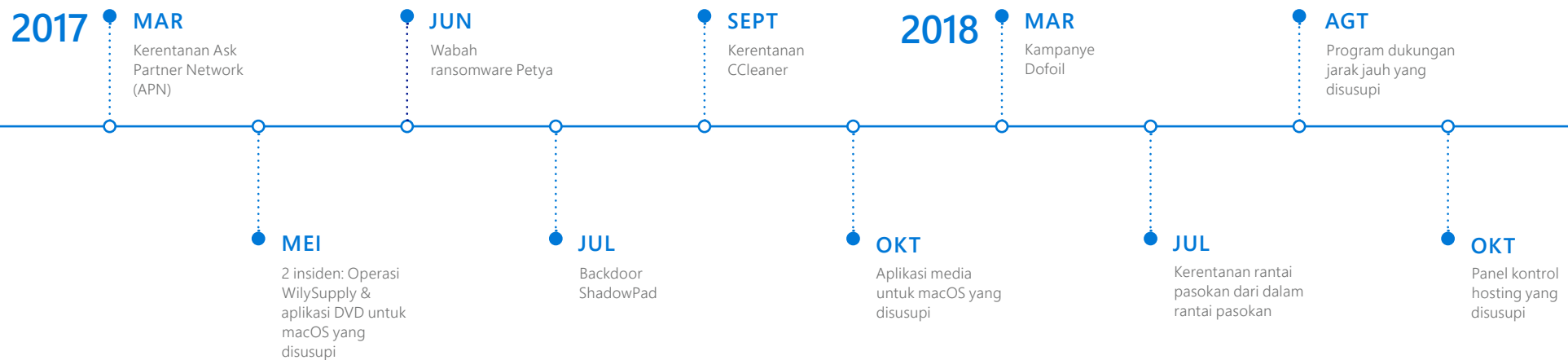
BAGIAN II

Rantai pasokan perangkat lunak terancam



Selama bertahun-tahun, Microsoft telah melacak pelaku ancaman yang menggunakan [kelemahan rantai pasokan](#) sebagai titik masuk penyerangan. Dalam serangan rantai pasokan, penyerang berkonsentrasi untuk melemahkan proses pengembangan atau pembaruan dari penerbit perangkat lunak yang sah.

Jika berhasil, penyerang dapat menggabungkan komponen yang telah dilemahkan tadi ke aplikasi yang sah atau paket pembaruan yang kemudian akan didistribusikan ke pengguna perangkat lunak. Kode berbahaya kemudian akan berjalan dengan kepercayaan dan izin yang sama dengan perangkat lunak. **Peningkatan jumlah serangan rantai pasokan perangkat lunak selama beberapa tahun terakhir** telah menjadi topik penting dalam banyak percakapan keamanan siber dan merupakan sumber kekhawatiran utama di banyak departemen TI.



SERANGAN BESAR RANTAI SUPLAI PERANGKAT LUNAK DI TAHUN 2017

Pada tahun 2017, serangan rantai suplai bertanggung jawab atas sejumlah insiden utama, yang paling terkenal adalah [wabah ransomware Petya](#) ipada bulan Juni, yang setelah dilacak berawal dari infeksi penyusupan pada proses pembaruan untuk aplikasi akuntansi pajak populer di Ukraina. Pada bulan Mei, [Operation WilySupply](#) menyusupi pembaruan perangkat lunak editor teks untuk menginstal backdoor pada organisasi target di sektor keuangan dan TI. Pada bulan Juli, sebuah backdoor bernama [ShadowPad](#) disembunyikan dalam paket perangkat lunak manajemen server, dan memungkinkan penyerang menginstal muatan malware tambahan untuk pencurian data dan kegiatan berbahaya lainnya. Pada bulan September, infrastruktur yang alat freeware populer CCleaner disusupi dan [versi yang telah diinfeksi backdoor](#) dikirim ke basis penggunanya.

▲ GAMBAR 5.

Serangan rantai suplai perangkat lunak pada tahun 2017 dan 2018

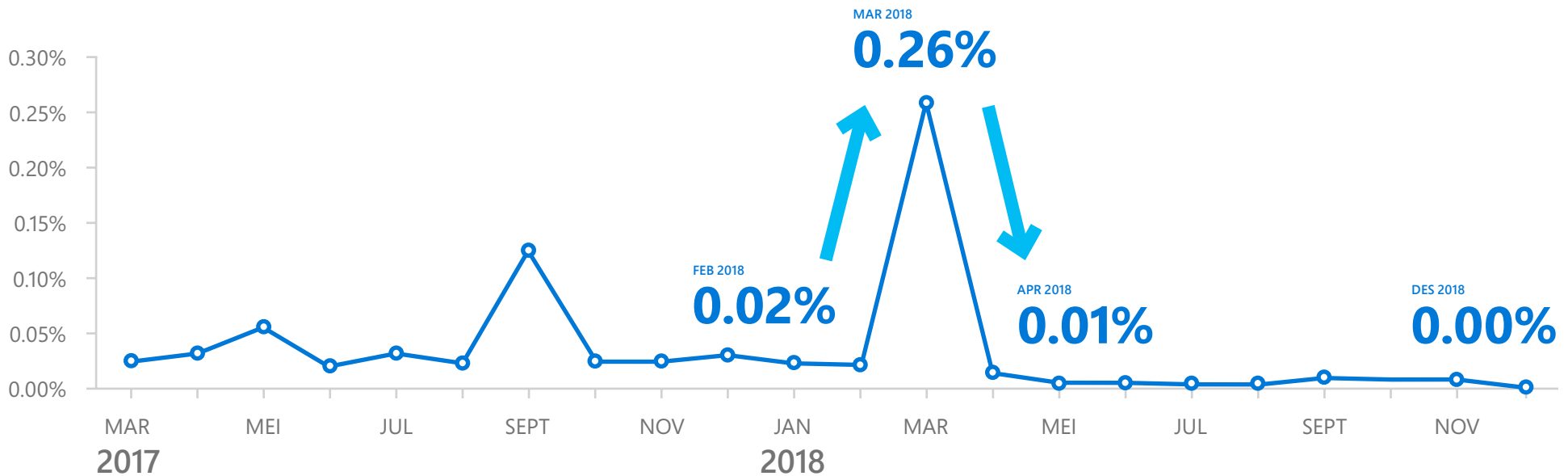
SERANGAN RANTAI SUPLAI PERANGKAT LUNAK PADA 2018 – AKAR PENYEBAB DAN DAMPAK

Insiden serangan rantai pasokan perangkat lunak besar pertama terjadi pada tanggal 6 Maret, ketika Windows Defender ATP memblokir kampanye masif untuk mengirim trojan Dofail (juga dikenal sebagai Smoke Loader). Kampanye malware masif ini dilacak ke aplikasi peer-to-peer yang diracuni. Paket pembaruan aplikasi diganti dengan yang berbahaya yang mengunduh kode yang telah disusupi, yang kemudian menginstal malware Dofail. Trojan canggih membawa muatan penambangan koin, dan menunjukkan teknik injeksi, mekanisme persistensi, dan metode penghindaran proses silang yang mutakhir.

▼ GAMBAR 6.

Insiden trending Dofail (Smoke Loader) di tahun 2018 menunjukkan lonjakan pemblokiran pada bulan Maret

Tingkat Insiden Dofail



Dalam 12 jam pertama kampanye tersebut, Windows Defender Antivirus **memblokir lebih dari 400.000 upaya infeksi di seluruh dunia.** Rusia menyumbang 73 persen dari insiden global, dengan Turki dan Ukraina menyusul yaitu masing-masing 18 persen dan 4 persen.

Beberapa serangan lainnya terdeteksi menggunakan rantai pasokan perangkat lunak yang disusupi sebagai mekanisme pengiriman di tahun 2018, termasuk yang dijelaskan dalam tabel berikut:

Periode	Serangan	Deskripsi	Perangkat lunak yang terpengaruh
Maret 2018	Kampanye penambangan koin Dofail (dilaporkan oleh Microsoft).	Penyerang menginfeksi proses pembaruan aplikasi peer-to-peer untuk menginstal Dofail, yang pada akhirnya menginstal malware penambangan koin.	Aplikasi peer-to-peer.
Juli 2018	Rantai pasokan yang disusupi di dalam rantai pasokan (dilaporkan oleh Microsoft).	Penyerang menyusupi infrastruktur bersama antara vendor aplikasi PDF editor dan salah satu mitra vendor perangkat lunaknya.	Aplikasi PDF editor dan vendor mitra pihak ketiga.
Agustus 2018	Program dukungan jarak jauh yang disusupi (Operasi Tanda Tangan Merah, dilaporkan oleh Trend Micro dan IssueMakersLab).	Server pembaruan penyedia solusi dukungan jarak jauh disusupi untuk memberikan alat akses jarak jauh yang disebut 9002 RAT.	Program dukungan jarak jauh.
Oktober 2018	Solusi panel kontrol hosting yang disusupi (dilaporkan oleh ESET).	Skrip instalasi untuk solusi panel kontrol hosting dimodifikasi untuk mencuri kredensial.	Solusi panel kontrol hosting.

◀ GAMBAR 7.

Serangan rantai suplai perangkat lunak lainnya pada tahun 2018

KEPERCAYAAN TERANCAM

Serangan rantai pasokan termasuk berbahaya karena mereka mengambil keuntungan dari kepercayaan yang ditanamkan pengguna dan departemen TI dalam perangkat lunak yang mereka gunakan. Perangkat lunak yang disusupi biasanya ditandatangani dan disertifikasi oleh vendor, dan mungkin tidak menunjukkan indikasi adanya kesalahan, yang secara signifikan menjadikannya lebih sulit untuk mendeteksi infeksi. Mereka dapat merusak hubungan antara rantai pasokan dan pelanggan, yaitu pengguna korporat atau pengguna rumahan. Dengan menginfeksi perangkat lunak dan distribusi yang telah disusupi atau infrastruktur pembaruan, serangan rantai pasokan dapat memengaruhi integritas dan keamanan barang dan jasa yang disediakan oleh organisasi.

Serangan rantai pasokan telah memengaruhi berbagai macam perangkat lunak dan organisasi yang ditargetkan di berbagai sektor dan lokasi geografis. Ancaman serangan rantai pasokan adalah masalah umum industri yang memerlukan perhatian dari beberapa pemangku kepentingan, termasuk pengembang perangkat lunak dan vendor yang menulis kode, administrator sistem yang mengelola instalasi perangkat lunak, dan komunitas keamanan informasi yang menemukan serangan ini dan menciptakan solusi untuk melindungi pengguna dan perangkat lunak dari serangan tersebut.

TIDAK HANYA PERANGKAT LUNAK: RANTAI PASOKAN DISUSUPI MELALUI OBJEK DI CLOUD

Kemampuan serangan rantai pasokan untuk melemahkan kepercayaan semakin kuat dan kompleks di cloud. Beberapa insiden penyusupan objek cloud, layanan, dan infrastruktur di tahun 2018 menyoroti kompleksitas ini:

- Ekstensi Chrome yang telah terinfeksi menginstal malware klik-penipuan (dilaporkan oleh [ICEBRG](#))
- Berbagai kerentanan repositori Linux (dilaporkan dalam beberapa forum online)
- Plug-in Wordpress berbahaya digunakan untuk berbagai kegiatan berbahaya, termasuk memungkinkan penyerang untuk mempublikasikan konten di situs Wordpress (dilaporkan oleh [Wordfence](#))
- Gambar Docker berbahaya yang berisi skrip untuk mengunduh malware penambangan koin mata uang kripto dan diunggah ke akun Docker Hub (dilaporkan oleh [Fortinet](#) dan [Kromtech](#))
- Sebuah paket typo-squatting berbahaya di repositori Python resmi; paket berisi skrip berbahaya yang mengunduh malware yang digunakan untuk membajak alamat penambangan koin di clipboard (dilaporkan di [Medium](#))
- Skrip yang disusupi di StatCounter memungkinkan penyerang menyuntikkan skrip berbahaya di situs web yang menggunakan StatCounter (dilaporkan oleh [ESET](#))

- Beberapa insiden modul npm berisi backdoor ([The npm Blog](#), [Medium](#)) yang, jika dieksploitasi, dapat mengakibatkan situasi seperti misalnya, penyerang dapat memasukkan kode arbitrer ke server yang sedang berjalan dan menjalankannya.

Insiden ini menunjukkan bagaimana penyusupan rantai pasokan dapat memperluas kemungkinan serangan. Jika tidak dilindungi, objek cloud dapat menjadi vektor entri yang tidak terduga. Misalnya, insiden Docker Hub melibatkan akun berbahaya yang mengunggah gambar Docker yang berisi backdoor penambangan koin tersembunyi. Gambar Docker dihosting di Docker Hub selama hampir satu tahun dan diunduh jutaan kali serta digunakan oleh administrator dan pengguna yang tidak menaruh curiga.

Risiko rantai pasokan meluas ke kode di cloud, open source, pustaka web, kontainer, dan objek lainnya di cloud. Risiko ini, ditambah dengan tingginya tingkat variasi di antara insiden perangkat lunak dan rantai pasokan hardware yang disusupi yang telah terdeteksi, membuat serangan rantai pasokan sebagai kategori ancaman yang luas. Meskipun tidak ada solusi tunggal untuk seluruh spektrum jenis serangan ini, organisasi perlu menerapkan [perlindungan preventif dan deteksi pasca pembobolan](#) dari serangan rantai pasokan dari pemasok hardware dan perangkat lunak yang disusupi, vendor dan akuisisi, pemasok perangkat lunak open source, serta layanan cloud dan pemasok infrastruktur.

Menyelidiki insiden siber dengan DART

Tim Deteksi dan Respons (DART) Microsoft adalah tim global yang terdiri dari pakar keamanan siber dan responden insiden yang membantu organisasi mendeteksi, menyelidiki, dan menanggapi insiden keamanan siber. Bagian ini menyoroti beberapa kasus pelanggan yang ditangani DART pada tahun lalu; menggambarkan tren penyerang umum dan bagaimana Microsoft dan pelanggan mampu mengaggalkannya.



ORGANISASI LAYANAN PROFESIONAL MENGALAMI SERANGAN PENARIKAN DATA NASIONAL

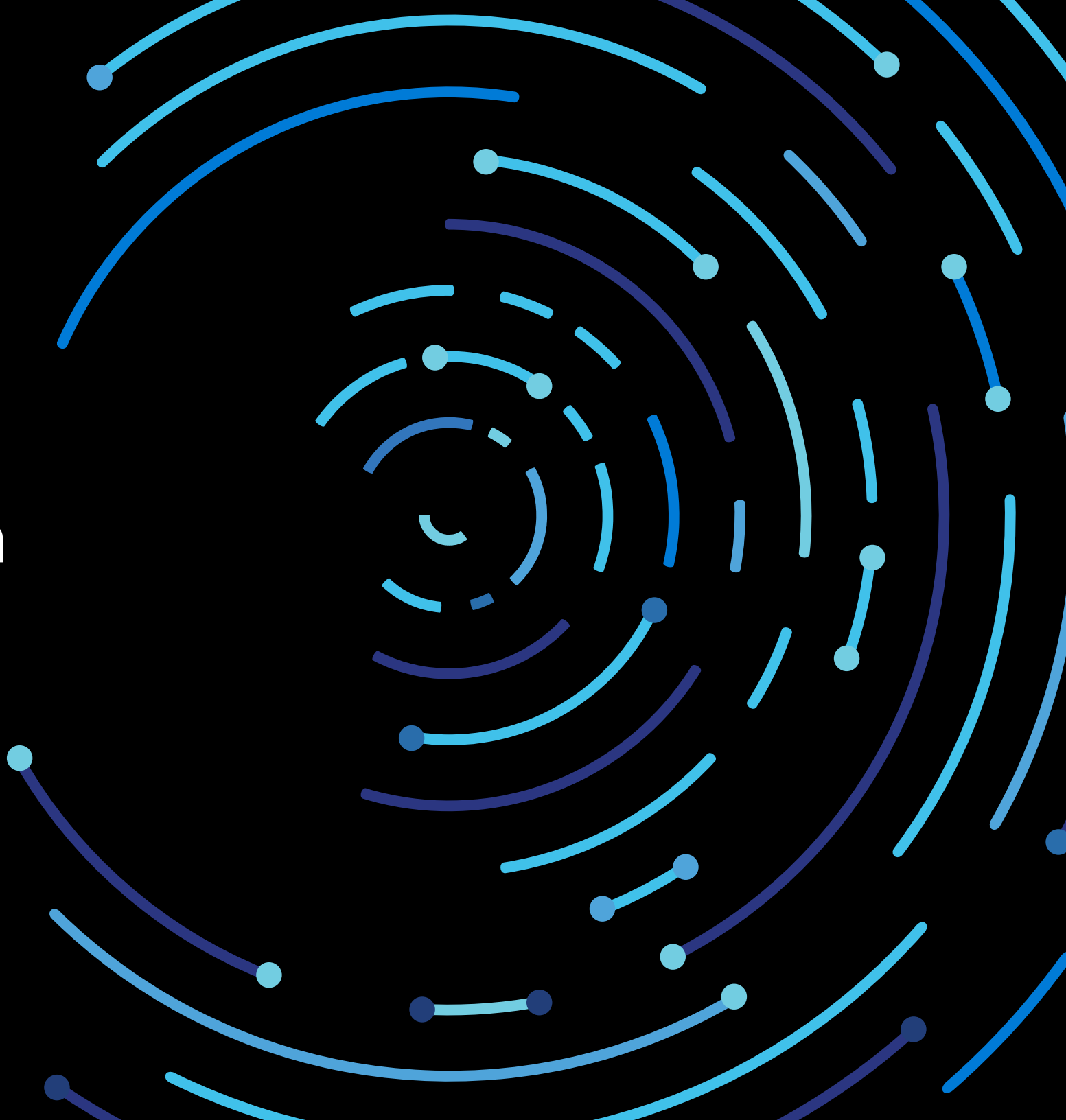
Sebuah organisasi layanan profesional mengalami ancaman persisten canggih (APT) bersponsor nasional untuk mengambil alih akses ke kredensial khusus organisasi tersebut. Para penyerang memperoleh akses ke jaringan dengan menggunakan serangan acak kata sandi, di mana mereka menggunakan sejumlah kecil kata sandi yang lemah atau umum digunakan (seperti "p@ssword" atau "123456") untuk menasar sejumlah besar akun pengguna dan mendapatkan kredensial administratif Office 365. (Serangan acak kata sandi digunakan untuk menghindari pendeteksian dengan membatasi jumlah upaya login untuk setiap akun.) Setelah menyusup ke jaringan, APT melakukan penarikan data yang rumit dan otomatis dari kotak pesan karyawan. Meskipun beberapa upaya internal dilakukan untuk menanggulangnya, penyusup tetap berada dalam jaringan selama lebih dari 200 hari. Sebagai bagian dari serangan ini, penyusup memanfaatkan perangkat lunak rantai pasokan organisasi dan penarikan data secara otomatis.

Karena mereka mencurigai adanya pembobolan data pelanggan, organisasi tersebut melibatkan tim DART untuk menyelidiki dan membantu mencegah kerusakan lebih lanjut. DART mengidentifikasi pencarian kotak pesan Office 365 tertarget, akun yang disusupi, dan saluran perintah dan kontrol penyerang. Pelajaran utama bagi pelanggan dari insiden ini adalah menerapkan kontrol untuk melindungi layanan cloud dari ancaman dan penyerang berbasis identitas. Organisasi mengadopsi otentikasi multi faktor (MFA), kebijakan akses bersyarat untuk aplikasi cloud tertentu, dan login Office 365. Untuk perlindungan tambahan terhadap ancaman serupa di masa depan, organisasi juga dapat mengadopsi solusi Deteksi Ancaman dan Respons Endpoint atau Endpoint Threat Detection and Response (EDR) untuk mendeteksi penyerang yang mungkin mencoba mengeksploitasi jaringan. Selain itu, kami merekomendasikan agar organisasi ini menunjuk badan

tata kelola cloud atau tim identitas global yang akan mengelola dan menerapkan kebijakan otentikasi pengguna yang sesuai, sehingga organisasi dapat mengawasi postur keamanan mereka dan dapat mengurangi risiko secara lebih efektif.

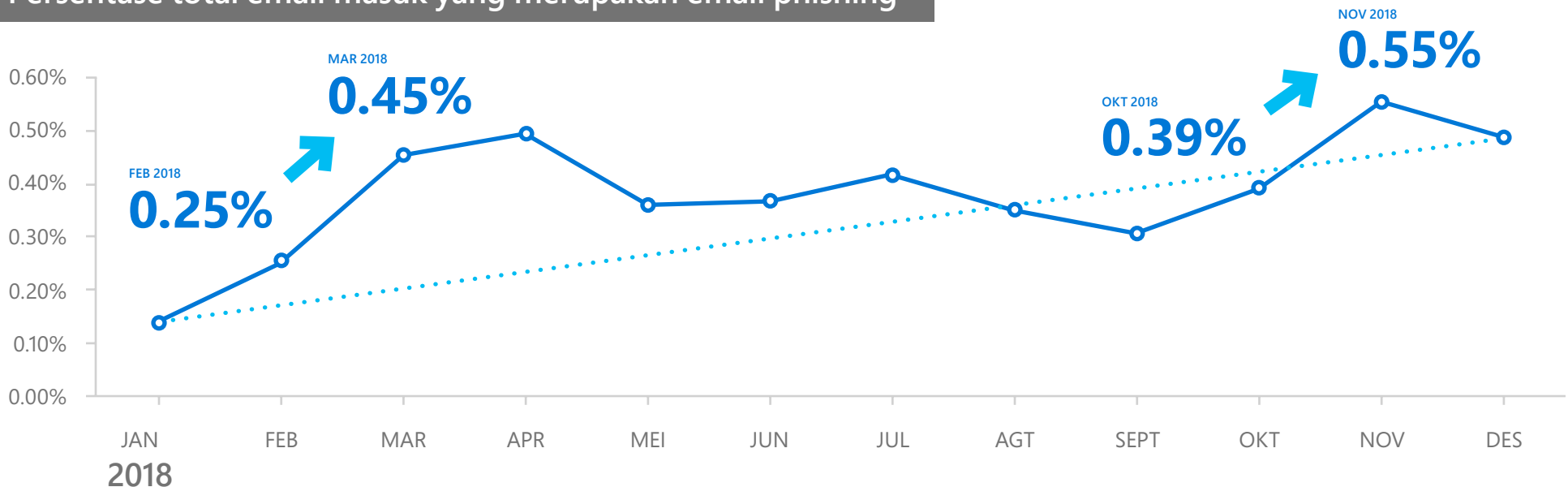
BAGIAN III

Phishing masih ada



Pada tahun 2018, analis ancaman Microsoft telah melihat bukti bahwa penyerang terus menggunakan phishing sebagai metode serangan yang disukai. Phishing akan tetap menjadi masalah di masa depan karena melibatkan keputusan dan penilaian manusia dalam menghadapi upaya gigih penjahat siber untuk membuat korban menggigit umpan mereka.

Tingkat phishing masih meningkat Persentase total email masuk yang merupakan email phishing



PHISHING TETAP MENJADI VEKTOR SERANGAN YANG DISUKAI SELAMA 2018

Microsoft menganalisis dan memindai phishing dan malware di lebih dari 470 miliar pesan email Office 365 setiap bulan, ini memberikan wawasan yang cukup bagi analis untuk mengetahui tren dan teknik penyerang. Porsi email masuk yang merupakan pesan phishing meningkat 250 persen antara Januari hingga Desember 2018. Phishing tetap menjadi salah satu dari vektor serangan utama yang digunakan untuk mengirimkan muatan zero-day yang berbahaya kepada pengguna, dan Microsoft terus melawan serangan ini dengan tambahan perlindungan, deteksi, investigasi, dan kemampuan respons anti-phishing untuk membantu melindungi pengguna.

▲ GAMBAR 8.

Email phishing selama 2018

Evolusi dalam metode serangan phishing

Semakin canggih alat dan teknik yang digunakan untuk melindungi orang dari phishing, penyerang dipaksa untuk beradaptasi. Bentuk serangan phishing menjadi semakin beragam, yang berarti penyerang tidak menggunakan satu URL, domain, atau alamat IP untuk mengirim email, tetapi memanfaatkan infrastruktur yang bervariasi dengan beberapa titik serangan. Sifat serangan itu sendiri juga telah berevolusi, dengan kampanye phishing modern mulai dari serangan jangka pendek yang aktif hanya selama beberapa menit hingga kampanye volume tinggi dengan durasi lebih panjang. Bentuk lain adalah serangan varian berseri, di mana penyerang mengirim sejumlah email selama beberapa hari berturut-turut.

Selain itu, Microsoft telah mengamati tren penyerang yang menggunakan infrastruktur yang dihosting dan infrastruktur cloud publik lainnya, sehingga menjadikannya lebih mudah menghindari deteksi dengan bersembunyi di antara situs dan aset yang sah. Misalnya, penyerang banyak menggunakan alat berbagi dokumen populer dan situs kolaborasi dan layanan untuk mendistribusikan muatan berbahaya dan formulir login palsu yang digunakan untuk mencuri kredensial pengguna. Juga telah terjadi peningkatan dalam penggunaan akun yang disusupi untuk kemudian mendistribusikan email berbahaya baik di dalam maupun di luar organisasi.

Kampanye phishing bervariasi, mulai dari kampanye tertarget hingga berbasis luas

Seperti pada distribusi malware secara umum, kampanye phishing bervariasi mulai dari tertarget hingga serangan yang umum dan berbasis luas. Meskipun serangan yang sangat canggih menghasilkan keuntungan uang yang lebih besar per akun yang terkena phishing, serangan yang lebih umum menghasilkan lebih sedikit uang per akun yang disusupi namun menjangkau pengguna yang lebih luas.

Contoh kampanye tertarget yang canggih adalah [Ursnif](#), di mana penyerang melokalisasi nama file dokumen agar spesifik untuk organisasi yang sudah mengenalnya atau industri target. Serangan semacam itu sangat berbeda dari kampanye berbasis luas dan terlihat lebih sah dan dapat dipercaya.

Beberapa kampanye berbasis luas di tahun 2018 berhubungan dengan kompromi email bisnis (BEC) dan peniruan merek yang dikenal, domain, atau pengguna dalam organisasi target dan kampanye spoofing canggih. Peniruan domain adalah taktik serangan yang umum digunakan untuk menjebak organisasi agar percaya bahwa email tersebut dapat dipercaya dan harus dibuka.

Umpan phishing hadir dalam berbagai bentuk

Para peneliti Microsoft telah menemukan bahwa banyak jenis umpan atau muatan phishing yang berbeda digunakan dalam kampanye, termasuk:

- **Spoofing domain** (domain pesan email sama persis dengan nama domain asli)
- **Peniruan domain** (domain pesan email mirip dengan nama domain asli)²
- **Peniruan pengguna** (pesan email terlihat seperti berasal dari seseorang yang Anda percayai)
- **Umpan teks** (pesan teks terlihat seperti berasal dari sumber yang sah seperti Bank, instansi pemerintah, atau perusahaan lain untuk meniru keabsahan klaim mereka dan biasanya meminta korban memberikan informasi sensitif seperti nama pengguna, kata sandi, atau data keuangan sensitif)
- **Tautan phishing kredensial** (pesan email berisi tautan ke halaman yang menyerupai halaman login untuk situs yang sah, sehingga pengguna akan memasukkan kredensial login mereka)
- **Lampiran phishing** (pesan email berisi lampiran file berbahaya di mana pengirim akan meminta korban untuk membukanya)

- **Tautan ke lokasi penyimpanan cloud palsu** (pesan email terlihat seperti berasal dari sumber yang sah dan membujuk pengguna untuk memberikan izin dan/atau memasukkan informasi pribadi seperti kredensial untuk dapat mengakses lokasi penyimpanan cloud palsu tersebut)

Berbagai umpan yang berpotensi dapat digunakan oleh penyerang meningkatkan kompleksitas ancaman phishing dan organisasi harus mampu mengenalinya.

CATATAN KAKI

² Peniruan domain bisa jadi mirip spoofing domain (sama persis dengan nama domain asli) dalam kasus tertentu di mana domain muncul dalam nama tampilan email.

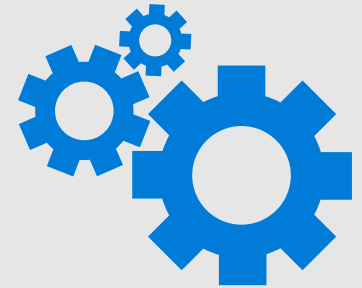
Menyelidiki insiden siber dengan DART

ORGANISASI MANUFAKTUR BESAR MENGALAMI INSIDEN PHISHING TERTARGET

Sebuah organisasi manufaktur mengalami kampanye phishing multi-fase dalam rentang beberapa bulan. Pendekatan seperti ini umum dilakukan. Selama fase pertama, penyerang akan melakukan pengintaian dan dalam fase kedua akan mengincar aset bernilai tinggi. Fase pertama dari kampanye ini memanfaatkan scam phishing terkenal yang didasarkan pada tautan halaman web yang tertanam dalam email yang dikirim ke sekelompok kecil target dalam organisasi. Email tersebut mengklaim bahwa target memiliki dokumen elektronik penting yang menunggu untuk ditinjau, dan semua penerima harus melakukan otentikasi dengan kredensial domain mereka untuk mendapatkan akses. Halaman arahan palsu yang telah diatur agar ditinjau oleh target karena disebut 'dokumen penting' ini sebenarnya adalah untuk mencuri kredensial dan memungkinkan penyerang mengakses akun Office 365 dari mana saja di dunia. Fase kedua dari kampanye phishing ditujukan untuk mengirim email phishing serupa ke aset bernilai tinggi di dalam organisasi manufaktur target, dengan harapan dapat memperoleh akses ke data yang lebih berharga. Microsoft terlibat dengan klien ini selama kampanye phishing fase kedua. Pelajaran utama dari insiden ini adalah: phishing tetap menjadi salah satu metode serangan yang paling efektif dan pengguna masih merupakan mata rantai

yang terlemah. Pelatihan pengguna untuk waspada terhadap scam phishing, menerapkan alat untuk mengidentifikasi penyerang dan mengambil tindakan, serta memperbaiki sistem secara teratur adalah langkah penting; jika organisasi tidak menerapkan salah satu dari langkah ini, maka bisa menjadi sangat rentan.

Dalam hal ini, kekhawatiran utama pelanggan adalah kebutuhan mendesak untuk memblokir akses ke akun yang disusupi. Dalam kemitraan dengan tim Azure Identity and Office 365, DART merancang rencana untuk membasmi penyerang dari jaringan dan memantau lalu lintas ke saluran perintah dan kontrol dengan menggunakan solusi Microsoft Azure Log Analytics baru. Tim dapat membantu menyelesaikan situasi ini hanya dalam tiga jam. Akses penyerang diblokir, dan organisasi dapat mengalihkan perhatian mereka ke evaluasi kerusakan dan pemulihan. DART menggunakan alat Azure Log Analytics untuk memburu perilaku penyerang, yang membantu mengungkap banyak kendala konfigurasi bagi organisasi. Misalnya, DART mengidentifikasi celah dalam patch server kritis, menemukan komputer di jaringan berkomunikasi dengan host yang dikenal buruk di internet, dan juga menemukan beberapa server penting tanpa perlindungan malware.



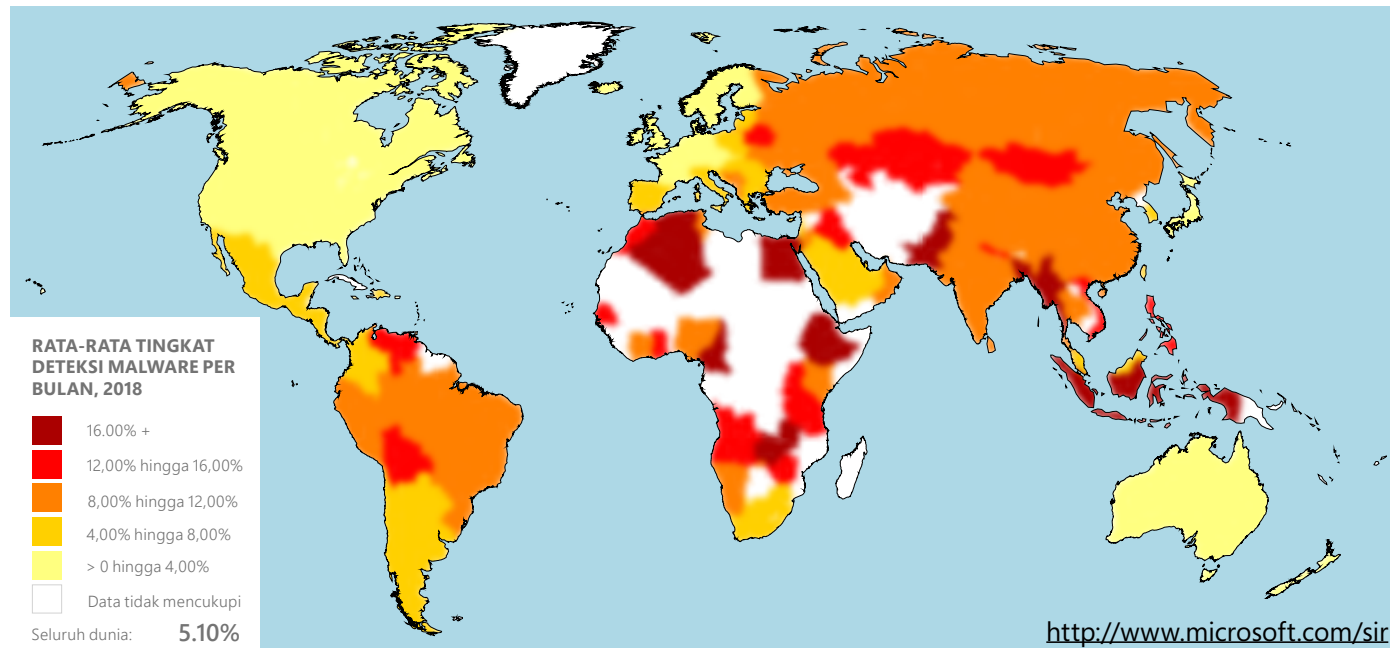


BAGIAN IV

Malware di seluruh dunia

Malware menimbulkan risiko untuk organisasi dan individu dalam bentuk gangguan penggunaan, kehilangan data, pencurian kekayaan intelektual, kerugian uang, tekanan emosional, dan bahkan dapat berisiko bagi keselamatan. Microsoft menggunakan beragam alat dan teknik untuk mengidentifikasi, memblokir, dan membasmi infeksi malware di mana pun mereka ditemukan.

Tingkat deteksi malware berkisar dari sekitar 5 persen menjadi lebih dari 7 persen di tahun 2017. Pada awal tahun 2018, semakin meningkat sebelum kemudian turun sepanjang tahun hingga menjadi hanya sedikit di atas 4 persen. Beberapa kemungkinan penyebab **penurunan tingkat deteksi malware di tahun 2018** adalah semakin banyaknya adopsi Windows 10 dan peningkatan penggunaan Windows Defender untuk perlindungan. Tingkat deteksi adalah persentase komputer yang menjalankan Windows Defender Antivirus yang melaporkan deteksi malware selama bulan tersebut, termasuk upaya infeksi yang diblokir Defender.



◀ **GAMBAR 9.**

Rata-rata tingkat deteksi malware per bulan di seluruh dunia berdasarkan negara/wilayah pada tahun 2018

Lima lokasi dengan deteksi malware tertinggi selama Januari-Desember 2018 adalah Etiopia (rerata tingkat deteksi malware bulanan 26,33 persen), Pakistan (18,94), wilayah pendudukan Palestina (17,50), Bangladesh (16,95), dan Indonesia (16,59), dengan rerata tingkat deteksi malware bulanan sekitar 16,59 persen atau lebih besar selama periode tersebut. Tingkat infeksi cenderung berhubungan erat dengan faktor pengembangan manusia dan kesiapan teknologi dalam masyarakat. Semua lokasi dengan tingkat deteksi tertinggi di tahun 2018 menduduki peringkat 40 persen terbawah negara-negara dan wilayah dalam indeks Information and Communications Technologies (ICT) 2017, yang diterbitkan oleh United Nations International Telecommunication Union (ICT) .

Lima lokasi yang memiliki deteksi malware terendah selama periode yang sama adalah Irlandia (1,26), Jepang (1,51), Finlandia (1,74), Norwegia (1,79), dan Belanda (1,82), yang semuanya memiliki tingkat dekteksi bulanan sebesar 1,82 persen atau lebih kecil selama periode tersebut. Negara-negara ini cenderung memiliki infrastruktur keamanan siber yang matang dan program yang mapan untuk melindungi infrastruktur penting dan menyampaikan komunikasi tentang keamanan dasar kepada warga negara mereka.

RATA-RATA TINGKAT DETEKSI PER BULAN DI NEGARA YANG PALING BANYAK TERSERANG MALWARE



Etiopia:

26.33%



Pakistan:

18.94%



Wilayah pendudukan
Palestina:

17.50%

Menyelidiki insiden siber dengan DART

BEBERAPA ORGANISASI LAYANAN KEUANGAN MENGALAMI SERANGAN NASIONAL YANG MENGGANGGU OPERASIONAL

Dalam salah satu dari insiden yang sangat merugikan, DART telah melihat, beberapa organisasi layanan keuangan ditargetkan oleh APT bersponsor nasional (kelompok yang berbeda dari yang menargetkan organisasi layanan profesional yang disebutkan sebelumnya) yang menjalankan metode serupa.

APT ini memperoleh akses administratif setelah menginfeksi mesin zero pasien dengan implan backdoor yang sangat tertarget dan obfusif, mungkin dikirim melalui email spear phishing. Selanjutnya, APT mengeksekusi beberapa transaksi curang, mentransfer uang dalam jumlah besar ke rekening bank asing. Dalam beberapa kasus, penyerang tetap tidak terdeteksi selama lebih dari 100 hari. Setelah penyerang menyadari bahwa mereka terdeteksi, penyerang dengan cepat mengarahkan serangan pra-staging, memberikan malware destruktif ke lebih dari separuh sistem dalam lingkungan itu; operasi pelanggan ditutup selama beberapa hari.

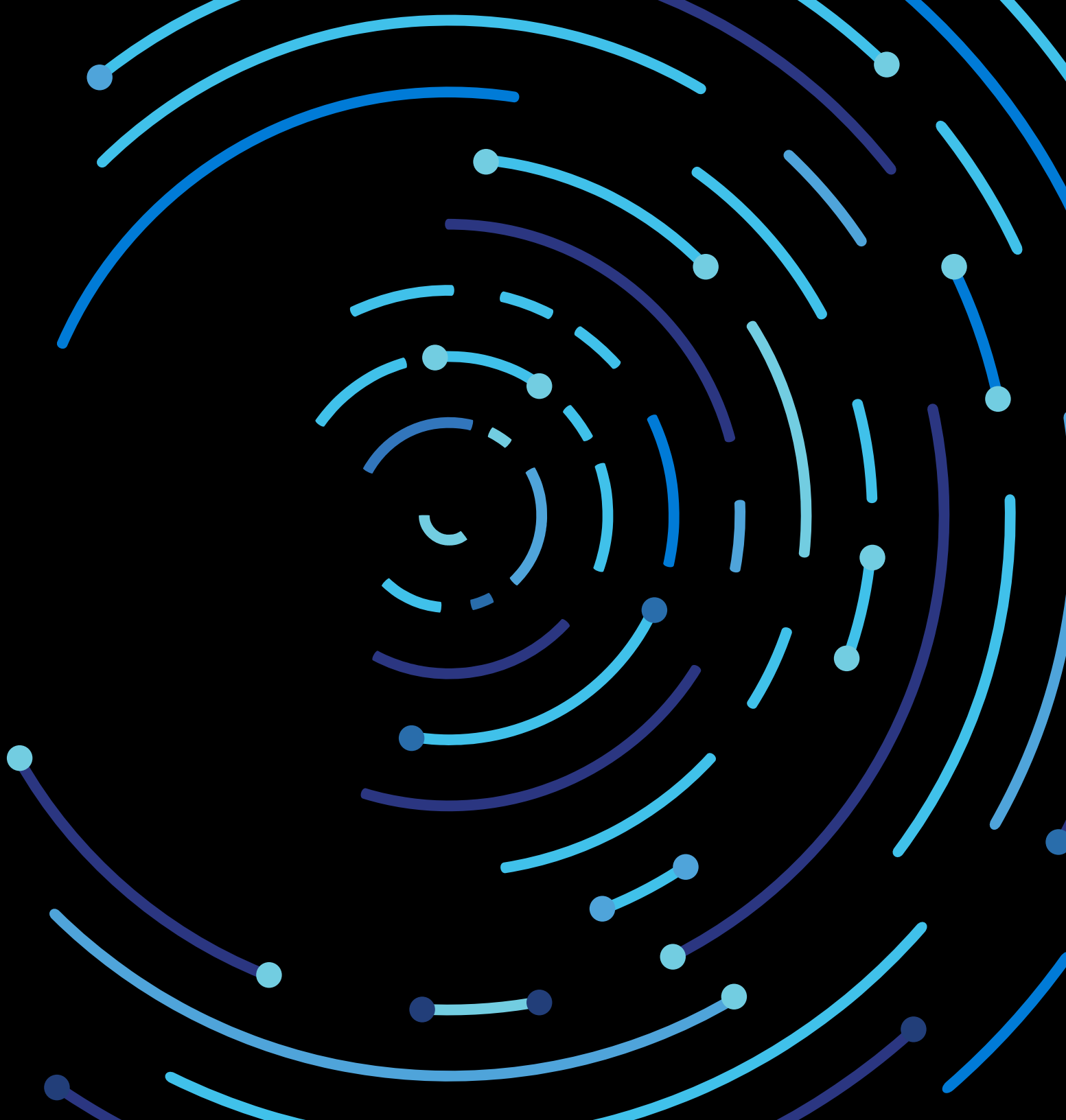
Ada beberapa pelajaran penting bagi pelanggan dari insiden ini. Yang pertama adalah bahwa manajemen siklus hidup perangkat lunak sangat penting, yang mencakup memastikan pembaruan sistem secara teratur (sistem operasi dan keamanan), patching,

dan audit. Dalam satu kasus, sebuah organisasi di lingkungan sistem Linux yang memiliki jumlah beban kerja yang sangat besar sama sekali tidak dikelola, sehingga menempatkannya pada risiko yang sangat rentan serangan. Pelajaran kedua adalah penting untuk mempertahankan cadangan data sistem di lokasi offline jika data utama hilang. Pelajaran lain adalah bahwa solusi antivirus tradisional mungkin kurang memadai jika Anda tahu tentang aktivitas lawan yang sebenarnya.

Kembali ke mode operasional normal adalah prioritas tertinggi untuk organisasi ini. DART membantu mengembalikan layanan dengan terlebih dulu menyelidiki dampak dan kemudian mengambil tindakan mitigasi yang diperlukan, seperti menghapus malware dari sistem yang terpengaruh dan memulihkannya ke kondisi yang sehat. Tim juga melatih pelanggan tentang cara menggunakan alat investigasi ancaman Microsoft, termasuk EDR dan yang lainnya, sehingga mereka dapat mencari perilaku anomali dan aktivitas penyerang di jaringan mereka. DART menekankan bahwa pemantauan endpoint sangat penting untuk membentengi dari serangan canggih dan tertarget yang mungkin tidak terdeteksi oleh solusi antivirus tradisional.



Panduan



Panduan

Membangun ketahanan organisasi dan mengurangi risiko memerlukan pendekatan keamanan yang mencakup pencegahan, deteksi, dan respons. Kami telah menyusun rekomendasi praktik dan kontrol keamanan terbaik berikut ke dalam kategori tersebut.

PENCEGAHAN:

Kontrol preventif memainkan peran kunci dalam strategi pertahanan secara keseluruhan karena investasi yang tepat dapat menimbulkan kerugian besar bagi penjahat siber dan mempertahankan kerugian besar tersebut dari waktu ke waktu (tanpa memerlukan analis ahli untuk memantau dan menafsirkan output). Investasi kontrol preventif harus ditargetkan pada teknik yang paling hemat biaya untuk menghapus teknik serangan yang murah dan efektif secara kontinu.

Empat hal yang perlu dipertimbangkan dalam pencegahan adalah:

1. Kebersihan keamanan sangat penting. Seperti yang terlihat dalam beberapa insiden siber yang disebutkan dalam laporan ini, masalah kebersihan umum dapat merusak kemampuan keamanan yang canggih, sehingga mengikuti tips ini dapat membantu mengurangi risiko:

- Hindari penggunaan perangkat lunak gratis dan/atau bajakan yang tidak dikenal. Hanya gunakan perangkat lunak dari sumber tepercaya.
- Mitigasi risiko pencurian kredensial, termasuk mengamankan akun khusus administrator.

Untuk mempelajari caranya, baca [blog](#) ini, yang menguraikan beberapa prinsip penting dan alat yang digunakan Microsoft untuk memandu dan meningkatkan postur keamanan kami dan beberapa saran untuk membantu Anda merencanakan inisiatif Anda sendiri.

- Terapkan basis dasar konfigurasi aman yang disediakan oleh vendor perangkat lunak Anda.
- Selalu perbarui mesin dengan segera menerapkan pembaruan ke sistem operasi dan aplikasi Anda, dan segera terapkan pembaruan keamanan penting untuk OS, browser, dan email. Mengisolasi (atau menghentikan penggunaan) mesin yang tidak dapat diperbarui atau ditambal.
- Menerapkan perlindungan browser dan email tingkat lanjut. Gunakan gateway email aman yang memiliki kemampuan perlindungan ancaman tingkat lanjut yang mampu bertahan dari varian phishing modern.
- Aktifkan host anti-malware dan pertahanan jaringan untuk mendapatkan respons pemblokiran mendekati real-time dari cloud (jika tersedia dalam solusi Anda).

2. Menerapkan kontrol akses. Pertimbangkan hal berikut:

- Menerapkan prinsip hak khusus paling sedikit, yang mencakup penerapan segmentasi jaringan, menghapus hak administrator lokal dari pengguna akhir, dan waspada saat memberikan izin pada aplikasi yang berjalan di komputer.
- Batasi pengunduhan aplikasi hanya dari sumber tepercaya (app store resmi).
- Menyebarkan kebijakan integritas kode yang kuat, termasuk membatasi aplikasi yang dapat dijalankan pengguna. Jika memungkinkan, adopsi solusi keamanan yang akan membatasi kode yang berjalan di inti sistem (kernel) dan dapat memblokir skrip yang tidak ditandatangani dan bentuk lain dari kode yang tidak tepercaya. Gunakan daftar putih aplikasi.
- Untuk mempelajari tentang serangan rantai pasokan perangkat lunak dan cara melindungi sistem Anda, baca blog ini dari peneliti Microsoft.

3. Simpan cadangan.

- Buat cadangan yang tidak dapat dimusnahkan untuk sistem dan data penting Anda.
- Gunakan layanan penyimpanan cloud untuk pencadangan data otomatis secara online. Untuk data yang ada di lokasi, secara teratur cadangkan data penting menggunakan aturan 3-2-1. Simpan tiga cadangan data, pada dua jenis penyimpanan yang berbeda, dan setidaknya satu cadangan offsite.

4. Berhati-hatilah dan ambil tindakan jika Anda mencurigai apa pun.

- Ajarkan karyawan untuk waspada terhadap komunikasi yang mencurigakan yang meminta informasi sensitif dan ajarkan mereka cara menanggapi dan segera melaporkannya kepada tim operasi keamanan organisasi. Pelatihan juga dapat membantu mengurangi serangan rekayasa sosial dan spear-phishing.
- Berhati-hatilah saat mengeklik tautan web. mempraktikkan kebiasaan penelusuran web yang aman dan menggunakan solusi yang memberikan peringatan tentang atau memblokir akses ke situs yang tidak aman dapat membantu mengurangi kemungkinan menghadapi situs web yang terkait dengan penambangan mata uang kripto.
- Jika komputer berjalan sangat lambat, cari file yang mencurigakan yang berjalan dan silakan kirimkan sampel ke vendor sistem operasi. Anda dapat mengirimkan file untuk analisis malware ke Microsoft di <https://www.microsoft.com/wdsi/filesubmission>.

DETEKSI DAN RESPONS:

Deteksi dan respons berkontribusi pada ketahanan dengan membatasi waktu penyerang mengakses sumber daya Anda. Hal ini mengurangi penyerang ROI dengan cara meningkatkan kerugian penyerang (mereka harus mencoba lagi atau memodifikasi operasi mereka) serta mengurangi pengembalian (membatasi peluang untuk mencapai tujuan mereka).

Teknologi cloud yang sama yang memungkinkan organisasi bisnis untuk memenuhi kebutuhan pasar dengan lebih baik juga dapat membantu mengoptimalkan operasi keamanan dalam melawan penyerang.



◀ **GAMBAR 10.**

Lintasan evolusi SOC

Ketika kita melihat lintasan dari evolusi Pusat Operasi Keamanan (SOC), kita melihat perkembangan teknologi terus meningkatkan kecepatan dan kualitas keputusan dan tindakan SOC. Banyak dari inovasi ini dapat dipetakan ke masing-masing tahap dari siklus Amati Orientasi Putuskan Bertindak (OODA) yang didokumentasikan oleh Kolonel USAF John Boyd.³

AMATI – SOC dapat memanfaatkan inteligensi keamanan yang luas yang tersedia (dari Microsoft dan sumber lain) untuk meningkatkan bidang pandang secara dramatis dalam organisasi dan lingkungan eksternal.

ORIENTASI – Setelah sumber data baru ini tersedia ke SOCS yang kelebihan beban, mesin pembelajaran (serangkaian kecerdasan buatan) menjadi alat penting di balik dataset masif ini dan mengidentifikasi anomali yang layak diselidiki. Vendor keamanan (termasuk Microsoft) telah mengadopsi teknologi mesin pembelajaran untuk memprioritaskan kejadian dengan cepat (dan membantu menggabungkan kejadian individual ini ke dalam insiden holistik).

PUTUSKAN – Karena volume serangan dan kompleksitasnya dapat dengan cepat membebani SOC, analis dan responden insiden perlu mengambil banyak

keputusan dan bertindak cepat dalam menanggapi peringatan dan deteksi. Microsoft dan vendor lainnya telah mengintegrasikan kemampuan investigasi otomatis serta panduan untuk membantu analis dengan cepat mengambil keputusan yang baik (untuk mengisolasi perangkat yang berpotensi terinfeksi atau disusupi misalnya). Untuk saat ini, otomatisasi difokuskan pada menyelesaikan insiden prioritas rendah dengan cepat sehingga keahlian khusus dapat diterapkan untuk masalah yang lebih kompleks.

BERTINDAK – Respons membutuhkan eksekusi yang cepat dan akurat di banyak teknologi dan platform, yang mana dimungkinkan melalui teknologi orkestrasi dan otomatisasi respons keamanan. Microsoft dan banyak perusahaan lainnya terus berinvestasi dalam teknologi ini termasuk deteksi ancaman modern dan solusi respons otomatis.

CATATAN KAKI

³<http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/>

Beberapa tren lain yang berlaku untuk SOC modern adalah:

- **Umpan peringatan kualitas lebih dari kuantitas** – Setelah organisasi bergeser dari mengelola "informasi yang sangat sedikit" menjadi mengelola "terlalu banyak informasi", waktu dan perhatian analis spesialis SOC menjadi semakin berharga. Hal ini mendorong perlunya peningkatan kualitas yang memerlukan keterlibatan analis Tingkat 1 dan 2. Sementara umpan data tambahan dapat membantu penyelidikan dan pemburuan proaktif, SOC TI Korporat Microsoft mengukur tingkat positif aktual dari umpan peringatan yang memerlukan tanggapan analis (dan saat ini membutuhkan 90% tingkat positif benar atau lebih).
- **Gravitasi data** – Analitik terhadap dataset besar (termasuk data keamanan) sulit dilakukan tanpa akses ke data mentah yang mendasarinya. Karena tersedia lebih banyak data keamanan, melakukan analisis keamanan menjadi lebih ekonomis dan praktis di cloud daripada melakukan backhaul data ke sistem lokal. Ini kemungkinan akan menyebabkan evolusi arsitektur SIEM dan SOC yang dapat termasuk pendekatan SIEM hibrid atau adopsi SIEM cloud asli sebagai layanan.
- **Konteks tinggi** – Jenis pendeteksian ini jauh lebih berguna karena kemampuannya untuk mengkorelasikan dataset secara lebih efektif. Sementara deteksi berbasis lalu lintas jaringan tradisional masih memberikan sejumlah nilai keamanan, lalu lintas jaringan mentah biasanya tidak

memiliki konteks untuk membedakan antara aktivitas yang sah dan aktivitas anomali. Kami melihat SOC mendapatkan lebih banyak deteksi kaya di luar konteks nilai seperti:

- **Solusi Deteksi dan Respons Endpoint (EDR)** yang memiliki konteks mendalam tentang aktivitas host
- Pendeteksian berdasarkan identitas yang mencakup wawasan tentang pola autentikasi pengguna normal (lokasi, waktu, layanan yang diakses, dll.) dan menerapkan analitik perilaku

Deteksi kaya konteks ini lebih sulit dihindari oleh lawan karena mereka harus meniru operasi yang jauh lebih kompleks (dibandingkan beberapa atribut teknis lalu lintas IP).

Pelajaran lain yang telah kita petik dari pembobolan besar pada pelanggan adalah kesulitan dengan cepat menanggapi insiden ketika fungsi IT ternyata sebagian atau sepenuhnya dari outsourcing. Kami sarankan Anda meninjau kontrak outsourcing TI dan perjanjian tingkat layanan (SLA) serta vendor rantai pasokan untuk memastikan mereka kompatibel dengan respons keamanan yang cepat. Untuk pembelajaran lain dari penyelidikan insiden kami di pelanggan, lihat Panduan Referensi Respons Insiden (IRRG) di <https://aka.ms/IRRG>.

Sumber data



Sumber data

Microsoft telah mengumpulkan data yang disertakan dalam laporan inteligensi keamanan Microsoft dengan menyediakan berbagai macam produk dan layanan Microsoft, seperti yang disebutkan dalam [Pernyataan Privasi Microsoft](#). Data ini memberi kami informasi berharga tentang keamanan dan pengoperasian produk dan layanan kami, serta wawasan tentang lanskap ancaman keamanan siber secara umum. Data ini mencakup analitik dari sumber berikut:⁴

- [Azure Security Center](#) adalah layanan yang membantu organisasi mencegah, mendeteksi, dan merespons ancaman dengan memberikan visibilitas yang ditingkatkan ke dalam keamanan beban kerja cloud serta menggunakan analitik dan inteligensi ancaman tingkat lanjut untuk mendeteksi serangan.
- [Bing](#) adalah mesin pencarian dan keputusan dari Microsoft, berisi teknologi yang menjalankan miliaran pemindaian halaman web per tahun untuk mencari konten berbahaya. Setelah konten tersebut dideteksi, Bing menampilkan peringatan kepada pengguna tentang ancaman ini untuk membantu mencegah infeksi.
- [Exchange Online](#) adalah layanan email dan produktivitas yang dihosting Microsoft. Layanan antimalware dan antispam Exchange Online memindai miliaran pesan setiap tahun untuk mengidentifikasi dan memblokir spam serta malware.
- [Malicious Software Removal Tool](#) (MSRT) adalah alat gratis yang didesain Microsoft untuk membantu mengidentifikasi dan menghapus kelompok malware umum tertentu dari komputer pengguna. MSRT semula dirilis sebagai pembaruan penting melalui Windows Update, Microsoft Update, dan Automatic Updates. Versi alat ini juga tersedia dari Microsoft Download Center. MSRT bukanlah pengganti untuk solusi antivirus real-time mutakhir.
- [Microsoft Safety Scanner](#) adalah alat keamanan yang dapat diunduh secara gratis untuk memberikan pemindaian sesuai permintaan serta menyingkirkan malware dan perangkat lunak berbahaya lainnya. Microsoft Safety Scanner bukan pengganti untuk solusi antivirus terbaru, karena tidak menawarkan perlindungan real-time dan tidak dapat mencegah komputer terinfeksi.

CATATAN KAKI

⁴Yang terpenting, data ini selalu melewati pemeriksaan privasi dan kepatuhan yang ketat sebelum digunakan untuk keamanan.

- **Microsoft Security Essentials** adalah produk perlindungan real-time yang mudah diunduh dan tersedia gratis yang memberikan perlindungan antivirus dan antispyware yang efektif untuk Windows Vista dan Windows 7.
- **Microsoft System Center Endpoint Protection** (sebelumnya Forefront Client Security dan Forefront Endpoint Protection) adalah produk terpadu yang memberikan perlindungan dari malware dan perangkat lunak yang tidak diinginkan untuk desktop, laptop, dan sistem operasi server perusahaan. Produk ini menggunakan Microsoft Malware Protection Engine dan database khas antivirus Microsoft untuk memberikan perlindungan real-time, terjadwal, dan sesuai permintaan.
- **Office 365** adalah layanan Microsoft Office berlangganan untuk organisasi dan pengguna rumahan. Paket berlangganan tertentu mencakup akses ke Office 365 Advanced Threat Protection.
- **Windows Security** di Windows 10 menyediakan pemindaian real-time dan penghapusan malware dan software yang tidak diinginkan. Selain itu, versi terbaru Windows memanfaatkan data kontekstual yang kaya seperti konfigurasi mesin, inerja dan kesehatan perangkat, dan informasi lainnya untuk meningkatkan keamanan bagi pelanggan. Pada saat yang sama, kami memberdayakan pelanggan agar lebih mengetahui tentang privasi mereka di Windows 10. Baca [blog ini](#) untuk mempelajari tentang beberapa cara Microsoft melakukannya.
- **Windows Defender Advanced Threat Protection** adalah layanan baru yang disertakan ke dalam Windows 10 Anniversary Update dan versi lebih baru yang memungkinkan pelanggan perusahaan mendeteksi, menyelidiki, dan mengatasi ancaman persisten dan pelanggaran data tingkat lanjut di jaringan mereka.
- **Windows Defender Offline** adalah alat yang dapat diunduh yang dapat digunakan untuk membuat CD, DVD, atau flash drive USB yang dapat di-boot untuk memindai malware dan ancaman lainnya pada komputer. Alat ini tidak menawarkan perlindungan real-time dan bukan pengganti solusi antimalware terbaru.
- **Windows Defender SmartScreen**, fitur di Microsoft Edge dan Internet Explorer, menawarkan perlindungan pengguna terhadap situs phishing dan situs yang menghosting malware. Microsoft mengelola database situs phishing dan malware yang dilaporkan oleh pengguna Microsoft Edge, Internet Explorer, serta produk dan layanan Microsoft lainnya. Ketika pengguna berupaya untuk mengunjungi situs di database dengan filter yang diaktifkan, browser menampilkan peringatan dan memblokir navigasi ke halaman tersebut.