PUSAT OPERASI KEAMANAN SIBER NASIONAL
NATIONAL CSIRT OF INDONESIA
id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

MEWASPADAI SERANGAN RANSOMWARE

TLP: WHITE

MEWASPADAI SERANGAN RANSOMWARE

Pedoman pencegahan ini dipublikasikan oleh **Pusopskamsinas BSSN** sebagai upaya untuk mewaspadai serangan ransomware di Indonesia. Panduan ini terbagi dalam beberapa bagian yaitu: Pendahuluan, Jenis-Jenis Ransomware, Kasus Ransomware, Indicator of Compromise (IoC) dari Ransomware, Mitigasi Jika Terkena Ransomware, dan Pencegahan Infeksi Ransomware.

DAFTAR ISI

PENDAHULUAN //

Serangan siber terkadang dianggap tidak terlalu penting atau disepelekan hingga benar-benar memberi dampak secara nyata, terutama kerugian finansial. Serangan siber tidak hanya menyebabkan kerusakan sistem, kehilangan data, atau pencurian data, tetapi juga kerugian finansial secara langsung. Ransomware adalah salah satu bentuk serangan siber yang akan mengunci akses dari pemilik aset (sistem ataupun data), kemudian menawarkan sejumlah biaya untuk menebus akses tersebut kepada pemilik aset.

Hal ini tentu menjadi risiko besar, terutama ketika sistem atau data yang dikunci merupakan data strategis dan sangat berperan penting bagi keberlangsungan proses bisnis sebuah perusahaan atau organisasi. Nilai yang diminta oleh pelaku kejahatan pun biasanya tidak sedikit (jutaan dolar AS) dan menjadi kerugian besar bagi organisasi. Untuk itu, setiap orang, terutama perusahaan atau organisasi, perlu memahami mengenai bahaya ransomware, apa yang harus diperhatikan agar terhindar dari ransomware, hingga langkah-langkah utama yang harus dilakukan ketika terkena serangan ransomware.

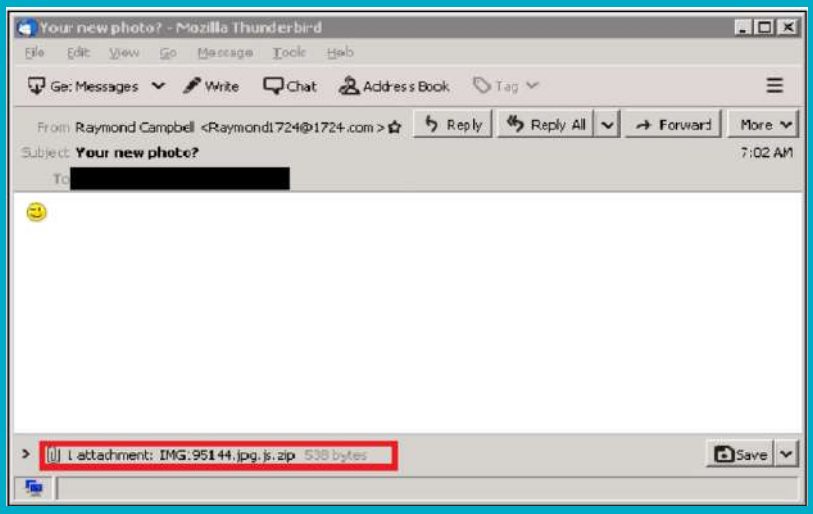
JENIS RANSOMWARE //

Berdasarkan hasil penelusuran Tim Pusopskamsinas BSSN, serangan Ransomware terus menjadi tren sepanjang tahun 2021. Berikut merupakan jenis-jenis ransomware tersebut:

Avaddon Ransomware

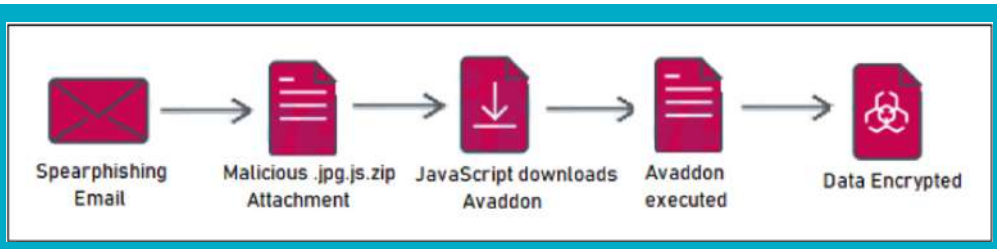
Avaddon pertama kali terdeteksi pada Februari 2020, ransomware ini dipasarkan sebagai Avaddon pertama kali terdeteksi pada February 2020, ransomware ini dipasarkan sebagai Ransomware-as-a-Service (RaaS) oleh pelaku kejahatan. Ransomware ini muncul sebagai cryptolocker yang ditulis dalam bahasa pemrograman C++ dan melakukan enkripsi file korban dengan menggunakan algoritma standar AES256 dan RSA2048. Distribusi Avaddon adalah melalui spam email.

Email tersebut berisi lampiran berbahaya, dengan subjek email yang menggoda korbannya untuk membuka email tersebut. Biasanya subjek berupa pertanyaan "*Do you like my photo?*" atau "*Your new photo?*", sehingga membuat korban penasaran dengan lampiran yang ada pada email tersebut. Isi dari email tersebut hanya berupa emoticon smiley dengan lampiran berupa gambar .jpg berformat .zip IMG<6randomdigit>.jpg.js.zip. Lampiran email tersebut merupakan file JavaScript berbahaya dalam bentuk gambar untuk menghindari deteksi firewall.



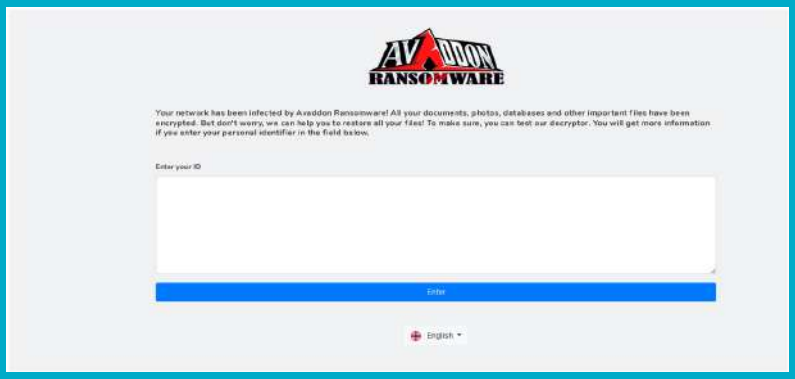
Gambar 1. Isi email berbahaya dari grup Ransomware Avaddon

Berdasarkan beberapa kasus sebelumnya, terdapat pola pada alamat email dari si pengirim, yaitu: <nama>[0-9]{2}@[0-9]{4}.com. Ketika korban membuka lampiran berbahaya tersebut, JavaScript akan menjalankan PowerShell dengan flag policy bypass sehingga script berjalan tanpa ada peringatan tanda bahaya. Command PowerShell kemudian akan mengunduh file executable (jpr.exe atau sava.exe) dari alamat IP "217.8.117.63" yang kemudian disimpan pada folder temp dan disimpan sebagai "<digit acak>.exe" sebelum dieksekusi. Gambar 2 merupakan kill chain proses dari Avaddon. Gambar 3 merupakan template command PowerShell Avaddon.

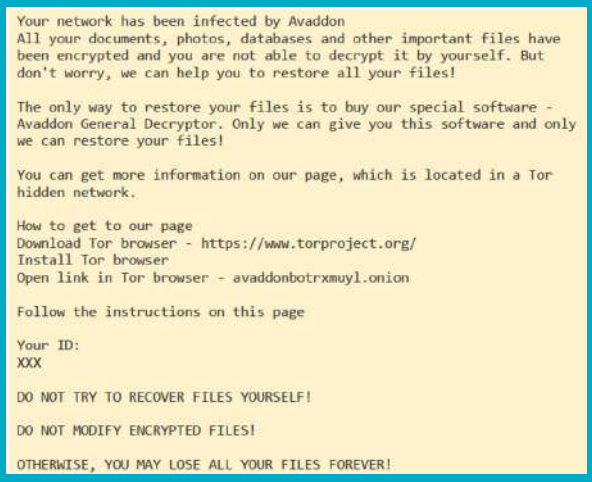


Gambar 2. Kill chain proses dari Ransomware Avaddon

Setelah berhasil terinfeksi, grup Ransomware "Avaddon" memposting beberapa dokumen milik korban pada situs onion http[:]//avaddongun7rngel[.]onion. Pada situs onion tersebut, terdapat beberapa judul post yang terdapat timer yang merujuk pada pembaharuan selanjutnya pada database tersebut. Korban akan diberikan ID sebagai tanda pengenal untuk membayar sejumlah tebusan dengan besaran tertentu dan diberikan tenggat waktu bagi korban untuk membayar tebusan tersebut. Apabila korban tidak membayar uang tebusan dalam jangka waktu yang sudah disebutkan, maka seluruh dokumen milik korban akan diunggah pada situs onion yang berelasi dengan grup Ransomware "Avaddon". Gambar 3 merupakan situs pembayaran tebusan grup Ransomware Avaddon.



Gambar 3. Tampilan situs pembayaran tebusan grup Ransomware Avaddon



```
Your network has been infected by Avaddon
All your documents, photos, databases and other important files have
been encrypted and you are not able to decrypt it by yourself. But
don't worry, we can help you to restore all your files!

The only way to restore your files is to buy our special software -
Avaddon General Decryptor. Only we can give you this software and only
we can restore your files!

You can get more information on our page, which is located in a Tor
hidden network.

How to get to our page
Download Tor browser - https://www.torproject.org/
Install Tor browser
Open link in Tor browser - avaddonbotrxmuyl.onion

Follow the instructions on this page

Your ID:
XXX

DO NOT TRY TO RECOVER FILES YOURSELF!

DO NOT MODIFY ENCRYPTED FILES!

OTHERWISE, YOU MAY LOSE ALL YOUR FILES FOREVER!
```

Gambar 4. Ransom notes Avaddon Ransomware

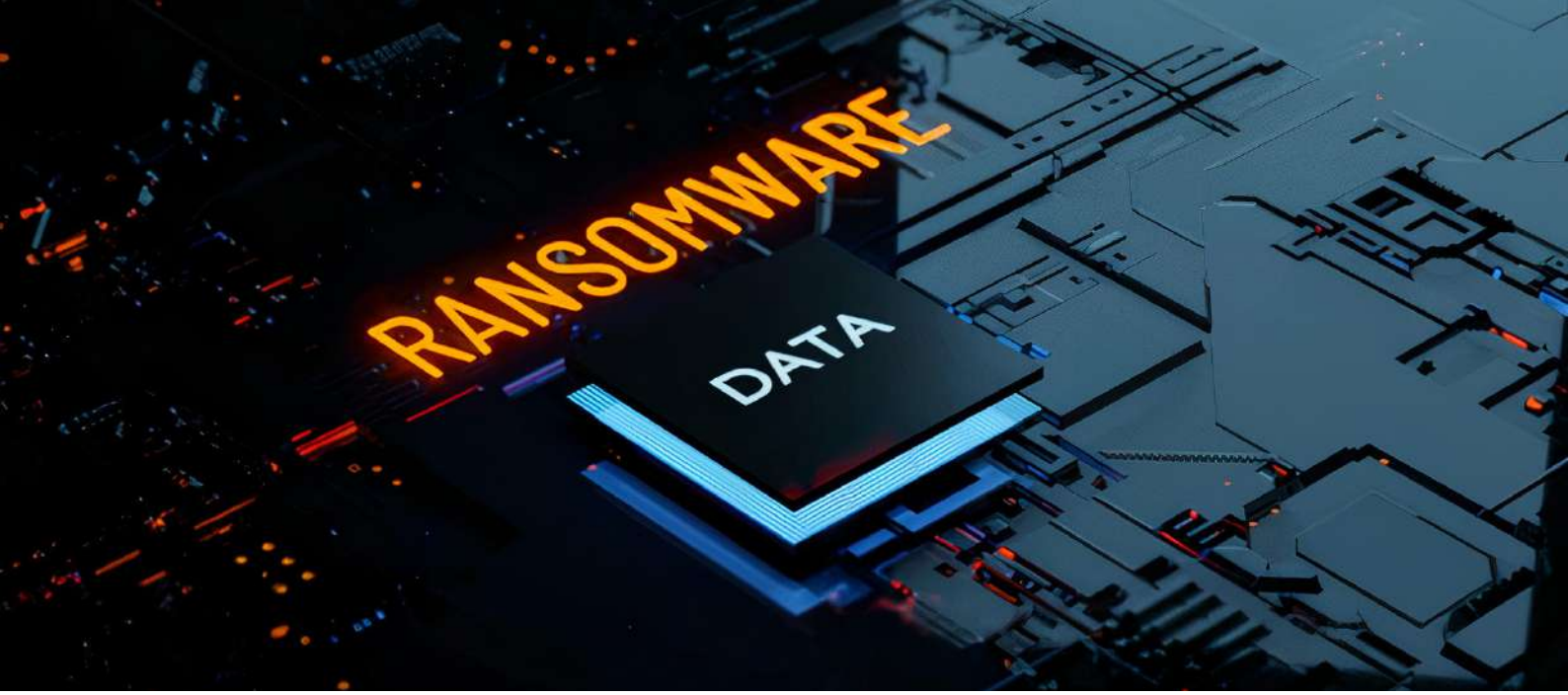
Selain itu, pelaku kejahatan yang mengoperasikan ransomware Avaddon secara aktif merekrut afiliasi untuk meningkatkan jangkauan malware menggunakan sistem pendapatan afiliasi. Pelaku kejahatan yang mendaftar sebagai afiliasi bertanggung jawab untuk mengirimkan malware dengan cara apa pun yang memungkinkan. Ransomware dapat digunakan dan didistribusikan oleh pelaku kejahatan tanpa biaya awal, tetapi 35% bagian dari pembayaran tebusan yang diperoleh masuk ke operator Avaddon sebagai bagian dari pengaturan ini. Pelaku kejahatan yang bertanggung jawab atas pendistribusian dapat menyimpan sisa 65% bagian dari pembayaran tebusan yang diterima. Gambar 4 merupakan salah satu contoh ransom notes dari Ransomware Avaddon.

Berikut merupakan timeline Avaddon Ransomware:

- February 2020 pertama kali terdeteksi
- Juni 2020 diperkirakan awal mula dijual ke criminal untuk digunakan sebagai RaaS (Ransomware as a Service).
- Agustus 2020 dilaporkan bahwa operator Avaddon mengumumkan situs data leak mereka pada forum hacker berbahasa Rusia
- Februari 2021 seorang peneliti (Javier Yuste) merilis decryptor tools secara gratis
- Mei 2021, operator Avaddon mengeluarkan versi kedua dari Avaddon dengan klaim bahwa decryptor tools yang dikeluarkan sebelumnya tidak berfungsi pada versi kedua Avaddon.

Tactic, Technique, dan Procedure yang digunakan Avaddon Ransomware:

TAKTIK	NAMA	DESKRIPSI
Initial access (T1193)	Spearphising Attachment	Avaddon dikirimkan melalui email phising yang mengandung JavaScript berbahaya disamarkan sebagai file gambar
Execution (T1035)	Service Execution	Avaddon membuat layanan Windows (wmic, wbadmin, vssadmin, bccdedit) menggunakan "OpenSCManager" selama proses eksekusi
Execution (T1047)	Windows Management Instrumentation	Avaddon menggunakan wmic untuk menghapus salinan
Persistence (T1215)	Kernel Modules and Extensions	Avaddon menyebarkan wmic, wbadmin dan vssadmin yang mengakses Kernel Security Device Driver, KsecDD
Persistence (T1060)	Registry Run Keys / Startup Folder	Avaddon menambahkan kunci Registry Run (%APPDATA%\ Filename) agar tercipta ketahanan
Persistence (T1179)	Hooking	Avaddon mennghubungkan beberapa fungsi API untuk menjalankan proses baru pada system
Privilege Escalation (T1055)	Process Injection	Avaddon mengambil dan memindahkan ke proses wbadmin, bcdedit dan vssadmin untuk menghapus cadangan system dan beberapa salinan lain
Defense Evasion (T1107)	File Detection	Avadon menghapus salinan lain, cadangan system, dan volume snapshot untuk mencegah proses pemulihan terjadi
Defense Evasion (T1112)	Modify Registry	Avaddon menggunakan modifikasi Registry (modifikasi sertifikat system, proxy dan pengaturan browser) sebagai bagian dari proses instalasi
Discovery (T1083)	File and Directory Discovery	Avaddon mencari file user berdasarkan ekstensi file sebelum dilakukan proses enkripsi
Discovery (T1012)	Query Registry	Avaddon melakukan query pada registry untuk mendapatkan MachineGUID, pengaturan browser serta pengaturan bahasa pada perangkat Windows
Discovery (T1497)	Virtualization / Sandbox Evasion	Avaddon menerapkan teknik anti-debug untuk menghindari deteksi
Discovery (T1016)	System Network Configuration Discovery	Avaddon mencoba menentukan segmen jaringan local yang merupakan bagiannya
Discovery (T1120)	Peripheral Device Discovery	Avaddon berisi utas yang akan meminta informasi volume guna proses enkripsi perangkat terinfeksi
Command and control (T1043)	Commonly Used Port	Avaddon menggunakan HTTP pada port 443 untuk proses komunikasi
Impact (T1486)	Data Encrypted for Impact	Avaddon mengenkripsi file pada perangkay dan meminta tebusan dalam Bitcoin agar file tersebut didekripsi
Impact (T1490)	Inhibit System Recovery	Avaddon menggunakan wmic,bcdedit, vssadmin dan wbadmin untuk menghapus dan menonaktifkan fitur pemulihan dari system operasi



DarkSide Ransomware

Darkside adalah ransomware yang dibuat menggunakan bahasa pemrograman C dan dapat dikonfigurasikan untuk melakukan enkripsi file pada fixed dan removable disks, serta network shares. Darkside Ransomware dikenal sebagai "Robin Hood". Hal tersebut dikarenakan hasil dari pemerasan dari aksi ransomwarenya diberikan untuk dana amal/kemanusiaan. Ransomware Darkside merupakan human operated ransomeware dan beroperasi sebagai ransomware-as-a-service (RaaS) yang membagi keuntungan antara pemilik dan afiliasinya yang menyediakan akses ke dalam organisasi dan menyebarkan ransomware.

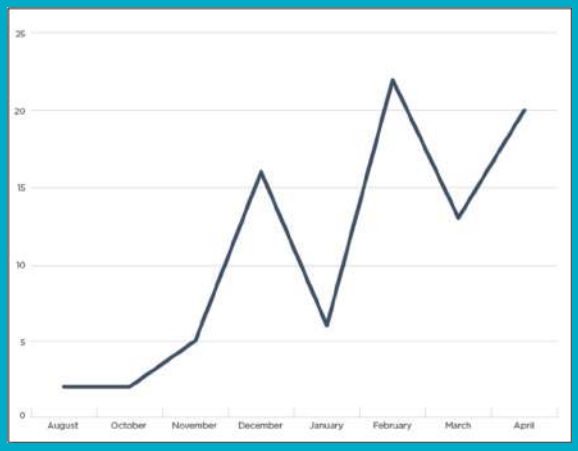
Ringkasan profile Darkside Ransomware:

NAMA	DarkSide
Jenis Ancaman	Ransomware, Virus Kripto, Enkripsi File.
Ekstensi File Terenkripsi	ID Korban
Tebusan	Melalui file README. [Korban_ID] .TXT, dan situs web Tor.
Kotak Kriminal Cyber	Situs web Tor
Antivirus yang mendeteksi	Avast (Win32: Malware-gen), BitDefender (Gen: Trojan.Heur.RP.bmGfbKkIF@n), Emsisoft (Gen: Trojan.Heur.RP.bmGfbKkIF@n (B)), Kaspersky (Trojan-Ransom.Win32. Gen.xyl), Daftar Lengkap Deteksi (VirusTotal)
Target	Ransomware ini menargetkan perusahaan dan organisasi besar.
Motode Distribusi	Lampiran email yang terinfeksi (makro), situs web torrent, iklan berbahaya.
Kerusakan	Semua file dienkripsi dan tidak dapat dibuka tanpa membayar uang tebusan. Trojan pencuri passwore tambahan dan infeksi malware dapat dipasang bersamaan dengan infeksi ransomware.

Target Ransomware Darkside

Ransomware ini pertama kali muncul pada bulan Agustus 2020 dan menargetkan perusahaan-perusahaan besar. Sebagian besar target adalah berbasis di Amerika Serikat dan tersebar diberbagai sektor, termasuk layanan keuangan, hukum, manufaktur, layanan professional, ritel, dan teknologi. Grup ransomware ini mengklaim bahwa hanya menargetkan perusahaan besar yang dapat membayar tebusan. Grup ransomware ini melakukan penyanderaan terhadap data pada system computer dan juga telah melakukan pencurian data hingga 100 GB data perusahaan. Data tersebut termasuk informasi sensitive seperti data klien, data keuangan, paspor karyawan, dan kontrak.

Berikut merupakan grafik korban Darkside Ransomware dari bulan Agustus 2020 sampai dengan April 2021 berdasarkan laporan dari Fire Eye.



Gambar 5. Korban DarkSide Ransomware yang diketahui (Agustus 2020-April 2021)

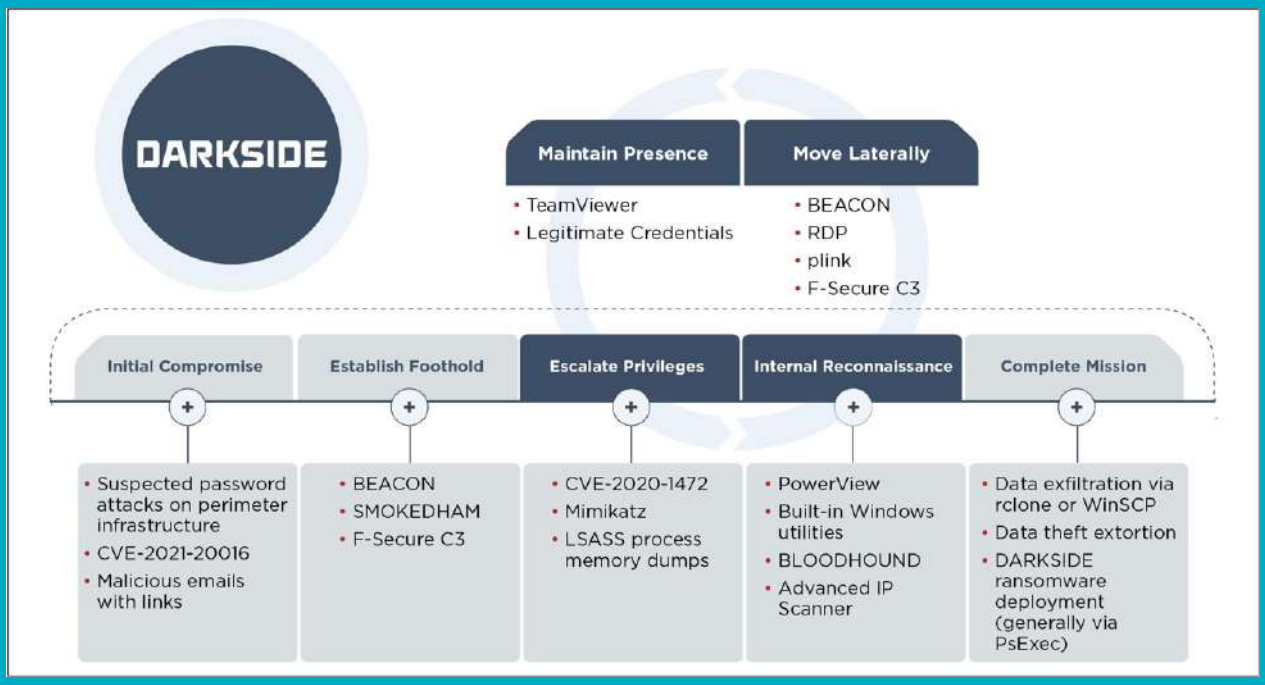
Berdasarkan situs yang bocor, setidaknya telah ada 90 korban yang terdampak DarkSide. Darkside menentukan jumlah tebusan yang diminta menyesuaikan dengan catatan keuangan organisasi yang menjadi target. Darkside Ransomware menyatakan bahwa mereka menghindari menargetkan perusahaan di industry tertentu, seperti sektor Kesehatan, Pendidikan, sektor public, dan sektor nirlaba.

Aktivitas Darkside Ransomware pada Agustus 2020 hingga Mei 2021

TAHUN	BULAN	AKTIVITAS
2020	Agustus	Pertama kali memperkenalkan ransomwarenya
	Oktober	Menyumbangkan USD 20.000 yang dicuri dari korbannya untuk kegiatan amal
	November	Mengubah bisnis modelnya menjadi Ransomware as a Services (RaaS). Grup ini menawarkan layanannya untuk digunakan oleh kelompok kriminal lainnya.
		Situs darkside ditemukan untuk mempublikasikan data korban yang dicurinya.
		Darkside meluncurkan Content Delivery Network (CDN) untuk menyimpan dan mengirimkan data yang dicuri
	Desember	Seorang actor darkside mengundang media dan organisasi pemulihan data untuk mengikuti Pusat Pers melalui situs darkside.

TAHUN	BULAN	AKTIVITAS
2021	Maret	Darkside versi 2 dirilis dengan beberapa penambahan fitur.
	Mei	Serangan Colonial Pipeline
		Serangan Toshiba Tec Corp

Berikut merupakan gambaran siklus serangan Darkside Ransomware:



Gambar 6. Siklus serangan Darkside Ransomware

Mapping MITRE ATT&CK dari TTP yang berkaitan dengan Darkside Ransomware:

TACTIC	TECHNIQUE
Reconnaissance	T1590 (Gather Victim Network Information)
Initial Access	T1078 (Valid Accounts)
	T1566 (Phishing)
	T1190 (Exploit Public-Facing Application)
Execution	T1059.004(Command and Scripting Interpreter: Unix Shell)
	T1059.001(Command and Scripting Interpreter: PowerShell)

TACTIC	TECHNIQUE
Persistence	T1569(System Services)
	T1078 (Valid Accounts)
	T1053 (Scheduled Task/Job)
	T1098 (Account Manipulation)
Privilege Escalation	T1548.002 (Abuse Elevation Control Mechanism: Bypass User Account Control)
	T1036 (Masquerading)
	T1140 (Deobfuscate / Decode Files or Information)
Defense Evasion	T1222.002 (File and Directory Permissions Modification: Linux and Mac File and Directory Permission Modification)
	T1214 (Credentials in Registry)
	T1083 (File and Directory Discovery)
	T1055 (Process Injection: Dynamic-link Library Injection)
	T1500 (Compile After Delivery)
	T1562.001 (Impair Defenses: Disable or Modify Tools)
Credential Access	T1555 (Credentials from Password Stores)
	T1082 (System Information Discovery)
	T1071 (Standard Application Layer Protocol)
	T1057 (Process Discovery)
	T1555.003 (Credentials from Password Stores: Credentials from Web Browsers)
Discovery	T1087 (Account Discovery)
	T1105 (Remote File Copy)
	T1490 (Inhibit System Recovery)
	T1105 (Ingress Tool Transfer)
	T1087.002 (Account Discovery: Domain Account)
	T1482 (Domain Trust Discovery)
	T1069.002 (Permission Groups Discovery: Domain Groups)
	T1018 (Remote System Discovery)
	T1016 (System Network Configurartion Discovery)

TACTIC	TECHNIQUE
Lateral Movement	T1080 (Taint Shared Content)
	T1486 (Data Encrypted for Impact)
Collection	T1113 (Screen Capture)
Command and Control	T1043 (Commonly Used Port)
Exfiltration	T1567.002 (Exfiltration Over Web Service: Exfiltration to Cloud Storage)
	T1048 (Exfiltration Over Alternative Protocol)
Impact	T1489 (Service Stop)

Egregor Ransomware

Ransomware Egregor adalah ransomware yang relatif baru (pertama kali terlihat pada September 2020). Egregor dianggap sebagai varian dari Ransom.Sekhmet berdasarkan kesamaannya dalam obfuscation, API, dan ransom note. Berdasarkan laporan Malwarebytes, grup ransomware bernama Maze merupakan grup yang merupakan pihak-pihak yang terkait dengan ransomware Egregor. Egregor telah menargetkan beberapa korban terkenal seperti Barnes & Noble, Kmart dan Ubisoft.

Metode Penyebaran

Metode distribusi utama untuk Egregor adalah Cobalt Strike. Lingkungan yang ditargetkan pada awalnya disusupi melalui berbagai cara (pemeriksaan RDP, phishing) dan setelah muatan Cobalt Strike sudah masuk dalam sistem target, kemudian digunakan untuk mengirim dan menjalankan muatan Egregor.

Egregor juga merupakan jenis ransomware-as-a-service (RaaS) dengan banyak afiliasi, taktik pengiriman dan serangan dapat bervariasi. Beberapa kali juga disebarkan melalui email phishing. Serangan tersebut biasanya terjadi dalam dua tahap: pengiriman surel yang berisi Qakbot, diikuti oleh ransomware Egregor yang sebenarnya. Tahap terakhir ini digunakan secara manual oleh penyerang yang sebelumnya mendapatkan akses sebagai hasil dari serangan tahap awal.

Pemetaan MITRE ATT&CK

TACTIC	TECHNIQUE
Initial Access	Phishing
Privilege Escalation	Valid Accounts
Defense Evasion	Group Policy Modification
	Impair Defenses
	Impair Defenses: Disable or Modify Tools
	Masquerading
Command and Control	Ingress Tool Transfer
Discovery	Account Discovery
	Domain Trust Discovery
	Permission Groups Discovery
	Permission Groups Discovery: Local Groups
Lateral Movement	Remote Services
Exfiltration	Exfiltration Over Web Service
Impact	Data Encrypted for Impact

Ransomware Egregor terakhir kali melakukan aksinya pada situs Indonesia yaitu situs MNC Group. Informasi ini berhasil didokumentasikan pada akun Twitter @darktracer_int. Postingan tersebut menyebutkan bahwa terdapat 6 (enam) organisasi Indonesia yang mengalami kebocoran data di dark web yang disebabkan oleh beberapa grup ransomware dan salah satunya diantaranya adalah MNC Group yang diinfeksi oleh ransomware Egregor.

Pysa Ransomware

Pysa Ransomware atau dikenal dengan Mespinoza Ransomware merupakan jenis malware yang dapat mengenkripsi berbagai data/file penting yang tersimpan didalam memory penyempanan suatu sistem. Untuk dapat membuka kunci enkripsi yang dilakukan oleh Pysa Ransomware, Korban diminta untuk membayar sejumlah tebusan. Berikut merupakan beberapa informasi umum terkait dengan pysa ransomware:

Nama	Pysa/Mespinoza Ransomware
Malware Family	Vurten malware family
Motivasi	Mencuri informasi, keuntungan finansial

Deskripsi Singkat	Ransomware Mespinoza termasuk malware family Ransomware Vurten, yang pertama kali dirilis pada April 2018, dengan meminta tebusan sebanyak $10.000 untuk mendapatkan perangkat lunak dekripsinya. Pysa Secara umum dapat melakukan akses ke korban dengan cara compromise kredensial Remote Desktop Protocol (RDP) melalui phishing email.
Type	File locking virus, cryptomalware
Kapabilitas	Eksfiltrasi data, mengenkripsi file penting yang tersimpan pada sistem pengguna
Indikasi	Enkripsi file oleh ransomware dilakukan dengan menggunakan algoritma enkripsi AES dan RSA. Setelah enkripsi selesai, ransomware menambahkan ekstensi pysa khususnya ke semua file yang dimodifikasi olehnya.
Metode Distribusi	Brute-force attacks, Spam atau phishing Emails, Email Attachments, Koneksi RDP.
Metode Enkripsi	Malware ini menggunkan algoritma enkripsi AES untuk mengunci gambar, dokumen, database, video, dan berbagai jenis file penting lain.
Ekstensi	Ekstensi enkripsi malware ini tergantung pada versi virus yang mengenkripsi, diantaranya yaitu .locked ; .pysa ; dan .newversion
Ransom note	Readme.README dimasukkan ke dalam berbagai folder di sistem, serta desktop
Termination	Untuk menghilangkan infeksi virus Ini, pengguna dapat memindai komputernya dengan perangkat lunak anti-malware. Jika virus menghentikan alat keamanan, mengakses dengan Safe Mode dengan Jaringan akan melewati fungsi ini.
Sektor Target (terobservasi)	Sektor Kesehatan, Keuangan, Teknologi Informasi, Industri non-profit, Sektor Publik, Layanan Makanan, 12 Institusi Pendidikan di Amerika Setikat dan Inggris
Target Sistem Operasi	Microsoft Windows

Pemetaan Mitre ATT&CK mengenai Tactic, Technique, dan Procedure yang digunakan oleh Pysa Ransomware.

TACTICS	TECHNIQUE	KETERANGAN
Initial Access	Phishing (T1566)	Penyerang mengirimkan email phishing ataupun email attachment
Credential Access	Brute Force (T1110)	Penyerang melakukan brute force attack untuk mendapatkan kredensial akses. Percobaan serangan ini menyerang central management console serta beberapa akun Active Directory. Selain itu, beberapa account domain administrator juga telah disusupi.
	Unsecured Credentials: Credentials In Files (T1552.001)	Penyerang dapat mencari lokasi local file system dan kemudian melakukan exfiltrasi database password.
	OS Credential Dumping (T1003)	Penyerang melakukan credential dumping dengen menggunakan Mimikatz.
Execution	Command and Scripting Interpreter: PowerShell (T1059.001)	Setelah mendapatkan akses, Penyerang melakukan lateral movement ke domain controller dan kemudian menjalankan perintah PowerShell.
	System Services: Service Execution (T1569.002)	Sekumpulan intrusion set menggunakan skrip «.bat» untuk menyalin dan menjalankan ransomware dengan menggunakan Remote Administration Tools PsExec.
Persistence	Boot or Logon Autostart Execution: Kernel Modules and Extensions (T1547.006)	Tahap ini dilakukan dengan menggunakan Koadic untuk menjadwalkan eksekusi file HTA yang terletak pada direktori C: \ ProgramData saat login sebagai sistem. Hal inilah yang akan menginisiasi komunikasi ke C2 Koadic server.
	Account Manipulation (T1098)	Mengubah local account password
Defense Evasion	Impair Defenses: Disable or Modify Tools (T1562.001)	Penyerang menghentikan layanan anti-virus, serta uninstalling Windows Defender.
Discovery	System Network Configuration Discovery (T1016)	Ditemukan network reconnaissance tools Advanced Port Scanner dan Advanced IP Scanner pada sistem informasi korban. Hal ini berarti penyerang mencari konfigurasi network dan system setting untuk melakukan remote access.
	Query Registry (T1012)	Penyerang mengakses Windows Registry untuk mengumpulkan informasi sistem, konfigurasi, dan software terinstall.

TACTICS	TECHNIQUE	KETERANGAN
Lateral Movement	Remote Services (T1021)	Beberapa alat yang ditumakan pada sistem informasi memungkinkan penyerang untuk maintain beberapa mesin atau mengekstrak data seperti Putty dan WinSCP
	Remote Services: Remote Desktop Protocol (T1021.001)	Penyerang masuk menggunakan Valid account ke dalam computer korban dengan menggunakan Remote Desktop Protocol (RDP).
Command and Control		Penyerang menggunakan 3 channel C2 yang berbeda, yaitu RDP, PowerShell Empire, dan Koadic
Collection	Email Collection (T1114)	Penyerang menargetkan email pengguna untuk mengumpulkan informasi penting.
Exfiltration		Tidak ditemukan file teks yang dieksfiltrasi, kemungkinan eksfiltrasi dilakukan melalui salah satu saluran Command and Control melalui RDP, Empire, atau Koadic.
Impact	Inhibit System Recovery (T1490)	Penyerang menghapus restore points dan shadow copies. Modifikasi file README yang mengijinkan agar dapat dibuka dengan double click. Mengirimkan secara broadcast MAC Address perangkat melalui protocol UDP dan mengirimkannya melalui port 7.
	Data Encrypted for Impact (T1486)	Penyerang mengenkripsi data pada sistem target

RansomEXX Ransomware

RansomEXX merupakan salah satu ransomware dengan indikasi bahwa sample malware secara hardcoded nama organisasi sebagai korban. RansomEXX ditemukan mulai aktif pada pertengahan 2020. Para korban yang pernah terinfeksi RansomEXX diperingatkan bahwa data-data korban akan dipublikasikan di situs tertentu, kecuali korban membayar tebusan yang diberikan. Untuk pembayaran tebusan korban akan diarahkan ke situs darkweb tertentu.

Nama	RansomEXX
Tipe Ancaman	Ransomware, Crypto Virus, Files locker.
Ekstensi File Terenkripsi	.***777, .[nama perusahaan]777 or karakter acak yang memuat informasi korban.
Pesan Menuntut Tebusan	!!!_Read_Me_How_To_DeCrypt_Files_!!!.txt; FILES.txt,HELP.txt, situs web Tor.

Jumlah Tebusan	$5000
Kontak Kriminal	Situs web Tor
Informasi Tambahan	Digunakan untuk menargetkan perusahaan dan organisasi besar
Metode Enkripsi	AES-256 and RSA-4096
Kerusakan	Semua file dienkripsi dan tidak dapat didekripsi sebelum melakukan pembayaran uang tebusan.
Beberapa Contoh Nama Lain Deteksi Ransomware	Ad-Aware - Trojan.GenericKD.45945353 AhnLab-V3 - Ransomware/Linux.Agent Avast - ELF:Encoder-K [Trj] AVG - ELF:Encoder-K [Trj] Avira - LINUX/Agent.gysyp BitDefender - Trojan.GenericKD.45945353 Comodo - Malware@#428f1zschrmw Cynet - Malicious (score: 85) Cyren - E64/Trojan.CLTZ-5 DrWeb - Linux.Encoder.75 Emsisoft - Trojan.GenericKD.45945353 (B) eScan - Trojan.GenericKD.45945353 ESET-NOD32 - A Variant Of Linux/Filecoder.RansomEXX.A FireEye - Trojan.GenericKD.45945353 Fortinet - Linux/Filecoder_RansomEXX.A!tr GData - Trojan.GenericKD.45945353 Ikarus - Trojan-Ransom.Ransomexx Jiangmin - Trojan.Linux.aye Kaspersky - HEUR:Trojan-Ransom.Linux.Ransomexx.c MAX - Malware (ai Score=99) McAfee-GW-Edition - Lnx/Encoder-GZJ!F7C4CB42780B Microsoft - Trojan:Win32/Ymacco.AA19 NANO-Antivirus - Trojan.Elf64.Ransom.ioxjer Qihoo-360 - Linux/Ransom.Encoder.HjsASQYA Rising - Ransom.RansomEXX/Linux!1.CE94 (CLASSIC) Sophos - Linux/Ransm-I Symantec - Trojan.Gen.NPE TrendMicro - Ransom.Linux.DEFRAY.A TrendMicro-HouseCall - Ransom.Linux.DEFRAY.A ZoneAlarm - HEUR:Trojan-Ransom.Linux.Ransomexx.c

Cringe Ransomware

Cringe ransomware terdeteksi melakukan exploitasi terhadap kerentanan server VPN FortiGate. Ransomware ini pernah terdeteksi menyerang berbagai perusahaan industry di negara-negara eropa. Serangan ini mengakibatkan penghentian sementara proses industri karena server digunakan untuk mengontrol proses industri terenkripsi.

Berikut merupakan gambaran umum terkait dengan Cringe Ransomware:

NAMA	Cringe Ransomware (Crypt3r, Vjiszy1lo, Ghost, Phantom)
Motivasi	▪ Threat actor memanfaatkan Cring Ransomware untuk mengeksploitasi celah kerentanan pada VPN Fortinet yaitu CVE-2018-13379. CVE-2018-13379 merupakan kerentanan traversal pada portal web FortiOS SSL VPN yang dapat eksploitasi oleh Threat actor yang tidak terautentikasi untuk mengunduh file sistem FortiOS secara khusus melalui crafted HTTP resource requests. ▪ Ransomware ini mengenkripsi data dari sistem korban menggunakan AES-256 + RSA-8192 serta meminta tebusan sebesar 2 BTC ▪ Penyerang mengunduh utilitas Mimikatz untuk mencuri kredensial pengguna dengan Sistem Operasi Windows.
Teknik yang digunakan	▪ Memanfaatkan kerentanan CVE-2018-13379 pada Fortigate SSL-VPN v.6.0.2 ▪ Mencuri kredensial menggunakan Mimikatz ▪ Memanfaatkan Cobalt Strike + PowerShell
Target	Organisasi-organisasi yang bergerak pada sector industri
Victim (terobservasi)	Perushaan sektor industry di beberapa negara Eropa. Serangan Ransomware melumpuhkan proses bisnis industry karena server down. Hal ini terjadi disebabkan server terenkripsi oleh Ransomware tersebut.

Tahapan infeksi yang dilakukan oleh Cringe Ransomware sebagai berikut:

1. Initial Vector Attack

Penyerang eksploitasi kerentanan CVE-2018-13379 pada server VPN FortiGate untuk mendapatkan akses ke jaringan. Kerentanan ini dimanfaatlan untuk mengekstrak file session pada VPN Gateway. Penyerang yang tidak terotentikasi ini terhubung ke internet mengakses file "sslvpn_websession" remote Session ini berisi informasi yang penting misalnya username dan password dan username dalam bentuk plaintext. Kerentanan ini dapat menginfeksi perangkat yang menggunakan FortiOS versi 6.0.0 sampai dengan 6.0.4, 5.6.3 sampai dengan 5.6.7, and 5.4.6 sampai dengan 5.4.12.

2. Lateral Movement

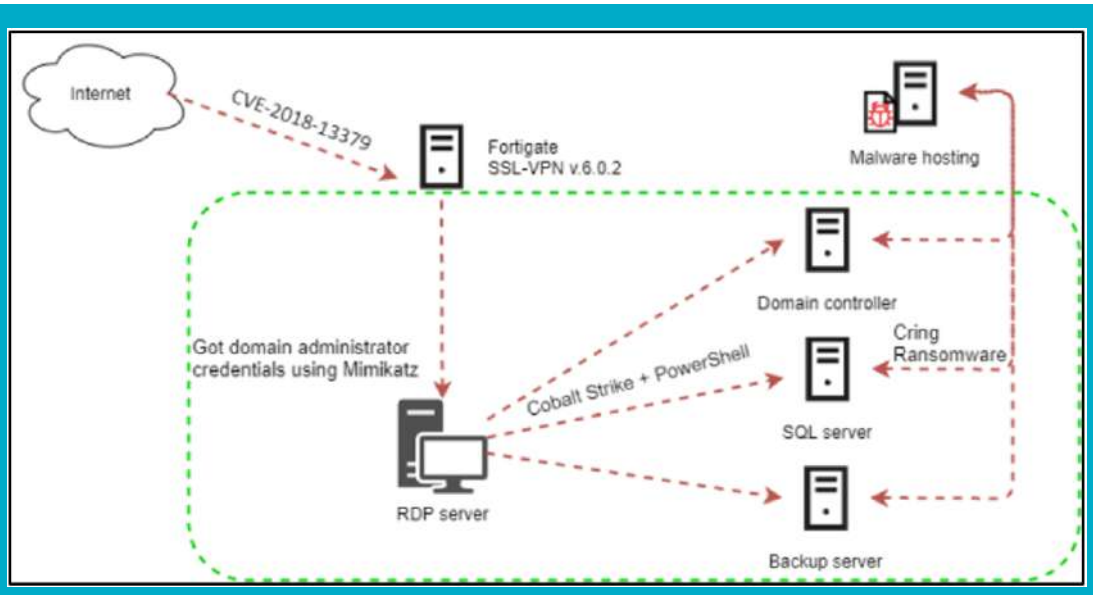
Setalah mendapatkan akses jaringan pada sistem pertama, Penyerang mengunduh Utilitas Mimikatz untuk mencuri kredensial pengguna sistem Operasi Windows yang baru saja melakukan log in ke sistem. Dengan memanfaatkan Mimikatz ini penyerang dapat melakukan compromiseakun domain Administrator, selanjutnya melakukan distribusi malware ke sistem lain dalam sistem yang sama. Penyerang biasanya menggunakan bantuan malware Cobal Strike yang di loaded pada sistem terdampak menggunakan PowerShell. CobalStrike akan memasang Backdoor untuk membuat komunikasi Commond and Control Server dengan alamat IP 198.12.112[.]204.

3. Encryption

Berikut Merupakan tahapan infeksi dari Cringe Ransomware:

- Setelah menginfeksi sistem, penyerang mengunduh cmd script ke sistem. Script tersebut sudah didesain untuk mengunduh dan menjalankan malware-Cring Ransomware.

- Setelah Script terinstall, cmd script ini akan diberi nama execute.bat dan akan dieksekusi. Penyerang akan menggunakan Teknik menghindari deteksi malware pada perangkat.
- Menjalankan perintah untuk mengunduh file dari internet ketika menjalankan PowerShell. File tersebut merupakan file perintah untuk menjalankan Cring Ransomware.
- Selanjutnya Cring Ransomware dapat mengenkripsi file di database serta menghapus Salinan backupnya. Selanjutanya Penyerang juga akan meletakkan sebuah Ransom Note

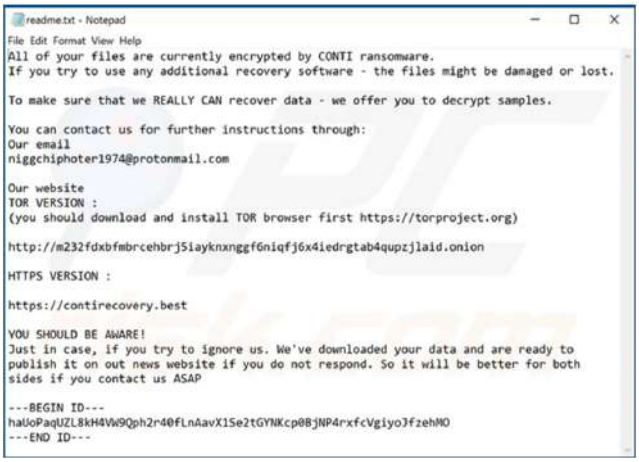


Gambar 7. Infeksi Cringe Ransomware

Sumber : https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Vulnerability-in-Fortigate-VPN-servers-is-exploited-in-Cring-ransomware-attacks-En.pdf

Conti Ransomware

Conti adalah jenis ransomware as a service dan evolusi dari ransomware Ryuk. Grup yang membuat Conti adalah "Wizard Spider" dari Rusia. Pertama kali terdeteksi Desember 2019. Aktivitas Conti meningkat secara signifikan pada tahun 2020. Pada Agustus 2020 Conti meluncurkan situs kebocoran di DarkWeb dan SurfaceWeb untuk mempublikasikan data yang dicuri dari korban yang tidak membayar. Conti memberikan ransomnote kepada korban yang memberi tahu korban bahwa jaringan korban terkunci, menginstruksikan untuk menghubungi alamat email untuk mendapatkan kunci dekripsi,


readme.txt - Notepad

File Edit Format View Help

All of your files are currently encrypted by CONTI ransomware.
If you try to use any additional recovery software - the files might be damaged or lost.

To make sure that we REALLY CAN recover data - we offer you to decrypt samples.

You can contact us for further instructions through:
Our email
niggchiphoter1974@protonmail.com

Our website
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://m232fdxbfmbrcehbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaid.onion

HTTPS VERSION :

https://contirecovery.best

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us ASAP

---BEGIN ID---
haUoPaqUZL8kH4VW9Qph2r40fLnAavX1Se2tGYNKcp0BjNP4rxfcVgiyoJfzehMO
---END ID---

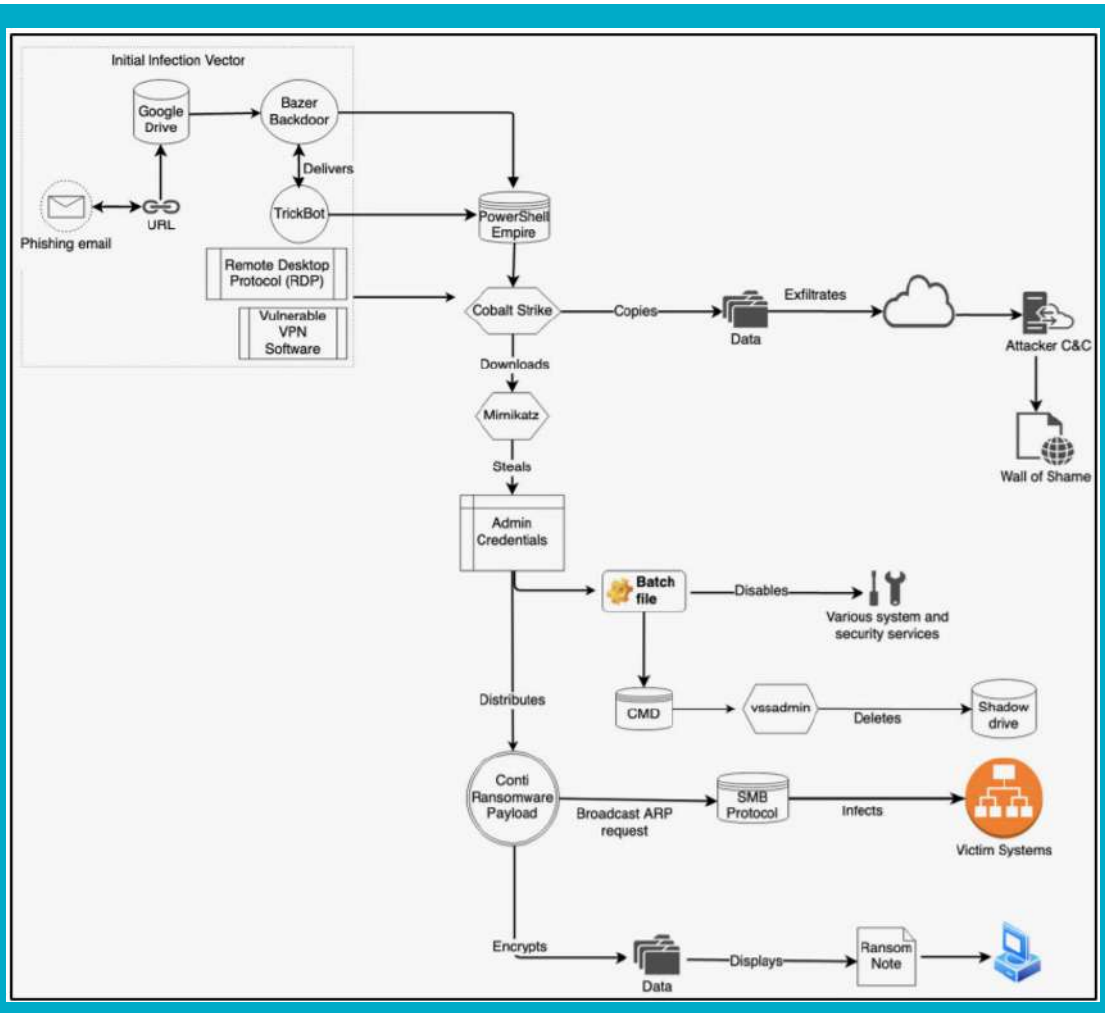
Gambar 8. Contoh Ransomnote Cooti Ransomware

Sumber: https://www.bleepingcomputer.com/news/security/conti-ransomware-also-targeted-irelands-department-of-health

dan menyatakan bahwa data pribadi akan dipublikasikan apabila pembayaran tidak dilakukan. Dalam kasus terkahir disebutkan bahwa Conti meminta tebusan sebesar $19.999.000.

Target dari ransomware Conti adalah entitas di sektor publik dan swasta, seperti retail, manufacturing, konstruksi, pemerintahan, kesehatan, makanan, logistik, layanan, hukum, nirlaba, perumahan, pendidikan, keuangan, farmasi, energi, media berita, akuntansi, komunikasi, hiburan, rumah sakit, pertambangan, dan utilitas. Secara geografis, insiden Conti ada di sekitaran Amerika Utara dan Eropa.

Berikut merupakan gambar dan penjelasan mengenai Attack Chain Conti Ransomware



Gambar 9. Attack Chain Conti Ransomware

- Wizard Spider mengirimkan email phishing yang menargetkan calon korban.
- Wizard Spider biasanya menggunakan Google Docs yang sah dalam bentuk URL di dalam email. Email phisihing mendorong pengguna untuk mengklik URL, yang kemudian akan mengunduh dokumen berbahaya yang akan mengirimkan backdoor Bazar atau Trickbot ke system korban.

- Melalui Bazar, Spider Wizard mengunduh Cobalt Strike dan beberapa hacktools untuk lingkungan korban.
- Bazar membuat scheduled task menjadi persistent.
- Cobalt Strike mengunduh dan menjalankan Mimikatz dalam memori korban untuk menghindari deteksi.
- Penyerang menggunakan Mimikatz untuk mencuri kredensial korban. Bazar juga dapat mencuri informasi kredensial dari browser korban.
- Data korban dan file/pesan terkait email dikumpulkan dan dikirim Kembali C&C.
- Cobalt Strike mengunduh dan menjalankan file batch yang sudah disediakan oleh penyerang. File batch mengidentifikasi dan menonaktifkan layanan yang dipilih oleh penyerang didistribusikan ke seluruh lingkungan dan dijalankan di setiap sistem.
- Penyerang menghapus local shadow copies melalui Windows Volume Shadow Copy Service (VSS) untuk mencegah korban memulihkan data.
- Cobalt Strike dan PSExec mendistribusikan payload ransomware Contri ke seluruh lingkungan. Dalam beberapa kasus, penyerang menggunakan domain controller melalui akses admin untuk menyebarkan ransomware ke seluruh jaringan.
- Setelah ransomware dijalankan, ransomnote diberikan kepada korban

Mapping MITRE ATT&CK terkait dengan TTP yang digunakan Conti Ransomware

TACTICS	TECHNIQUE	KETERANGAN
Execution	Native API (T1106)	Conti menggunakan API call selama eksekusi
	Command and Scripting Interpreter : Windows Command Shell (T1059.003)	Conti dapat menggunakan opsi command line untuk memungkinkan penyerang mengontrol cara memindai dan mengenkripsi file.
Privilege Escalation	Process Injection: Dynamic-link Library Injection (T1055.001)	Conti telah memuat DLL terenkripsi ke dalam memori dan kemudian menjalankannya
Defense Evasion	Deobfuscate/ Decode Files or Information (T1140)	Conti telah mendekripsi payload dengan kunci AES-256 yang di-harcode
	Obfuscated Files or Information (T1027)	Conti telah mengenkripsi DLL dan menggunakan obfuscation untuk menyembunyikan panggilan Windows API

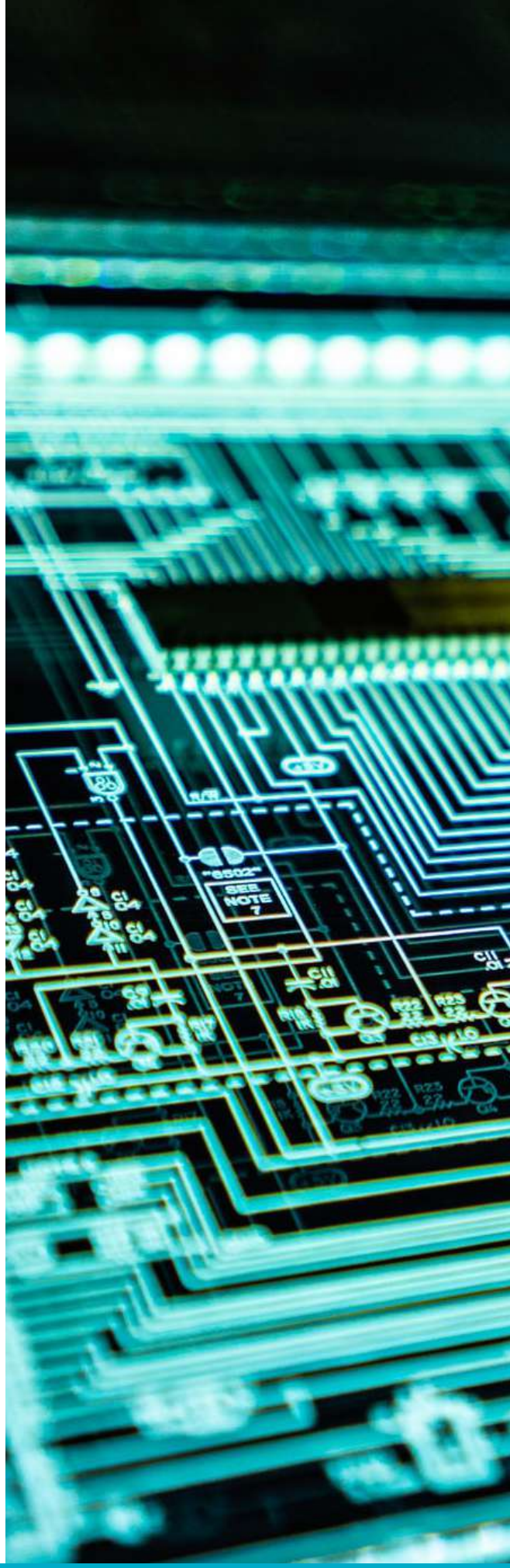
TACTICS	TECHNIQUE	KETERANGAN
Discovery	File and Directory Discovery (T1083)	Conti dapat menemukan file di sistem lokal
	Network Share Discovery (T1135)	Conti dapat melakukan enumerasi berbagai jaringan SMB jarak jauh yang terbuka menggunakan NetShareEnum()
	Process Discovery (T1057)	Conti dapat melakukan enumerasi melalui semua proses yang terbuka untuk mencari apapun yang memiliki string "sql" dalam nama prosesnya
	System Network Configuration Discovery (T1016)	Conti dapat mengambil cache ARP dari sistem lokal dengan menggunakan GetIpNetTable()API call dan memeriksa memastikan alamat IP yang dihubungkannya untuk sistem lokal, non-Internet
	System Network Connections Discovery (T1049)	Conti dapat melakukan enumerasi koneksi jaringan rutin dari host yang dikompromikan
Lateral Movement	Taint Shared Content (T1080)	Conti dapat menyebar sendiri dengan menginfeksi remote machine lainnya melalui network shared drive
	Remote Services: SMB/Windows Admin Shares (T1021.002)	Conti dapat menyebar melalui SMB dan mengenkripsi file pada host yang berbeda dan berpotensi membahayakan seluruh jaringan
Impact	Data Encrypted for Impact (T1486)	Conti dapat menggunakan CreateIoCompletionPort(), PostQueuedCompletionStatus(), dan GetQueuedCompletionPort() untuk mengenkripsi file dengan cepat, tidak termasuk file yang berekstensi .exe, .dll, dan .lnk. Ini telah menggunakan kunci enkripsi AES-256 yang berbeda per file dengan kunci enkripsi publik RAS-4096 yang dibundel unik untuk setiap korban. Conti dapat menggunakan "Windows Restart Manager" untuk memastikan file tidak terkunci dan terbuka untuk enkripsi
	Inhibit System Recovery (T1490)	Conti dapat menghapus Windows Volume Shadow Copies menggunakan vssadmin
	Service Stop (T1489)	Conti dapat menghentikan hingga 146 layanan Windows yang terkait dengan keamanan, pencadangan, basis data, dan solusi email melalui penggunaan net stop

Babuk Ransomware

Babuk Ransomware atau Babuk Locker adalah ransomware baru yang diluncurkan pada awal tahun 2021. Babuk Locker, juga dikenal sebagai Babyk dan awalnya dikenal sebagai Vasa Locker. Babuk Locker menggunakan taktik big-game hunter untuk mencuri, mengenkripsi, dan membocorkan data korban yang menargetkan perusahaan. Berdasarkan negosiasi tebusan dengan korban yang berhasil diidentifikasi, permintaan uang tebusan berkisar dari USD 60.000 hingga USD 85.000 dalam bentuk Bitcoin.

Sebagaimana kebanyakan ransomware, korban kemungkinan besar ditentukan berdasarkan seberapa mudah data korban di-compromised serta kemampuan korban dalam membayar uang terbusan. Meskipun demikian, Threat Actor dari Babuk menyatakan bahwa grup tersebut tidak akan menargetkan rumah sakit, badan amal non-profit atau sekolah serta menghindari organisasi dengan pendapatan tahunan kurang dari USD 4 juta. Meskipun demikian, klinik swasta dan universitas besar bersama dengan yayasan amal yang membantu perjuangan LGBT dan BLM masih dianggap sebagai target.

Sejalan dengan dengan hal di atas, korban yang dapat diidentifikasi sejauh ini mencakup organisasi yang beroperasi di sektor layanan digital, teknik, dan perawatan kesehatan yang beroperasi di Jerman, Hong Kong, Swedia, dan Amerika Serikat. Data lain juga menunjukkan bahwa sampel malware ini telah muncul di negara-negara Asia, Eropa, dan Amerika Utara lainnya meskipun hal ini lebih cenderung disebabkan oleh aktivitas peneliti keamanan yang meningkat.



NetWalker Ransomware

Netwalker merupakan jenis ransomware yang dikembangkan pertama kali oleh kelompok hacker berbahasa Rusia "Circus Spider" pada September 2019. Netwalker menggunakan pendekatan sebagai Ransomware-as-a-Service (RaaS) dalam operasinya. Ransomware ini menggunakan teknik enkripsi tingkat lanjut untuk mengargetkan sistem operasi berbasis Windows. Netwalker mendistribusikan malware melalui email spam yang memikat korban sebagai umpan phishing dan menginfeksi komputer di jaringan mereka. Isu COVID-19 dimanfaatkan oleh Netwalker dalam melakukan phising melalui email, dilanjutkan dengan eksfiltrasi dan enkripsi data.

Selain itu serangan Netwalker menggunakan ekploitasi VPN, jaringan interface aplikasi web dan Remote Desktop Protocol (RDP). Setelah mendapatkan data dari korban, Pelaku kejahatan Netwalker akan mempublikasikan hasil data pada Darkweb sebagai bukti serangan yang berhasil. Selanjutnya korban akan ditekan untuk membayar tebusan dalam bentuk Bitcoin. Serangan Netwalker menargetkan perusahaan yang berkaitan dengan penyedia layanan kesehatan, fasilitas pendidikan, pemerintah lokal, dan perusahaan swasta.

Berikut merupakan tahapan infeksi NetWalker Ransomware:

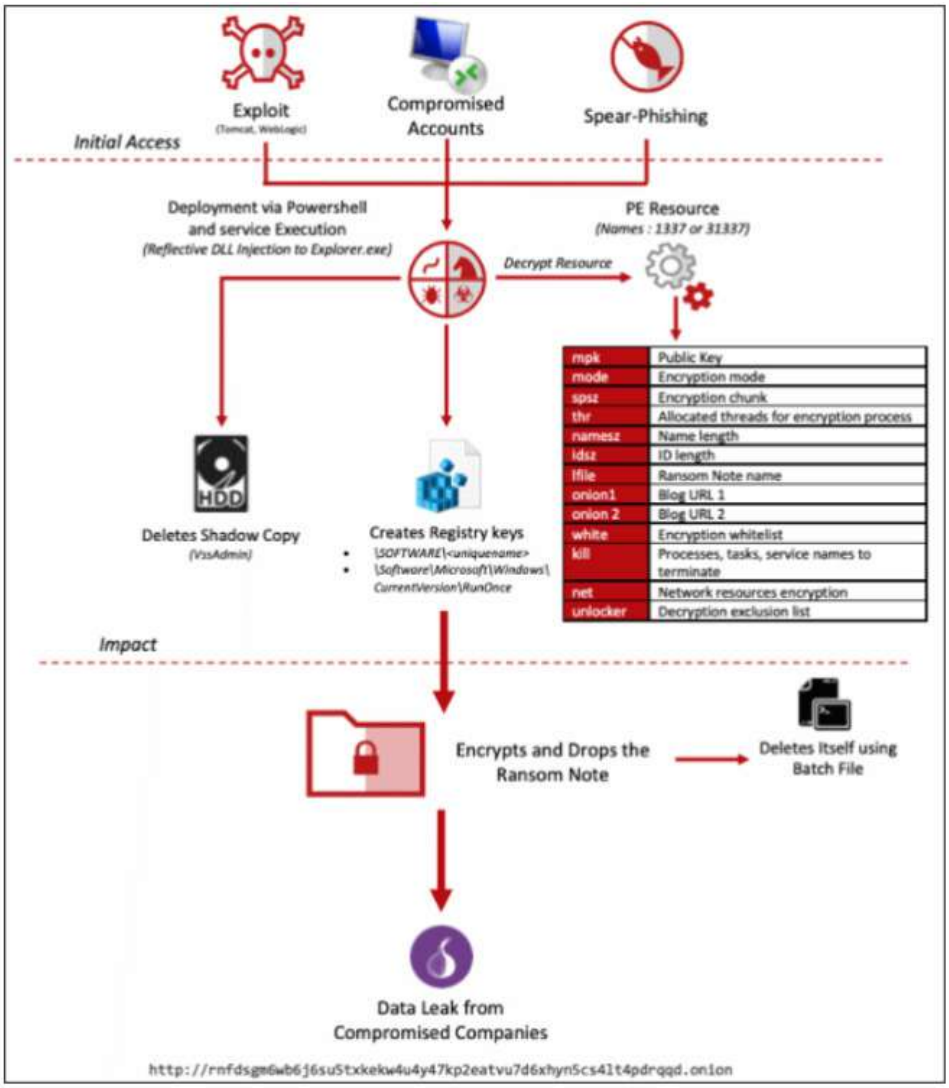
1. Netwalker sangat bergantung pada phishing dan spear-phishing sebagai metode penyusupan mereka. Netwalker mengirimkan email yang seolah-olah dikirim dari sumber yang sah untuk menjebak korban. Biasanya Netwalker akan melampirkan skrip VBS bernama "CORONAVIRUS_COVID-19.vbs" yang akan mengeksekusi ransomware ketika mereka mengklik dua kali email atau membuka dokumen terlampir.

2. Setelah berada di sistem, ransomware ini akan akan mengelabuhi sistem sehingga melakukan proses yang tampak sah, biasanya dalam bentuk Microsoft. Selanjutnya akan proses hollowing akan memulai proses hollowing dimana memberi ransomware banyak waktu untuk bekerja melalui jaringan, mengeksfiltrasi dan mengenkripsi data, menghapus cadangan, dan meninggalkan backdoor sebelum ada yang menyadari ada yang salah.

3. Setelah Netwalker selesai mengeksfiltrasi dan mengenkripsi data, korban akan menyadari ada sesuatu yang salah dan menemukan catatan tebusan. Netwalker kemudian akan meminta sejumlah uang untuk dibayarkan dalam Bitcoin, menggunakan portal browser TOR.

4. Setelah korban memenuhi tuntutan pelaku, mereka akan diberikan akses ke alat dekripsi khusus untuk mendekripsi data dengan aman. Netwalker akan meningkatkan tebusan atau melepaskan sebagian atau semua data yang dicuri ke darkweb jika korban tidak memenuhi permintaan sesuai waktu yang ditentukan.

Pada gambar berikut juga dijelaskan mengenai diagram infeksi yang dilakukan oleh NerWalker Ransomware:



Gambar 10. Diagram infeksi NetWalker Ransomware

INSIDEN RANSOMWARE //

Berikut ini merupakan contoh kasus ransomware yang menyerang beberapa Instansi di seluruh dunia:

Korban Ransomware dari Harrison Federation yang Berbasis di London

Ringkasan Insiden

Harrison Federation, lembaga nonprofit multi-akademi terpercaya yang berbasis di London, menjadi korban serangan ransomware.

Analisis

Harrison Federation adalah badan amal pendidikan yang menjalankan 50 Sekolah Dasar dan Menengah yang mmeiliki 37.000 siswa dari London dan sekitarnya. Mereka menyadari telah menjadi korban serangan ransomware pada 27 Maret 2021. Lembaga nonprofit tersebut juga menonaktifkan sistem email dan telepon rumah, serta semua panggilan telepon dialihkan ke ponsel.

Harrison Federation bekerja sama dengan National Crime Agency (NCA), National Cyber Security Centre (NCSC), dan perusahaan keamanan siber untuk menyelidiki insiden tersebut.

Ransomware yang digunakan dalam serangan tersebut saat ini tidak diketahui. NCSC mengeluarkan peringatan di awal bulan tentang peningkatan ransomware yang menargetkan institusi pendidikan.

Black KingDom Ransomware Targeting Vulnerable Exchange Servers

Ringkasan Insiden

Sophos mendeteksi varian ransomware baru yang digunakan dalam serangan terhadap Server Microsoft Exchange yang rentan yang masih belum dilakukan *patching* untuk kerentanan ProxyLogon.

Analisis

Telemetri Sophos mendeteksi varian ransomware baru dengan aktivitas yang dimulai pada 18 Maret 2021. Ransomware baru, yang disebut Black KingDom, digunakan dalam serangan yang menargetkan server Microsoft Exchange yang belum menerapkan patch untuk kerentanan ProxyLogon CVE-2021-27065.

Pengiriman dimulai oleh alamat IP yang memiliki geolokasi di Jerman dan termasuk dalam exit node Tor. Setelah mengeksploitasi, pelaku ancaman mengirimkan webshell dan memanfaatkan Remote Code Execution di server Exchange. Perintah PowerShell tersebut mengunduh dan menjalankan payload ransomware.

Ransomware mengimplementasikan TTP ransomware dasar sebagai berikut:

- Daftar folder yang tidak dienkripsi untuk memastikan sistem yang ditargetkan masih dapat berfungsi dan menampilkan catatan tebusan.
- Pasangan kunci korban dan ID agar mudah mengidentifikasi korban dan memberikan kunci dekripsi terkait saat pembayaran tebusan.
- Enkripsi file dan penggantian nama ekstensi.

Rumah Sakit Belgia CHwapi terkena serangan Ransomware - Kemungkinan Smokescreen

Ringkasan Insiden

Tim menilai dengan "low confidence" bahwa insiden di Belgian Hospital Hub CHwapi kemungkinan operasi dari Smokescreen, karena detail di sekitarnya tidak konsisten dengan operasi ransomware biasa.

Analisis

Pada malam tanggal 17 Januari 2021, pusat rumah sakit Wallonie Picarde, CHwapi, mengalami serangan dunia maya yang mengenkripsi 80 dari 300 server yang menyebabkan gangguan besar pada layanan TI, memaksa rumah sakit untuk mengarahkan kembali pasien yang masuk ke rumah sakit dan klinik terdekat. Staf harus bergantung pada pena dan kertas untuk terus bekerja.

Alih-alih mengandalkan perangkat lunak malware, penyerang menggunakan alat Windows resmi BitLocker untuk mengenkripsi 100TB data. Menurut penyelidik forensik, para penyerang tidak meninggalkan catatan tebusan dengan informasi kontak dan pembayaran karena ini adalah praktik umum dalam serangan ransomware.

Conti Ransomware yang menyerang Departemen Kesehatan Irlandia

Ringkasan Insiden

Pada Tanggal 14 Mei 2021, terdeteksi adanya aktivitas siber yang berbahaya di jaringan Departemen Kesehatan Irlandia. Kemudian dilakukan investigasi diketahui bahwa departemen Kesehatan terkena serangan ransomware Conti di bagian Health Service Executive (HSE).

Analisis

Saat proses investigasi, terdeteksi upaya eksekusi ransomware yang sedang berlangsung sehingga langsung dihentikan. Ditemukan Cobalt Strike Beacon yang dipasang di jaringan. Cobalt Strike Beacon merupakan alat akses jarak jauh yang sering digunakan oleh penyerang untuk melakukan lateral movement di suatu lingkungan sebelum melakukan eksekusi muatan ransomware. Serangan ransomware ini menyebabkan HSE menutup seluruh infrastruktur TI layanan Kesehatan untuk membatasi dampaknya. Serangan tersebut berdampak kepada operasi Kesehatan dan beberapa prosedur non darurat yang ditunda karena rumah sakit sedang mengimplementasikan Business Continuity Plan (BCP). Conti mengklaim memiliki 700 GB file yang tidak terenkripsi, seperti info karyawan dan pasien, laporan keuangan, penggajian, kontrak, dan banyak lagi. Namun HSE menolak untuk membayar tebusan stersebut seharga $19.999.000

INDICATOR OF COMPROMISE (IOC) //

Indicator of Compromise Avaddon Ransomware

Javascript Downloader (SHA256)
12bc439445f10a04b574d49ed8ccc405e2dfaa493747585439643e8a2129e5e5
cc4d665c468bcb850baf9baab764bb58e8b0ddcb8a8274b6335db5af86af72fb
94faa76502bb4342ed7cc3207b3158027807a01575436e2b683d4816842ed65d
b8d6fd333973adb640649cab8c9e7575a17b5a8bc382e3335400d43a606a6253
5a47a89a870d7db244c76da43887e33c9ee4b26f9972878b1a6616be0302439f
a481d2b64c546f68d55e1fd23e57ada80b6b4e2c3dd7b0466380dba465f3d318
c06e2e3fe09f92007ff589e46a57cb8efa1fe261d7b8193190eb648cf7961a4b

Avaddon Ransomware (SHA256)
d1c1dfa0117fc595419464578959feb4c459ab99a498e0cb66cee626ceff6835
f3f4d4e4c6704788bc8954ca6f6ddc61b006aba89d5d384794f19424a3d24132
6616abb725c24307f4f062996edc5150079bc477acd4236a4f450e5835a20c62
05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2
dccc689c986e357d5dbdc987e72e6b8a0e9017cbf347449b27c84b8b7b9d507a

Indicator of Compromise DarkSide Ransomware

MD5
04fde4340cc79cd9e61340d4c1e8ddfb
0e178c4808213ce50c2540468ce409d3
0ed51a595631e9b4d60896ab5573332f
130220f4457b9795094a21482d5f104b
1a700f845849e573ab3148daef1a3b0b
1c33dc87c6fdb80725d732a5323341f9
222792d2e75782516d653d5cccfcf33b
29bcd459f5ddeeefad26fc098304e786
3fd9b0117a0e791918596301480dcdc6d
47a4420ad26f60bb6bba5645326fa963
4d419dc50e3e4824c096f298e0fa885a
5ff75d33080bb97a8e6b54875c221777
66ddb290df3d510a6001365c3a694de2
68ada5f6aa8e3c3969061e905ceb204c
69ec3d1368adbe75f3766fc88bc64afc
6a7fdab1c7f6c5a5482749be5c4bf1a4
84c1567969b86089cc33dccf41562bcd
885fc8fb590b899c1db7b42fe83dddc3
91e2807955c5004f13006ff795cb803c
9d418ecc0f3bf45029263b0944236884
9e779da82d86bcd4cc43ab29f929f73f
a3d964aaf642d626474f02ba3ae4f49b
b0fd45162c2219e14bdccab76f33946e
b278d7ec3681df16a541cf9e34d3b70a
b9d04060842f71d1a8f3444316dc1843
c2764be55336f83a59aa0f63a0b36732
c4f1a1b73e4af0fbb63af8ee89a5a7fe
c81dae5c67fb72a2c2f24b178aea50b7
c830512579b0e08f40bc1791fc10c582
cfcfb68901ffe513e9f0d76b17d02f96

MD5
d6634959e4f9b42dfc02b270324fa6d9
e44450150e8683a0addd5c686cd4d202
f75ba194742c978239da2892061ba1b4
f87a2e1c3d148a67eaeb696b1ab69133
f913d43ba0a9f921b1376b26cd30fa34
f9fc1a1a95d5723c140c2a8effc93722

Indicator of Compromise Conti Ransomware

SHA-256
d21c71a090cd6759efc1f258b4d087e82c281ce65a9d76f20a24857901e694fc
234e4df3d9304136224f2a6c37cb6b5f6d8336c4e105afce857832015e97f27a
1429190cf3b36dae7e439b4314fe160e435ea42c0f3e6f45f8a0a33e1e12258f
8837868b6279df6a700b3931c31e4542a47f7476f50484bdf907450a8d8e9408
A390038e21cbf92c36987041511dcd8dcfe836ebbabee733349e0b17af9ad4eb
d4a1cd9de04334e989418b75f64fb2cfbacaa5b650197432ca277132677308ce
5a2e947aace9e081ecd2cfa7bc2e485528238555c7eeb6bcca560576d4750a50
d3c75c5bc4ae087d547bd722bd84478ee6baf8c3355b930f26cc19777cd39d4c
f092b985b75a702c784f0936ce892595b91d025b26f3387a712b76dcc3a4bc81
e64e350861b86d4e05668bc25e6c952880f6b39ca921496ccce1487dbf6acab6
707b752f6bd89d4f97d08602d0546a56d27acfe00e6d5df2a2cb67c5e2eeee30
03b9c7a3b73f15dfc2dcb0b74f3e971fdda7d1d1e2010c6d1861043f90a2fecd
b524ed1cc22253f09d56f54d8ded4566b63352ff739f58de961f8a5bebb0fad9
1ef1ff8b1e81815d13bdd293554ddf8b3e57490dd3ef4add7c2837ddc67f9c24
c14f8bc656284715516f26935afe487a1d584f56ffabbcb98f2974f6ca6cd3a4
e16fea1b8874cc6b26e7e2df9697f03f86efa82247bb3b2922f1d05052dbcbb4
5d8a701110d58ab7c1aa8bae6bc9d5358b8cd508115891320e6af6c68f3bbd74
ebeca2df24a55c629cf0ce0d4b703ed632819d8ac101b1b930ec666760036124
D236d64b7bf9510ea1746d10a4c164a2ef2c724cc62b2bca91d72bdf24821e40
2579148e5f020145007ac0dc1be478190137d7915e6fbca2c787b55dbec1d370
Files
b52c0640957e5032b5160578f8cb99f9b066fde4f9431ee6869b2eea67338f28.dll.exe
b52c0640957e5032b5160578f8cb99f9b066fde4f9431ee6869b2eea67338f28
icju1.exe
e54f38d06a4f11e1b92bb7454e70c949d3e1a4db83894db1ab76e9d64146ee06
rate_x32.dat
eb79168391e64160883b1b3839ed4045b4fd40da14d6eec5a93cfa9365503586
192145.dll
f29bc338e63a62c24c301c0496108401381673 3dad446a29c20d4413c5c818af9
_EXE.bat
_COPY.bat

Network
IcedID
vaclicinni[.]xyz
thulleultinn[.]club
oxythuler[.]cyou
dictorecovery[.]cyou
expertulthima[.]club
68.183.20[.]194:80
159.89.140[.]116:443
83.97.20[.]160:443
Cobalt Strike
dimentos[.]com
192.99.178[.]145:80
Proxy 38.135.122[.]194:8080

MITIGASI JIKA TERKENA RANSOMWARE //

Hal-hal harus dilakukan jika perusahaan atau organisasi terkena serangan ransomware:

- Berikut merupakan best practices yang dapat dilakukan dalam proses tanggap insiden untuk kasus insiden ransomware:
    1. Tentukan jenis ransomware yang menginfeksi. Langkah ini bertujuan untuk melakukan langkah tanggap insiden yang tepat. Hal ini dapat dilakukan dengan melakukan langkah-langkah berikut:
        - Mengidentifikasi pesan yang ditampilkan oleh Ransomware, baik yang ditampilkan melalui GUI (Graphical User Interface), text atau file html yang umumnya kerap kali muncul setelah proses infeksi ransomware.
        - Identifikasi kontak email dan ekstensi file yang dihasilkan oleh ransomware saat mengenkripsi file pada komputer yang terinfeksi.
    2. Lakukan asesmen ruang lingkup dari infeksi ransomware. Hal ini bertujuan untuk mengetahui sistem apa saja yang terdampak sehingga dapat diketahui potensi penyebaran ransomware tersebut.
    3. Lakukan asesmen dampak untuk menentukan level prioritas dari langkah penanganan insiden. Pada tahapan ini lakukan penilaian terhadap hal berikut:
        - Lakukan penilaian dampak fungsional, yang menyebabkan terganggungnya layanan atau proses operasional bisnis.
        - Lakukan penilaian dampak mengenai informasi yang disandera oleh pelaku kejahatan.
    4. Temukan bagaimana proses infeksi malware berjenis ransomware tersebut dapat terjadi. Lakukan pemeriksaan terhadap kemungkinan sumber penyebab infeksi, misal attachment e-mail, kerentanan aplikasi, self propagasi dari malware, infeksi melalui perangkat removable drives, infeksi oleh malware lainnya.
    5. Tentukan rencana remediasi berdasarkan analisis dampak, serta pertimbangan lain yang dihasilkan dari langkah sebelumnya.

6. Lakukan proses containment atau isolasi. Pada kasus insiden ransomware tahapan ini merupakan tahapan kritikal. Langkah ini bertujuan untuk mencegah penyebar luasan infeksi ransomware. Beberapa hal yang perlu dilakukan karantina antara lain, yaitu:
    - Sistem yang terinfeksi;
    - Pengguna dan grup pengguna yang terdampak;
    - Isolasi layanan file sharing;
    - Isolasi layanan database;
    - Isolasi backup file yang dimiliki;
    - Lakukan pemblokiran akses ke domain dan alamat IP yang digunakan oleh ransomware;
    - Pastikan proteksi endpoint diaktifkan dan dimutakhirkan;
    - Lakukan patch terhadap celah keamanan yang dimanfaatkan oleh ransomware.
7. Lakukan Proses Eradikasi. Langkah ini bertujuan untuk menghapus infeksi ransomware sebelum proses recovery dilakukan, guna memastikan tidak ada reinfeksi kembalik. Lakukan proses eradikasi secara bertahap dengan memantau apakah kemungkinan terjadi proses reinfeksi kembali.
8. Komunikasikan langkah penanganan insiden malware kepada pemangku kepentingan, seperti penyedia teknologi keamanan dan TI, pelanggan maupun pengguna internal, pihak regulator atau otoritas keamanan siber.
9. Lakukan Proses pemulihan. Hal ini bertujuan agar proses operasional bisnis dapat berjalan kembali. Lakukan langkah berikut ini:
    - Cari mengenai kemungkinan adanya decryptor dari ransomware tersebut;
    - Lakukan pemulihan dari salinan yang bersih atau bebas dari infeksi, lakukan pemantauan setelah proses eradikasi.

- Lakukan penambahan IoC pada perangkat keamanan yang dimiliki untuk mengetahui luas dari infeksi malware tersebut.
- Melakukan edukasi kesadaran dan budaya keamanan siber kepada seluruh pemangku kepentingan.

PENCEGAHAN INFEKSI RANSOMWARE //

A. Selalu Melakukan Backup Secara Berkala

Dengan memiliki backup yang senantiasa diperbarui, maka jika terjadi serangan siber keseluruhan sistem dapat dipulihkan dengan cepat dan mudah dimana backup yang tersimpan dapat menggantikan sistem yang terganggu oleh serangan. Beberapa hal tambahan yang perlu diperhatikan pada saat melakukan backup antara lain:

- Pastikan backup yang sudah dibuat dapat digunakan. Untuk memastikan hal ini, dapat dilakukan pengujian untuk mengetahui kehandalan dari sistem backup yang digunakan.
- Pastikan terdapat backup yang disimpan secara offline atau terpisah dan tidak terhubung dengan sistem utama yang di-backup. Hal ini untuk mencegah ransomware menemukan backup yang sudah dibuat dan menghapusnya sebelum melakukan infeksi.

B. Meningkatkan Kesadaran Keamanan Siber Personel

Pengetahuan dan kesadaran personil terhadap keamanan siber merupakan hal yang sangat penting dalam upaya memberikan perlindungan terhadap sistem dari serangan siber. Beberapa hal yang dapat dilakukan personil untuk terhindar dari serangan ransomware atau malware lainnya antara lain:

- Tidak mengunjungi situs-situs yang tidak dapat dipercaya atau berbahaya, contohnya situs yang menyediakan konten film, musik, atau aplikasi ilegal.

- Menghindari membuka attachment e-mail yang berasal dari sumber yang tidak dikenal.
- Menggunakan internet dengan bijak dan aman.
- Tim yang bertanggung jawab terhadap jaringan atau sistem yang terhubung dengan internet harus memiliki kewaspadaan lebih sehingga dapat mendeteksi jika terdapat upaya-upaya serangan yang ditujukan terhadap sistem yang dikelola.

C. Memblokir akses terhadap situs yang tidak dapat dipercaya atau berbahaya

Situs-situs yang tidak dapat dipercaya atau berbahaya, seperti situs yang menyediakan konten atau software ilegal berpotensi dikendalikan oleh penjahat siber untuk menanamkan malware, termasuk ransomware kepada komputer pengunjung. Dengan melakukan pemblokiran, maka personil yang bertugas tidak dapat mengunjungi situs-situs berbahaya baik secara sengaja maupun tidak disengaja sehingga akan menurunkan risiko infeksi malware.

D. Melakukan penyaringan email (spam filtering)

Penyaringan email dapat membantu mencegah penyebaran ransomware melalui metode phishing yang dilakukan melalui email. Jika memungkinkan, gunakan teknologi seperti Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), dan DomainKeys Identified Mail (DKIM) untuk mencegah email spoofing.

E. Mengimplementasikan Intrusion Prevention System (IPS)/Intrusion Detection System (IDS) serta firewall

IPS/IDS serta firewall dapat melakukan pemblokiran terhadap alamat IP malicious yang diketahui serta memberikan peringatan (alert) apabila terdapat indikasi adanya serangan, termasuk serangan ransomware di dalam jaringan sehingga pengelola jaringan dapat melakukan tindakan-tindakan yang diperlukan untuk mencegah infeksi ransomware di dalam jaringan yang dikelolanya.

F. Menutup akses internet kepada servis yang tidak membutuhkan akses internet

Servis yang tidak membutuhkan diakses melalui internet seperti Server Message Block (SMB) dan Remote Desktop Protocol (RDP)

G. Memastikan penggunaan password yang kuat pada seluruh sistem dan servis yang berjalan

Pastikan semua pengguna, sistem, dan servis yang berjalan tidak menggunakan password bawaan atau password yang mudah ditebak.

H. Selektif dalam memilih vendor pengembang aplikasi atau sistem

Pastikan vendor yang bekerja sama memiliki pengetahuan dan kemampuan untuk menerapkan tindakan-tindakan pengamanan terhadap sistem atau aplikasi anda.

I. **Melakukan patch security secara berkala khususnya untuk sistem operasi, software, dan firmware yang digunakan.** Jika memungkinkan, gunakan centralized patch management system.

J. **Menggunakan Antivirus yang selalu diperbarui** pada komputer yang digunakan untuk operasional organisasi.

K. **Mengelola penggunaan akun yang memiliki hak akses (privilege) dengan baik,** yaitu dengan hanya memberikan pengguna akses administratif jika diperlukan dan pengguna yang bertindak sebagai administrator hanya digunakan saat diperlukan.

L. **Memberlakukan pembatasan akses** melalui akses kontrol dengan baik.

M. **Menerapkan application whitelisting,** yaitu dengan hanya mengizinkan program tertentu untuk dijalankan.

N. **Melakukan pengkategorian** data berdasarkan nilai data tersebut bagi organisasi serta mengimplementasikan pemisahan fisik dan logik terhadap jaringan dan data bagi setiap unit organisasi yang berbeda.

O. **Mengimplementasikan Software Restriction Policies (RSP)** atau kontrol keamanan lainnya untuk mencegah program mengeksekusi ransomware dari lokasi yang biasanya digunakan oleh ransomware, seperti folder temprorer dan folder AppData/LocalAppData.

P. **Melakukan vulnerability assessment dan penetration test secara berkala** untuk mengetahui kerentanan-kerentanan yang terdapat pada sistem sehingga dapat dilakukan perbaikan untuk menutup kerentanan-kerentanan tersebut.

PUSAT KONTAK SIBER

Pusat Kontak Siber merupakan salah satu layanan publik yang dimiliki oleh BSSN dan dikelola oleh Pusopskamsinas. Layanan ini diberikan untuk masyarakat yang akan melakukan **Aduan Siber** secara perorangan maupun secara organisasi. Media yang dapat digunakan oleh masyarakat untuk melakukan pelaporan aduan siber, yaitu melalui telepon, surat elektronik (email), ataupun datang secara langsung ke kantor BSSN.

PUSOPSKAMSINAS BADAN SIBER DAN SANDI NEGARA

(021)788 33610
BANTUAN70@BSSN.GO.ID / WWW.IDSIRTII.OR.ID
JL. HARSONO RM NO. 70, KEL. RAGUNAN,
KEC. PASAR MINGGU, JAKARTA SELATAN, 12550

PUSAT OPERASI KEAMANAN SIBER NASIONAL
NATIONAL CSIRT OF INDONESIA
id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER