



2025

SECURITY REPORT

**Comprehensive Analysis of BERT Ransomware
Infection Chain and Countermeasures**



github.com/Abdibimantara



abdibimantara.github.io



abdibimantara91@gmail.com

Contents

1. Overview of BERT ransomware.....	3
2. Ransomware Target National and Sector	3
3. Attack vector and Delivery Methods	5
4. Ransomware infection chain	5
5. Preparation for lab.....	7
6. Finding and Analysis	10
7. Conclusion	19
8. Recommendation	20
Reference	20

1. Overview of BERT ransomware

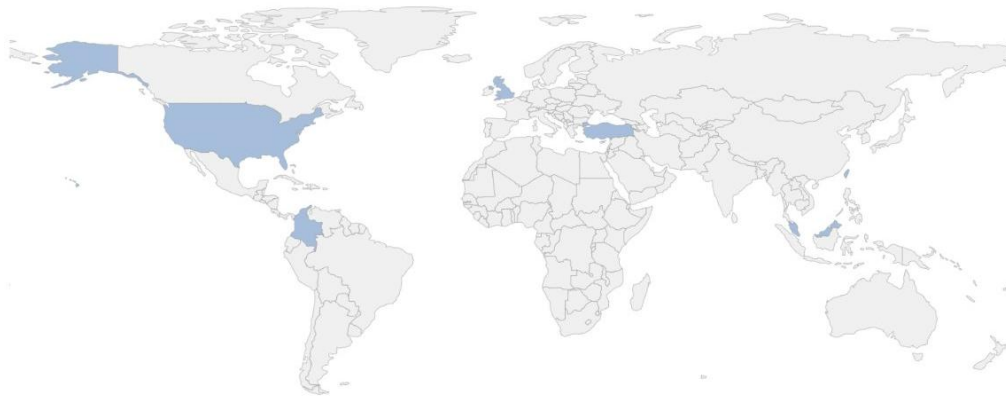
Aktivitas ransomware bert pertama kali dimulai pada pertengahan maret 2025, namun berhasil terdeteksi pertama kali pada April 2025. Korban pertama yang diketahui dari serangan ini merupakan sebuah perusahaan manufaktur di Amerika Serikat, SIMCO Electronics, yang mengalami kompromi pada tanggal 30 April 2025. Sejak awal kemunculannya, BERT menunjukkan modus operasi yang terorganisir dan terencana dengan membangun infrastruktur di dark web, yang meliputi situs kebocoran data khusus serta platform negosiasi. Hal ini menandakan bahwa grup ini mengadopsi strategi jangka panjang berfokus pada pemerasan dan eksploitasi data hasil serangan.















Selain menargetkan sistem operasi Windows, kelompok BERT juga mengembangkan kemampuan serangan lintas platform dengan menyasar sistem berbasis Linux. Pendekatan multi-platform ini meningkatkan kompleksitas dan cakupan dampak serangan, karena ransomware harus mampu mengatasi berbagai mekanisme pertahanan dan struktur sistem yang berbeda. Dengan demikian, serangan BERT bukan hanya ancaman konvensional tetapi juga memperlihatkan evolusi teknik yang menggabungkan eksploitasi sistem operasi dan penggunaan algoritma enkripsi yang kuat di kedua lingkungan tersebut.

Keberadaan infrastruktur dark web yang kokoh dan diversifikasi target platform menjadikan BERT sebagai ancaman siber yang tidak hanya canggih secara teknis tetapi juga sangat berbahaya dari segi operasional. Strategi mereka yang menggabungkan enkripsi data agresif, pengelolaan platform negosiasi, dan ancaman publikasi data rahasia menunjukkan bahwa serangan ini dirancang untuk memaksimalkan tekanan finansial dan psikologis pada korban. Institusi ataupun organisasi yang menjadi target harus memahami ancaman ini sebagai ancaman tingkat tinggi yang memerlukan kesiapan teknis dan operasional yang sangat matang.

2. Ransomware Target National and Sector

Berdasarkan laman resmi yang dipublikasi oleh tim riset trendmicro.com disertai dengan statistik dari ransomware.live, terdapat beberapa negara yang menjadi target serangan ransomware Bert tersebut.



S5 Agency World  Discovery Date: 2025-06-10  S5 Agency World is a global port agency operating in over 360 ports, specializing in vessel and cargo...	Columbia TI  Discovery Date: 2025-06-05  Columbia Integración delivers IT solutions in cloud, cybersecurity, and infrastructure to drive digital...	Wawasan Dengkil Sdn Bhd  Discovery Date: 2025-05-22  Wawasan Dengkil Sdn Bhd is a Malaysian construction company founded in 2003. It specializes in earth...
ALL RING TECH CO., LTD.  Discovery Date: 2025-05-16  All Ring Tech is a Taiwanese company producing advanced automation equipment for semiconductors, LED...	SIMCO Electronics  Discovery Date: 2025-04-30  SIMCO Electronics is a leading provider of calibration and software solutions for technology companies...	Yozgat City Hospital  Discovery Date: 2025-04-09  Modern hospital in Yozgat offering quality care and innovation. Patient health is protected — their...
National Ticket Company  Discovery Date: 2025-04-06 Estimated Attack Date: 2025-04-04  National Ticket Company — Tickets and wristbands since 1907...		

Grup ransomware BERT telah menargetkan berbagai organisasi di sejumlah negara dengan cakupan sektor yang beragam. Di Amerika Serikat, beberapa korban yang telah teridentifikasi meliputi SIMCO Electronics di sektor elektronik, National Ticket Company di sektor tiket, serta S5 Agency World yang bergerak di bidang layanan maritim. Di Turki, serangan BERT juga berhasil menembus sebuah rumah sakit modern di Yozgat, menimbulkan dampak signifikan di sektor kesehatan. Selain itu, kelompok ini turut menyerang perusahaan di Malaysia dengan fokus pada konstruksi, perusahaan teknologi dan otomasi di Taiwan, serta penyedia solusi TI di Kolombia. Korban di Inggris juga tercatat, termasuk S5 Agency World yang menunjukkan jangkauan internasional dari kelompok ini. Target yang luas dan beragam ini mencerminkan strategi BERT dalam menyerang sektor-sektor kritical dan industri yang sangat bergantung pada ketersediaan data dan layanan digital.

3. Attack vector and Delivery Methods

Menurut tulisan yang dimuat pada laman resmi blog.hunterstrategy.net, Attack vector yang digunakan oleh group ransomware ini ada beberapa, dimulai dari Phishing berperan sebagai metode infeksi utama, memanfaatkan teknik rekayasa sosial untuk memperoleh akses awal ke jaringan. Malicious Downloads melibatkan distribusi payload melalui situs web yang telah dikompromikan atau file unduhan berbahaya. Exploiting Vulnerabilities menargetkan kerentanan perangkat lunak yang belum diperbarui (*unpatched*), khususnya pada layanan yang berjalan di server Linux, untuk mendapatkan kendali sistem. Sementara itu, Malicious Software Updates menggunakan pembaruan perangkat lunak atau keamanan palsu sebagai sarana penyebaran ransomware. Pendekatan multi-vektor ini memungkinkan BERT meningkatkan peluang keberhasilan serangan sekaligus memperluas cakupan target, baik pada lingkungan Windows maupun Linux.



4. Ransomware infection chain

Secara umum, *infection chain* serangan ransomware BERT mengikuti rangkaian tahapan yang terstruktur untuk memastikan infiltrasi, eksekusi, dan dampak maksimal pada sistem target. Tahap pertama dimulai dengan pengiriman *phishing email* yang menjadi vektor infeksi utama. Email ini dirancang menggunakan teknik *social engineering* untuk memicu interaksi dari penerima,

seperti membujuk korban untuk membuka *attachment* atau mengklik tautan tertentu. *Attachment* yang disertakan dapat berupa dokumen berformat Office dengan *malicious macro* tersemat atau *link* yang mengarahkan korban ke situs web yang telah dikompromikan. Kedua metode ini memiliki tujuan yang sama, yaitu men-download file berbahaya ke perangkat korban.



Setelah file tersebut diunduh dan dijalankan, *payload* awal biasanya berupa skrip berformat .ps1 (*PowerShell script*). Skrip ini berisi instruksi berbahaya yang berfungsi untuk melakukan eskalasi hak akses (*privilege escalation*), memodifikasi konfigurasi sistem, serta menonaktifkan atau mematikan layanan *security tools* seperti antivirus, EDR (*Endpoint Detection and Response*), atau firewall. Hal ini dilakukan guna meminimalkan kemungkinan deteksi dan mengamankan jalur eksekusi tahap berikutnya.

Tahap selanjutnya adalah proses *staging* dan pengunduhan komponen inti ransomware dari *command and control server* (C2). Komponen ini bertanggung jawab untuk memulai proses enkripsi pada file korban, menggunakan algoritma enkripsi yang kuat dan biasanya memodifikasi ekstensi file yang telah terenkripsi. Selain itu, ransomware BERT sering kali meninggalkan catatan tebusan (*ransom note*) yang berisi instruksi pembayaran dan ancaman terhadap korban, termasuk kemungkinan kebocoran data jika tebusan tidak dibayar.

Pendekatan yang digunakan BERT bersifat *multi-stage* dan *multi-vector*, memadukan teknik manipulasi manusia (*human-driven attack*) dengan eksekusi

otomatis berbasis skrip untuk memastikan tingkat keberhasilan yang tinggi. Strategi ini membuat serangan tidak hanya efektif pada lingkungan Windows, tetapi juga dapat diperluas ke sistem berbasis Linux, sehingga memperbesar cakupan target dan dampaknya.

5. Preparation for lab

Dalam analisis teknikal ini, digunakan dua sampel file yang terindikasi berperan dalam proses infeksi ransomware BERT. Kedua sampel diperoleh dari situs resmi Any.Run, yang terdiri dari file malware asli serta file enkriptor yang digunakan selama proses enkripsi.

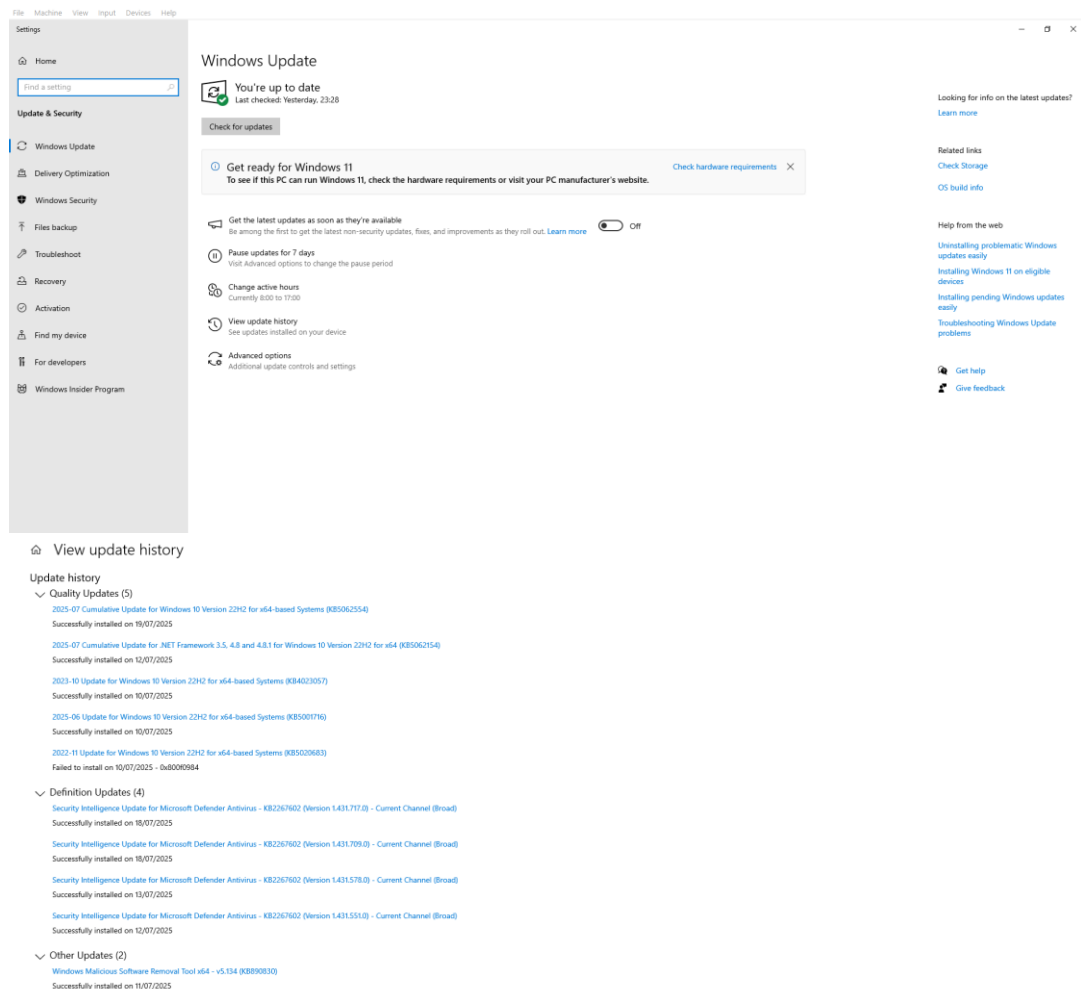
Proses analisis dilakukan secara manual di dalam isolated environment untuk memastikan keamanan sistem utama. Virtualisasi dilakukan menggunakan VirtualBox dengan host operating system Windows 10 versi terbaru, yang diunduh langsung dari situs resmi Microsoft dan telah dipastikan dalam kondisi ter-update, sebagaimana ditampilkan pada gambar di bawah ini.



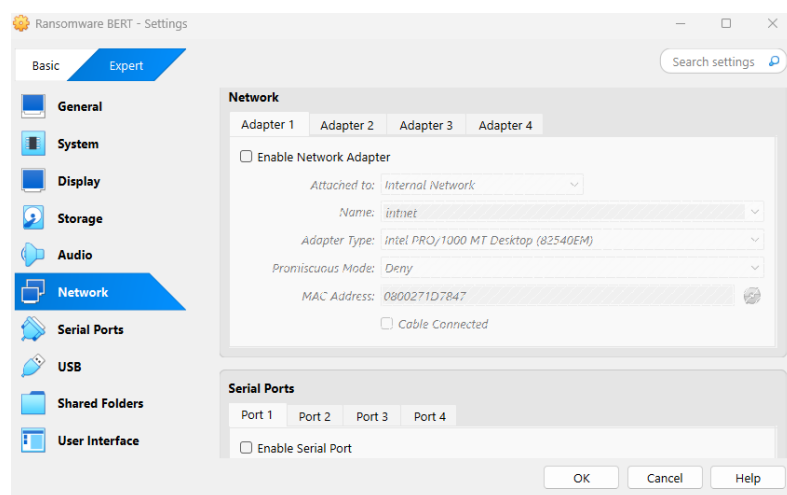
```
CA\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

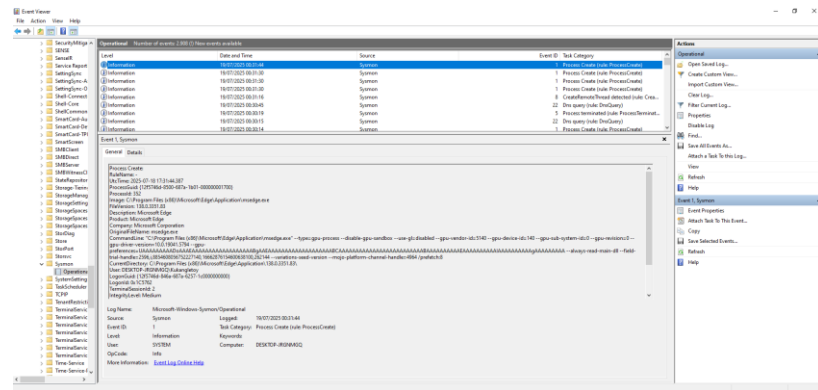
C:\Users\Kukangletoy>ver

Microsoft Windows [Version 10.0.19045.3803]
C:\Users\Kukangletoy>
```

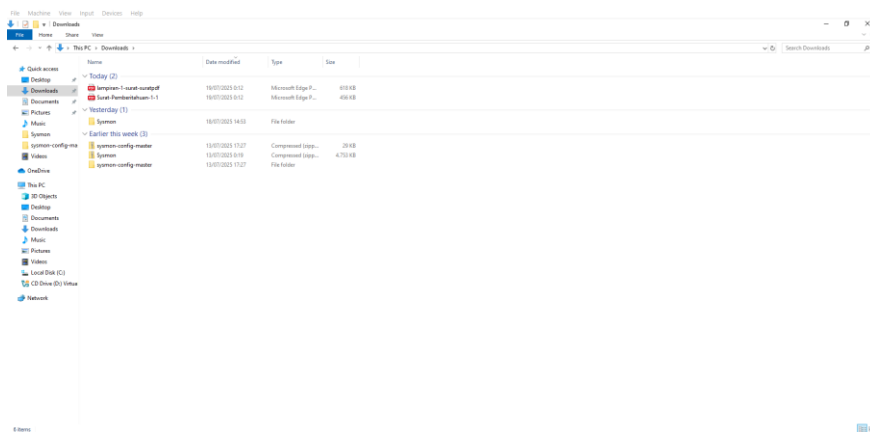
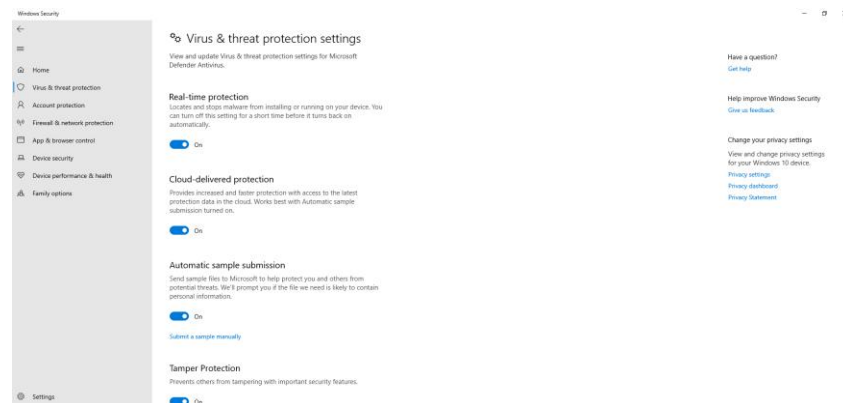


Karena file yang dianalisis merupakan file berbahaya (malicious), seluruh proses dilakukan dalam konfigurasi Internal Network tanpa akses internet untuk mencegah potensi koneksi keluar yang tidak diinginkan. Selain itu, Sysmon telah dipersiapkan untuk memantau dan mencatat aktivitas proses yang berkaitan dengan infeksi ransomware tersebut.





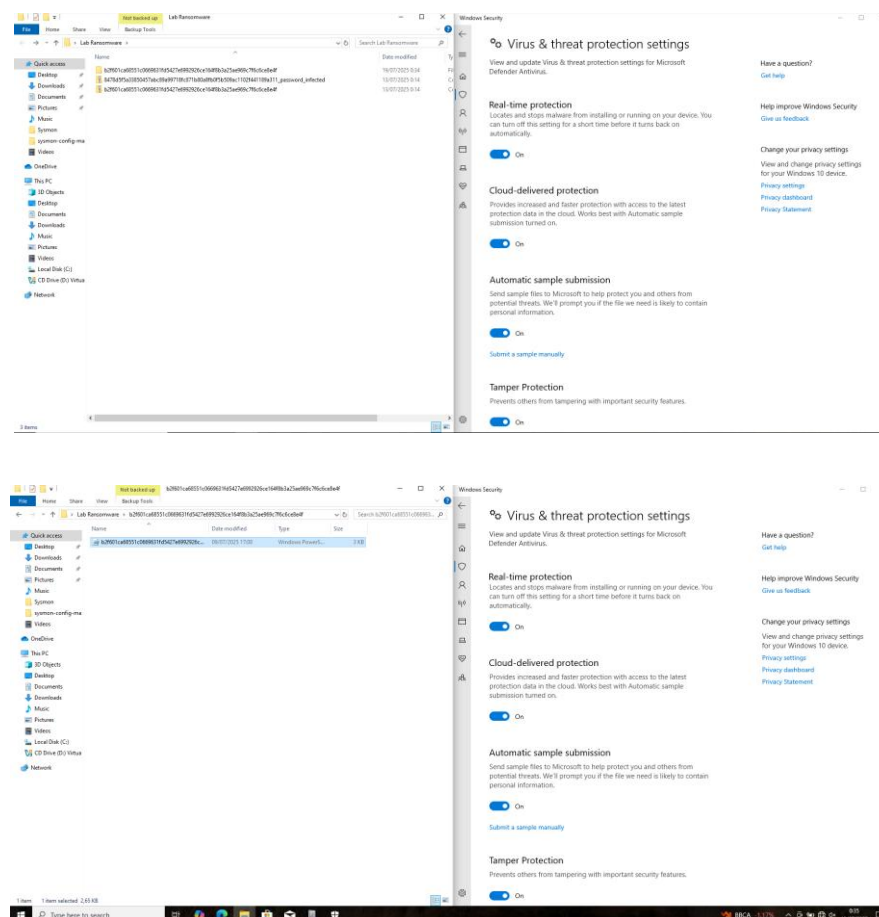
Kami juga memastikan bahwa Windows Defender pada host telah diaktifkan. Dalam skenario ini, kami akan menguji apakah Windows Defender mampu mendeteksi kedua file malicious yang digunakan. Sebagai bagian dari simulasi, kami menyiapkan file PDF dummy di direktori Downloads untuk mengamati perilaku enkriptor saat dijalankan, termasuk apakah file tersebut menjadi target enkripsi.



6. Finding and Analysis

Proses diawali dengan mengunduh dua file *malicious* yang telah dipersiapkan sebelumnya. Pada tahap awal, saat file masih dalam format arsip (.zip), Windows Defender tidak memberikan indikasi deteksi terhadap file berbahaya, sebagaimana ditunjukkan pada gambar di bawah. Ketika file diekstrak, hasilnya tetap sama, tidak terdapat peringatan dari Windows Defender, meskipun di dalam arsip tersebut terdapat file skrip PowerShell (.ps1).

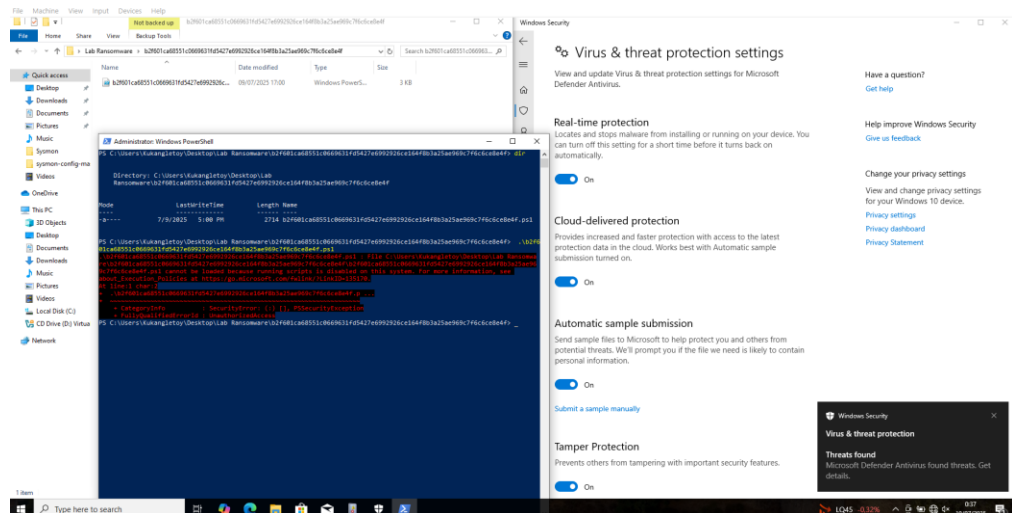
Temuan ini cukup mengejutkan, mengingat file yang dimaksud merupakan file *malicious* yang seharusnya dapat terdeteksi, meskipun belum dijalankan secara aktif.



Selanjutnya, kami menjalankan file PowerShell tersebut menggunakan perintah `.\namafile.ps1` melalui PowerShell dengan privilege akses Administrator. Dari eksekusi ini, kami memperoleh dua temuan utama.

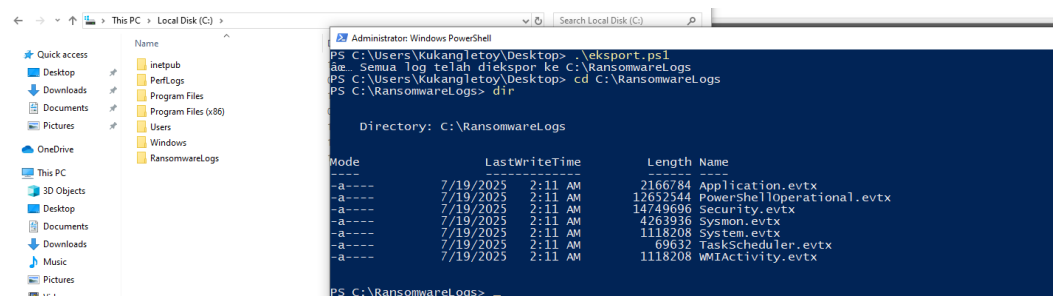
Pertama, saat skrip dijalankan dalam kondisi default di mana Windows Defender dan *Tamper Protection* masih aktif, Windows Defender secara otomatis mendeteksi skrip sebagai ancaman (*threat detection*) dan memblokir prosesnya. Ini menunjukkan bahwa mekanisme proteksi berjalan sebagaimana mestinya.

Kedua, ketika *Tamper Protection* dinonaktifkan, skrip PowerShell berhasil menonaktifkan Windows Defender. Meskipun hasil ini sudah kami perkirakan, tindakan tersebut tetap dilakukan karena kami ingin mengobservasi keseluruhan proses infeksi ransomware secara utuh tanpa intervensi dari proteksi bawaan Windows.



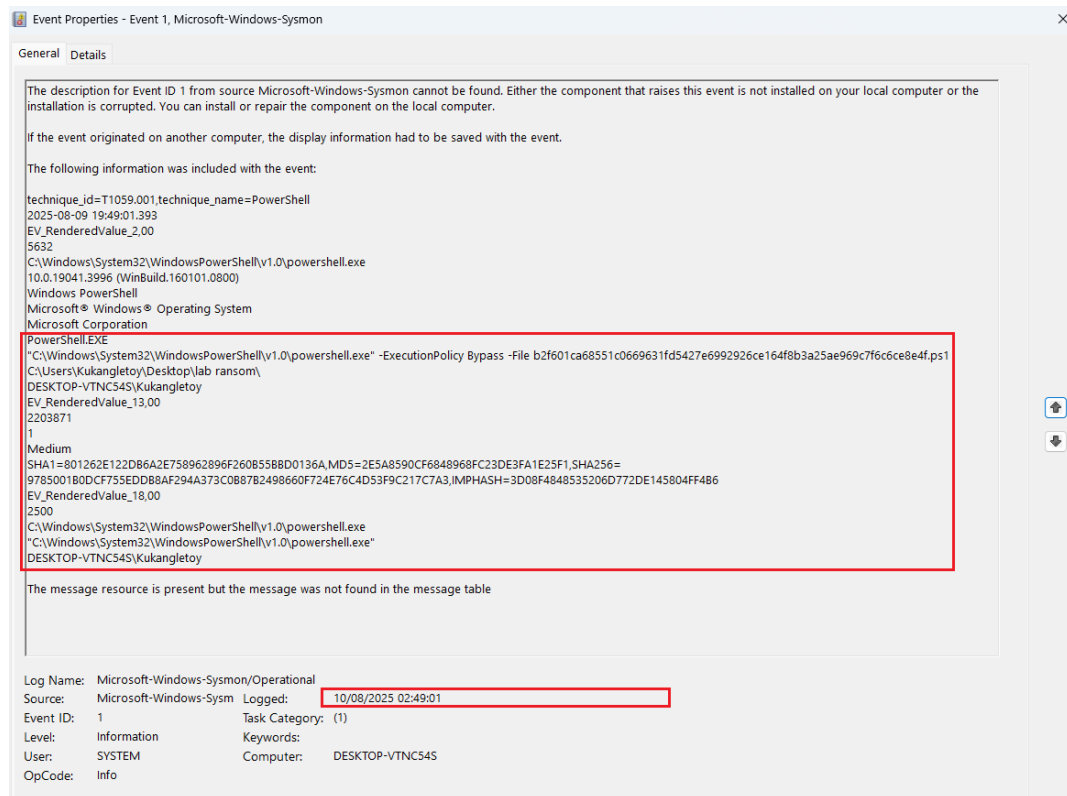
Setelah berhasil mengeksekusi file PowerShell yang merupakan bagian dari ransomware, langkah selanjutnya adalah melakukan identifikasi proses yang berjalan melalui *Windows Event Log*, termasuk log dari Sysmon yang telah kami pasang sebelumnya pada endpoint.

Untuk mendukung proses identifikasi ini, kami memanfaatkan berbagai sumber log, antara lain Sysmon, *PowerShell Operational Log*, dan *Security Log*. Pengumpulan data dilakukan menggunakan skrip berbasis PowerShell yang telah disiapkan sebelumnya, sebagaimana ditunjukkan pada gambar di bawah ini.

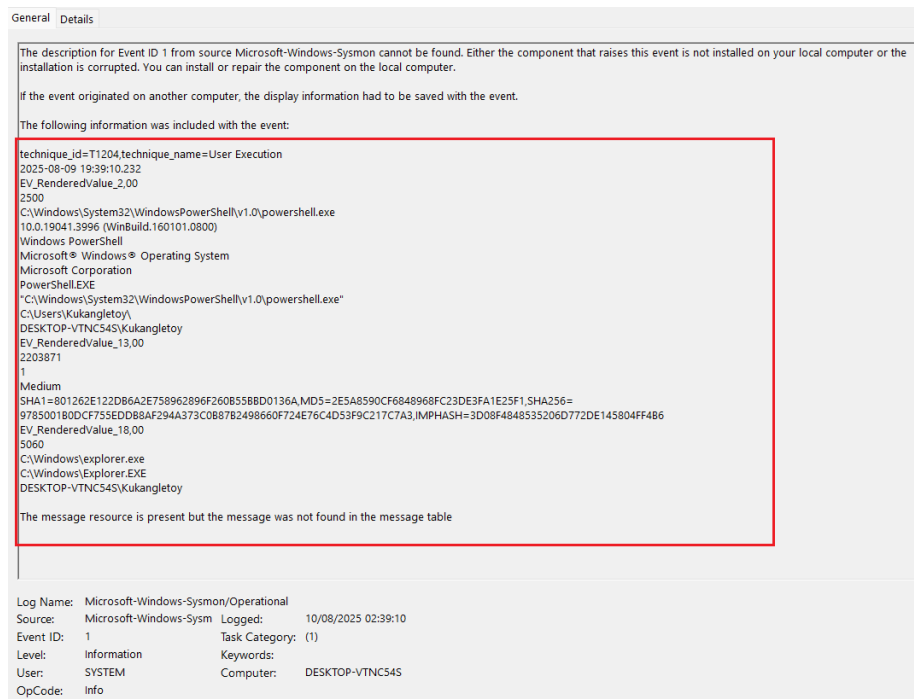


Penelusuran awal dilakukan dengan memanfaatkan log Sysmon yang terpasang pada perangkat terindikasi terinfeksi. Log tersebut menyediakan rekaman aktivitas sistem secara rinci pada Windows Event Log, yang kemudian dianalisis untuk mengidentifikasi peristiwa-peristiwa relevan dalam konteks

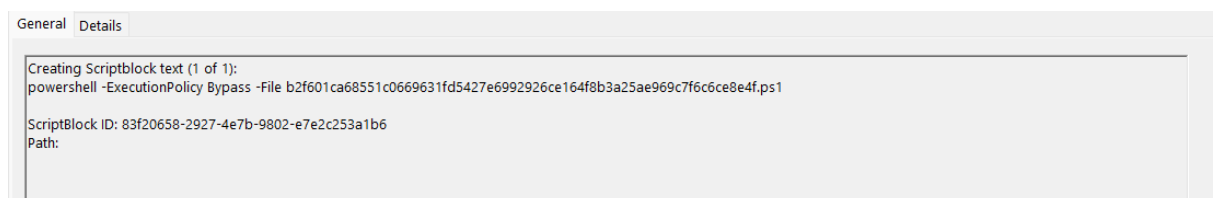
security monitoring dan *threat hunting*. Penelusuran dilakukan dengan menganalisa langsung terhadap log sysmon .evtx melalui event viewer.



Dilihat dari gambar diatas, berhasil diketahui adanya process menjalankan file b2f601ca68551c0669631fd5427e6992926ce164f8b3a25ae969c7f6c6ce8e4f.ps1 (file utama malware bert) pada jam 02:49:01 WIB. Process tersebut terdeteksi berasal dari log Sysmon dengan event id 1 (process creation) dengan eksekui parameter powershell "ExecutionPolicy Bypass". Parameter powershell tersebut digunakan untuk membypass aturan windows yang melarang eksekusi suatu file secara default melalui powershell. Process tersebut juga diketahui memiliki parent process id (PID) yaitu 2500 seperti pada gambar dibawah ini.



Berdasarkan analisis log Sysmon, teridentifikasi proses PowerShell dengan parameter ExecutionPolicy Bypass yang berasal dari proses induk explorer.exe pada pukul 02:39:10 WIB. Eksekusi ini dilakukan oleh pengguna lokal **DESKTOP-JRGNMGQ\Kukangletoy**, yang mengindikasikan bahwa proses PowerShell dibuka secara langsung oleh pengguna tersebut. Mengingat Sysmon tidak mencatat secara rinci konten script .ps1 yang dijalankan, analisis lanjutan dilakukan dengan memanfaatkan PowerShell Operational Log untuk memperoleh detail isi script secara menyeluruh.



Pada waktu yang sama, **PowerShell Operational Log** juga mencatat eksekusi file .ps1 dengan parameter ExecutionPolicy Bypass. Temuan ini mengonfirmasi konsistensi deteksi antara log Sysmon dan log PowerShell, yang sama-sama mengindikasikan adanya eksekusi skrip dengan upaya bypass kebijakan eksekusi pada sistem.

Sesaat menjalankan script diatas, Sysmon juga mendokumentasi adanya pembuatan file sementara pada folder temp dengan nama __PSScriptPolicyTest_x52jmlpq.y3i.ps1. File ini dibuat oleh PowerShell untuk keperluan internal, khususnya saat menjalankan perintah dengan pengaturan kebijakan eksekusi (Execution Policy) tertentu.

```
The description for Event ID 11 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

technique_id=T1059.001,technique_name=PowerShell
2025-08-09 19:49:02.177
EV_RenderedValue_2,00
5632
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Users\Kukangletoy\AppData\Local\Temp\_PSScriptPolicyTest_x52jmlpq.y3i.ps1
2025-08-09 19:49:02.177
DESKTOP-VTNC54S\Kukangletoy

The message resource is present but the message was not found in the message table
```

Temuan serupa juga terdeteksi pada log Sysmon dengan event id 13 (Registry value set) yang mencatat adanya proses yang membuat atau memodifikasi nilai pada registry Windows.

```
The description for Event ID 13 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

technique_id=T1562.001,technique_name=Disable or Modify Tools
SetValue
2025-08-09 19:49:19.013
EV_RenderedValue_3,00
5872
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
DWORD (0x00000001)
DESKTOP-VTNC54S\Kukangletoy

The message resource is present but the message was not found in the message table

The description for Event ID 13 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

technique_id=T1562.001,technique_name=Disable or Modify Tools
SetValue
2025-08-09 19:49:19.016
EV_RenderedValue_3,00
5872
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring
DWORD (0x00000001)
DESKTOP-VTNC54S\Kukangletoy

The message resource is present but the message was not found in the message table
```

The description for Event ID 13 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

technique_id=T1562.001,technique_name=Disable or Modify Tools
SetValue
2025-08-09 19:49:19.016
EV_RenderedValue_3,00
5872
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Cloud Based Protection\DisableCloudProtection
DWORD (0x00000001)
DESKTOP-VTNC54S\Kukangletoy

The message resource is present but the message was not found in the message table

Berdasarkan log Sysmon diatas, terdapat bukti bawah adanya dokumentasi melalui Sysmon event id 13 terhadap Windows Defender. Process tersebut berupa perubahan nilai registry HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware, HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-TimeProtection\DisableRealtimeMonitoring serta HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\CloudBasedProtection\DisableCloudProtection menjadi 1 (DWORD), yang berfungsi menonaktifkan fitur anti-spyware dan Realtime Monitoring melalui proses powershell. Aktivitas ini diketahui terjadi pada waktu 02:49:19 WIB.

The description for Event ID 13 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

technique_id=T1548.002,technique_name=Bypass User Access Control
SetValue
2025-08-09 19:49:29.674
EV_RenderedValue_3,00
5872
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
DWORD (0x00000000)
DESKTOP-VTNC54S\Kukangletoy

The message resource is present but the message was not found in the message table

Selanjutnya pada waktu 02:49:29 juga terdeteksi adanya modifikasi pada registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA. Hal ini bertujuan untuk menonaktifkan UAC (User Account Control), yang biasanya dilakukan untuk melemahkan proteksi keamanan Windows. Temuan ini juga berhubungan dengan script yang dieksekusi diawal tadi.

Selanjutnya untuk aktivitas download yang dilakukan oleh malware tersebut tidak terdokumentasi melalui windows event log. Selain dari script utama yang dijalankan oleh malware tersebut, tidak ada temuan lain yang mendokumentasi process download ke arah ip 185.100.157(.)74. Ip tersebut merupakan ip dari negara swedia dan untuk saat ini ip tersenut sudah di nonaktifkan service httpnya .Namun dikarenakan tidak berhasil mendokumentasi process download

payload.exe tersebut, dilakukanlah download manual namun dengan nama newencryptor.exe. Process download tersebut berasal dari malware bazzar.

File tersebut memiliki ekstensi .exe dan saat dijalankan melalui run as administrator terdapat beberapa windows event yang terdokumentasi pada log Sysmon.

```
The description for Event ID 1 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

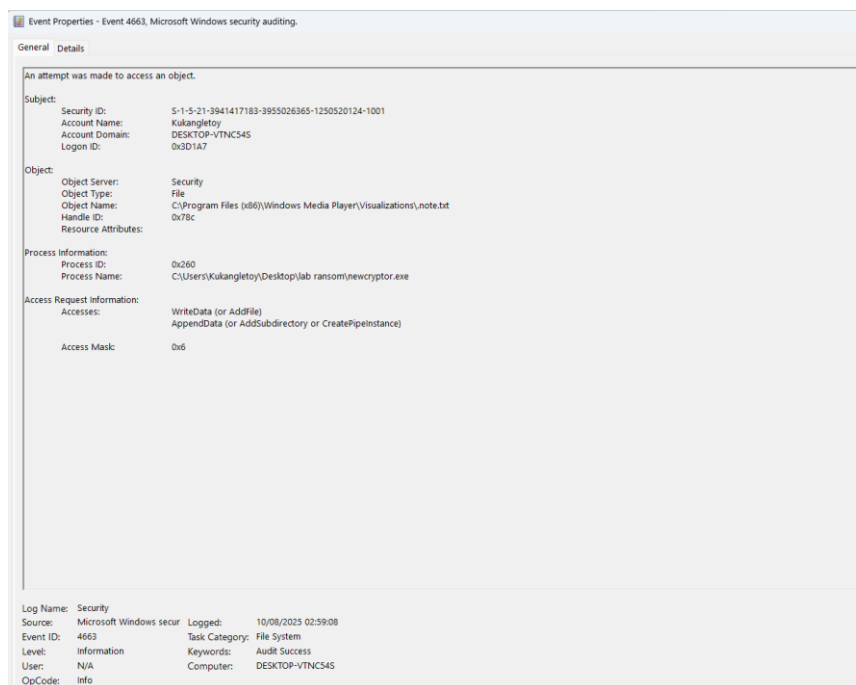
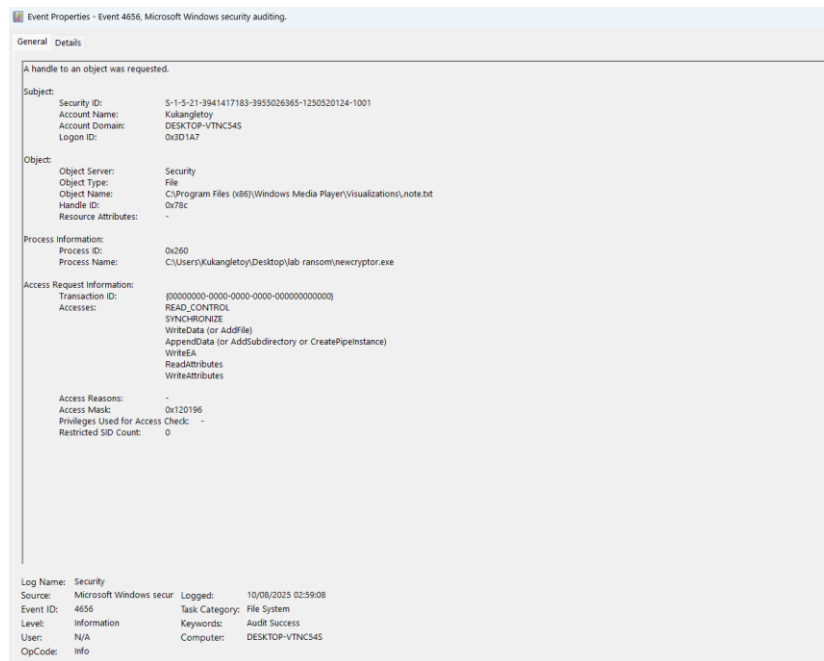
If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

technique_id=T1204,technique_name=User Execution
2025-08-09 19:58:16.573
EV_RenderedValue_2,00
608
C:\Users\Kukangletoy\Desktop\lab ransom\newcryptor.exe
1.0.0.0
newcryptor
newcryptor
-
newcryptor.exe
"C:\Users\Kukangletoy\Desktop\lab ransom\newcryptor.exe"
C:\Users\Kukangletoy\Desktop\lab ransom\
DESKTOP-VTNC54S\Kukangletoy
EV_RenderedValue_13,00
250279
1
High
SHA1=7AA1DE73654F7D6605C81D93F89245A8969D589C,MD5=71DC9540EB03F2ED4D186496813FE839,SHA256=8478D5F5A33850457ABC89A99718FC871B80A8FB0F58509AC1102F441189A311,IMPHASH=
00000000000000000000000000000000
EV_RenderedValue_18,00
4824
C:\Windows\explorer.exe
C:\Windows\Explorer.EXE
DESKTOP-VTNC54S\Kukangletoy

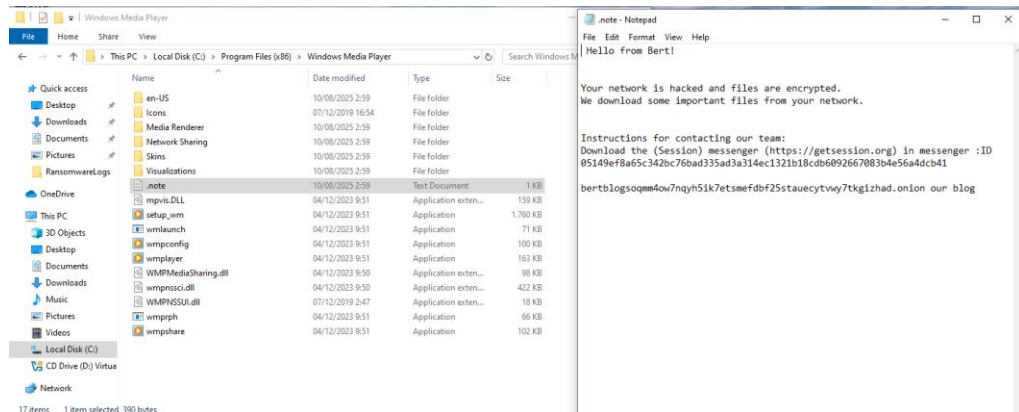
The message resource is present but the message was not found in the message table
```

Diketahui bahwa pada jam 02:58:16 WIB terdapat process menjalankan malicious file lainnya dengan nama newencryptor.exe dengan parent process berasal dari explorer.exe (dijalankan langsung oleh user). Dari process execute tersebut menghasilkan process lain seperti yang terdokumentasi pada log dibawah ini. Dimana newencryptor.exe merupakan suatu file malicious yang bertujuan untuk melakukan enkripsi suatu file. Penelusuran dilanjutkan dengan menemukan adanya aktivitas log perubahan file pada event id 4663 dan 4656 seperti pada gambar dibawah.



Kedua log tersebut menggambarkan aktivitas akses file yang dilakukan oleh proses newcryptor.exe yang dijalankan oleh pengguna Kukangletoy pada file .note.txt di direktori C:\Program Files (x86)\Windows Media Player\Visualizations. Keduanya saling berhubungan sebagai bagian dari rangkaian aktivitas di mana proses newcryptor.exe pertama-tama meminta handle dengan hak akses tertentu untuk membuka file, kemudian melakukan usaha untuk menulis atau memodifikasi isi file tersebut. Hal ini mengindikasikan proses yang berpotensi

melakukan perubahan atau enkripsi terhadap suatu file. File .note.txt tersebut bersikan informasi bahwa device tersebut seudah berhasil di enkripsi sepertiip ada gambar dibawah ini.



Berikut adalah contoh file yang berhasil di enkripsi oleh ransomware bert tersebut. Dimana file file tersebut memiliki ekstensi file dengan nama . Data pdf ini bersifat dummy, sehingga tidak masalah bila terenkripsi.

Name	Date modified	Type	Size
Testing 2.pdf.encryptedbybert	10/08/2025 2:59	ENCRYPTEDBYBE...	16 KB
Testing 1.pdf.encryptedbybert	10/08/2025 2:59	ENCRYPTEDBYBE...	16 KB
percobaan.pdf.encryptedbybert	10/08/2025 2:59	ENCRYPTEDBYBE...	16 KB
halo.pdf.encryptedbybert	10/08/2025 2:59	ENCRYPTEDBYBE...	16 KB
.note	10/08/2025 2:59	Text Document	1 KB

7. Conclusion

Berdasarkan hasil analisis terhadap ransomware BERT, ditemukan bahwa serangan ini memiliki tingkat kompleksitas tinggi dengan memanfaatkan multi-vector attack dan teknik multi-stage execution. Tahapan infeksi diawali dari pengiriman phishing email yang berisi attachment atau tautan berbahaya, diikuti eksekusi skrip PowerShell berformat .ps1 dengan parameter *ExecutionPolicy Bypass* untuk menonaktifkan mekanisme pertahanan Windows, seperti Windows Defender, Firewall, dan UAC, serta melakukan eskalasi hak akses.

Selanjutnya, ransomware mengunduh *payload* tambahan (encryptor) dari server C2 untuk melakukan enkripsi file menggunakan algoritma kuat, disertai catatan tebusan (*ransom note*). Infrastruktur dark web yang dimiliki grup ini, serta

kemampuan lintas platform (Windows dan Linux), menunjukkan tingkat kematangan operasi yang tinggi.

Hasil pengujian di lingkungan *isolated lab* mengonfirmasi bahwa Windows Defender dapat mendeteksi ancaman jika *Tamper Protection* aktif, namun tidak efektif pada file yang disimpan dalam format arsip (.zip). Aktivitas berbahaya terdokumentasi melalui *Sysmon logs*, *PowerShell Operational Logs*, dan *Windows Security Logs*, termasuk modifikasi registry, pematian layanan keamanan, dan proses enkripsi file. Serangan ini terbukti mampu menimbulkan dampak signifikan baik secara operasional maupun finansial bagi organisasi yang menjadi korban.

8. Recommendation

- Aktifkan Tamper Protection dan gunakan EDR/XDR untuk melakukan *continuous monitoring* terhadap aktivitas mencurigakan.
- Implementasi email protection dengan Advanced Threat Protection dan sandboxing.
- Lakukan patch rutin pada Windows & Linux untuk menutup celah eksploitasi.
- Lakukan monitoring dan Batasi terhadap eksekusi melalui powershell
- Terapkan segmentasi jaringan untuk mencegah penyebaran ransomware.
- Adakan pelatihan kesadaran keamanan & simulasi phishing secara berkala.
- Pastikan cadangan data (*backup*) tersimpan secara *offline*, aman, dan lakukan uji pemulihan (*restore test*) secara rutin.

Reference

- <https://unit42.paloaltonetworks.com/category/malware/>
- https://blog.hunterstrategy.net/evolution-of-bert-ransomware/?utm_source=chatgpt.com#20-threat-actors-using-bert
- <https://theravenfile.com/2025/06/16/bert-ransomware/>