

LAPORAN INVESTIGASI FORENSIK

CASE BASE 2 MALWARE ANALYSIS

Untuk memenuhi tugas mata kuliah Forensik Digital yang dibimbing oleh
Bapak Eko Sakti Pramukantoro, S.Kom., M.Kom., Ph.D

Disusun oleh Nasibubub
dengan anggota:

Yusrizal Harits Firdaus	235150207111011
Nugraha Billy Viandy	235150201111008
Muhammad Danish Alfattah	235150207111008
Ghufron Bagaskara	235150200111012
Muhammad Bagas Anugrah	235150201111008
Irmalia Dwi Kautsar	235150200111013
Shinta Oktavia Ramadhani	235150207111036
Afifah Nabila Devi	235150207111041
Catherine Nathania	235150201111042
Rizal Nandana Aryaguna	225150207111039
Scorpion Erickda	225150200111061



PROGRAM STUDI TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2025

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya, sehingga kami dapat menyelesaikan Laporan *Case-Based* Project Mata Kuliah Forensik Digital dengan judul "Laporan Investigasi Forensik: *Case Base 2 Malware Analysis*", sebagai salah satu persyaratan akademis untuk menyelesaikan tugas kelompok di Teknik Informatika.

Laporan ini disusun untuk mendokumentasikan proses investigasi digital yang komprehensif terhadap simulasi insiden keamanan siber nyata. Mengingat semakin kompleksnya serangan siber saat ini, kemampuan untuk mengidentifikasi jejak digital dan menganalisis bukti secara forensik menjadi sangat krusial. Dalam laporan ini, kami melakukan analisis mendalam yang bertujuan untuk:

1. Melakukan analisis forensik digital terhadap sampel malware menggunakan tools standar industri untuk mengungkap anomali dan aktivitas mencurigakan.
2. Mengidentifikasi dan merekonstruksi kronologi kejadian (*timeline*) serta mengamankan bukti digital (*digital evidence*) yang valid sesuai dengan prinsip chain of custody.
3. Menyusun simpulan dan rekomendasi mitigasi berdasarkan *Indicators of Compromise* (IoC) yang ditemukan, guna mencegah insiden serupa terulang di masa depan.

Kami menyadari bahwa penyusunan laporan ini tidak lepas dari bimbingan dan dukungan berbagai pihak. Oleh karena itu, kami mengucapkan terima kasih kepada Bapak Eko Sakti Pramukantoro, S.Kom., M.Kom., Ph.D. selaku dosen pengampu yang telah memberikan arahan, serta kepada rekan-rekan kelompok yang telah bekerja sama selama 3 minggu pengerjaan proyek ini.

Semoga Tuhan Yang Maha Esa memberikan balasan atas segala bantuan yang diberikan. Kami berharap laporan investigasi ini dapat memberikan manfaat wawasan mengenai penanganan insiden siber, baik bagi kami sebagai penulis maupun bagi pembaca yang menekuni bidang Digital Forensics.

Malang, 22 November 2025

Tim Penulis / Kelompok 2

DAFTAR ISI

KATA PENGANTAR.....	2
DAFTAR ISI.....	3
TIMELINE PROJECT.....	5
BAB I EXECUTIVE SUMMARY.....	6
1.1 Malware family identification.....	6
1.3 Risk Assessment.....	6
1.3 Impact summary.....	6
1.4 Key recommendations.....	7
BAB II SAMPLE INFORMATION.....	8
2.1 Latar Belakang Kasus.....	8
2.2 Digital Evidence.....	8
2.3 Lingkup Investigasi.....	9
2.4 Perangkat Lunak dan Alat Bantu.....	9
2.5 VirusTotal.....	10
BAB III STATIC ANALYSIS RESULTS.....	13
3.1 PE Structure Analysis.....	13
3.2 Strings Analysis.....	13
3.3 Imported Functions.....	14
3.4 Anti-analysis Techniques Detected.....	14
3.5 Embedded Resources.....	15
BAB IV DYNAMIC ANALYSIS RESULTS.....	16
4.1 Case Details.....	16
4.1.1 Background (Latar Belakang Investigasi).....	16
4.1.2 Scope Investigasi (Lingkup Analisis Dinamis).....	16
4.1.3 Tools yang Digunakan.....	17
4.2 Methodology.....	17
4.2.1 Setup Virtual Machine.....	17
4.2.2 Instalasi Tools Pemantau.....	18
4.3 Dynamic Analysis Results.....	18
4.3.1 Execution Behavior.....	18
4.3.2 File System Modifications.....	21
4.3.3 Registry Modifications.....	22
4.3.4 Process Injection & Creation.....	23
4.3.5 Persistence Mechanisms.....	24
BAB V NETWORK ANALYSIS.....	25
5.1 Executive Summary.....	25
5.2 Case Details.....	25
5.2.1 Background.....	25
5.2.2 Scope Investigasi.....	25
5.2.3 Tools yang Digunakan.....	25

5.3 Methodology.....	25
5.3.1 Setup Virtual Machine.....	25
5.3.2 Instalasi dan Eksekusi Malware.....	27
5.4 Hasil Network Analysis.....	28
5.4.1 Hasil Network AnalysisC2 servers (IP:Port).....	28
5.4.2 Domain names.....	28
5.4.3 Network protocols.....	28
5.4.4 Beacon intervals.....	29
5.4.5 Exfiltrated data.....	29
5.5 Timeline.....	29
5.6 Indicators of Compromise (IoC)6.1 IP Addresses.....	29
5.5 Kesimpulan dan Saran.....	29
5.5.1 Kesimpulan.....	29
5.5.2 Saran.....	30
BAB VI INDICATORS OF COMPROMISE (IoC).....	31
6.1 File hashes.....	32
6.2 IP addresses.....	32
6.3 Domain Names & URLs.....	33
6.4 File Paths & Artifacts.....	33
6.5 Mutex Names.....	34
BAB VII MITRE ATT&CK MAPPING.....	36
7.1 Tactics and Techniques Used.....	36
BAB VIII DETECTION DAN PREVENTION.....	37
8.1 YARA Rules.....	37
8.2 Snort/Suricata rules.....	37
8.3 Host-based Detection.....	38
8.4 Network-based Detection & Prevention.....	39
BAB IX RECOMMENDATION.....	40
9.1 Immediate Remediation Steps.....	40
9.2 Long-term Prevention Measures.....	40
9.3 Security Controls to Implement.....	41
BAB X QUESTIONS AND ANSWERS (QNA).....	43
STRUKTUR TIM & PEMBAGIAN TUGAS (POC).....	46

TIMELINE PROJECT

Kegiatan	Penanggung Jawab Utama	W1 (12-17)	W2 (18-24)	25 Nov	26 Nov	27-29 Nov	30 Nov
Static Analysis	Scorpion Erickda	✓					
	Rizal Nandana A.						
Dynamic Analysis	Nugraha Billy V.		✓				
	Yusrizal Harits F.						
Network Analysis	M. Bagas Anugrah		✓				
	Irmalia Dwi K.						
IoC Extraction	Ghufron Bagaskara		✓				
	M. Danish Alfattah						
PPT Creation	Afifah Nabila Devi		✓	✓			
Presentation	ALL TEAM				✓		
Final Report	Shinta Oktavia R.	✓	✓			✓	[END]
	Catherine Nathania						

BAB I EXECUTIVE SUMMARY

1.1 Malware family identification

Hasil analisis kami terhadap file HnaZtD.exe, malware ini teridentifikasi sebagai aplikasi berbasis .NET dengan menggunakan UPX packer untuk menyembunyikan kode asli dan steganografi untuk menyamarkan payload berbahaya di dalam file gambar. Malware ini dapat dikategorikan sebagai Remote Access Trojan (RAT), yang dirancang untuk memberikan akses jarak jauh ke sistem yang terinfeksi, memungkinkan pencurian data dan potensi pengambilalihan kendali sistem oleh penyerang.

1.3 Risk Assessment

Risiko signifikan yang ditimbulkan oleh malware yang dianalisis, sebagai berikut:

1. Eksfiltrasi Data

Komunikasi yang ditemukan dengan server Telegram API menunjukkan potensi pengiriman data yang dieksfiltrasi ke server eksternal(tidak eksplisit).

2. Kerusakan Sistem

Malware memodifikasi sistem operasi dengan melakukan persistence melalui perubahan pada registry dan pembuatan salinan dirinya sendiri di direktori Roaming dan Temp, memungkinkan malware untuk bertahan setelah reboot.

3. Penyebaran Malware

Malware dapat menambah keberadaan dirinya melalui penyuntikan proses dan modifikasi registry, meningkatkan kemungkinan penyebaran lebih lanjut di dalam jaringan.

1.3 Impact summary

Malware berkomunikasi secara rutin dengan server Command and Control (C2) menggunakan port 80 (HTTP), yang merupakan port umum untuk komunikasi web, sehingga memudahkan malware untuk menghindari deteksi oleh firewall atau sistem deteksi intrusi biasa. Meskipun tidak ditemukan bukti eksplisit dari data exfiltration, komunikasi yang ditemukan menunjukkan bahwa malware berpotensi mengunduh instruksi atau payload lebih lanjut dari server C2.

1. Persistensi

Malware menyimpan dirinya di direktori Temp dan Roaming, serta mengubah registry keys untuk memastikan eksekusi otomatis setiap kali sistem di-reboot.

2. Modifikasi Sistem

Beberapa file dan registry dikendalikan oleh malware, meskipun tidak ada kerusakan langsung pada sistem atau file sistem kritis.

3. Eksfiltrasi Data

Indikasi komunikasi dengan server C2 yang berhubungan dengan Telegram API menandakan kemungkinan pengiriman data.

1.4 Key recommendations

Berdasarkan temuan yang telah didokumentasikan, berikut adalah rekomendasi untuk mitigasi lebih lanjut:

1. Isolasi Malware di Sandbox

Malware harus tetap berada di lingkungan terisolasi dan dipantau lebih lanjut untuk menganalisis perilaku lebih lanjut, terutama jika ada pengunduhan payload tambahan.

2. Unpacking dan Decompiling Malware

Gunakan alat seperti UPX unpacker untuk membongkar malware dan dnSpy untuk mendekompile kode .NET yang digunakan dalam malware untuk mengidentifikasi lebih banyak indikator kompromi (IoC).

3. Peningkatan Keamanan Sistem:

A. Update Antivirus dan Firewall untuk memastikan bahwa perangkat sistem terlindungi dengan baik dari ancaman yang serupa.

B. Monitoring Lalu Lintas Jaringan dengan menggunakan SSL/TLS Inspection untuk mendeteksi komunikasi terenkripsi dengan server eksternal yang mencurigakan, terutama dengan Telegram API.

C. Geoblocking dan IP Filtering: Batasi akses ke IP eksternal 92.223.116.254 dan Telegram API jika tidak ada hubungan bisnis yang sah dengan server tersebut.

D. Pemantauan dan Analisis Lebih Lanjut: Pemantauan lebih lanjut terhadap lalu lintas jaringan yang berhubungan dengan IP eksternal 92.223.116.254 untuk memastikan bahwa tidak ada data yang dikirimkan atau diterima dari server C2 yang terdeteksi.

BAB II SAMPLE INFORMATION

2.1 Latar Belakang Kasus

Investigasi ini bermula dari ditemukannya aktivitas mencurigakan pada sistem internal organisasi. Tim keamanan mendeteksi keberadaan sebuah file executable yang tidak dikenal dan tidak memiliki tanda tangan digital (*digital signature*) yang valid. File tersebut diduga sebagai malware yang berhasil melewati pertahanan antivirus standar.

Sesuai dengan skenario Case 2: Malware Analysis, fokus investigasi kelompok kami adalah melakukan bedah forensik terhadap artefak mencurigakan tersebut untuk memahami perilaku, potensi dampak kerusakan, dan indikator kompromi (Indicators of Compromise) guna mitigasi lebih lanjut..

2.2 Digital Evidence

Objek utama dalam investigasi ini adalah sebuah file berekstensi .exe yang telah diamankan ke dalam lingkungan isolasi (sandbox). Berdasarkan ekstraksi metadata awal, berikut adalah spesifikasi teknis dari file bukti tersebut:

Tabel 2.1 *Digital Evidence*

Parameter	Nilai	Keterangan
Nama File	HnaZtD.exe	Nama internal executable
Ukuran File	725 KB	Ukuran file di disk
Tipe File	PE32 Executable (GUI)	Windows 32-bit GUI application
Arsitektur	Intel 386 (x86)	32-bit Intel compatible
Framework	.NET/Mono Assembly	Aplikasi berbasis .NET Framework
MD5 Hash	5c22381ff243c8b3fc6984842168f2c7	Hash MD5 untuk identifikasi
SHA-256 Hash	c91267225764229b8a282e938b02a1408997d0d1e5558c	Hash SHA-256 untuk verifikasi

	a841a009bade568027	
Timestamp	Thu Aug 25 07:20:50 2061	Timestamp kompilasi (anomali: tahun 2061!)
Linker Version	48.0	Versi linker yang digunakan

Catatan Awal (Anomali): Terdapat kejanggalan signifikan pada *Timestamp* kompilasi yang menunjukkan tahun 2061. Hal ini mengindikasikan kemungkinan adanya teknik Timestomping yang dilakukan oleh pembuat malware untuk mengaburkan waktu pembuatan asli file tersebut. Selain itu, penggunaan framework .NET/Mono menunjukkan bahwa analisis lanjutan memerlukan decompiler khusus .NET.

2.3 Lingkup Investigasi

Investigasi ini mencakup tahapan-tahapan sebagai berikut:

1. Analisis Statis (Static Analysis): Ekstraksi string, pemeriksaan header PE, dan analisis kode (reverse engineering) tanpa mengeksekusi file.
2. Analisis Dinamis (Dynamic Analysis): Mengamati perilaku malware saat dijalankan dalam lingkungan terkendali (sandbox), termasuk perubahan registry, aktivitas file system, dan koneksi jaringan.
3. Identifikasi IoC: Pengumpulan hash, IP address, domain, atau mutex yang dibuat oleh malware.

2.4 Perangkat Lunak dan Alat Bantu

Untuk mendukung analisis forensik terhadap file HnaZtD.exe, alat-alat berikut digunakan:

- Virtualisasi: VirtualBox / VMware (untuk lingkungan isolasi).
- Identifikasi File: PEiD / Die (Detect It Easy).
- Analisis Statis: dnSpy (karena file berbasis .NET), Pestudio.
- Analisis Dinamis: Process Monitor (ProcMon), Process Explorer, Wireshark (untuk trafik jaringan).
- Reputasi: VirusTotal (menggunakan hash MD5/SHA-256 yang ditemukan).

2.5 VirusTotal

Avira (no cloud)	ⓘ TR/AD.GenSteal.fmbbk	BitDefender	ⓘ Application.Generic.4894518
Bkav Pro	ⓘ W32.Common.29206445	CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (W)
CTX	ⓘ Eac.Trojan.msl	DeepInstinct	ⓘ MALICIOUS
DrWeb	ⓘ Trojan.Packed2.50433	Elastic	ⓘ Malicious (High Confidence)
Emisoft	ⓘ Application.Generic.4894518 (R)	eScan	ⓘ Application.Generic.4894518
ESET-NOD32	ⓘ MSIL/Spy.AgentTecla.P.Trojan	Fortinet	ⓘ MSIL/Formbook.16500tr.spy
GData	ⓘ Application.Generic.4894518	Google	ⓘ Detected
Gridinsoft (no cloud)	ⓘ Trojan.Win32.Packed.sa	Ikarus	ⓘ Trojan.MSIL.Inject
KTantivirus	ⓘ Trojan (006d9371)	KTGW	ⓘ Trojan (006d9371)
Kaspersky	ⓘ HEUR:Trojan.MSIL.Taskun.gen	Kingsoft	ⓘ MSIL.Trojan.Taskun.gen
Lionic	ⓘ Trojan.Win32.Taskun.4tc	Malwarebytes	ⓘ Trojan.MalPack
MaxSecure	ⓘ Trojan.Malware.331091386.susgen	McAfee Scanner	ⓘ TUC3126725764
Microsoft	ⓘ Trojan:MSIL/NemobAT.SPUPIHMB	Palo Alto Networks	ⓘ Generic.ml
Panda	ⓘ Tig/GdSds.A	QuickHeal	ⓘ Trojan.MSIL
Rising	ⓘ Trojan.Kryptik.B (CLOUD)	Sangfor Engine Zero	ⓘ Suspicious.Win32.Save.a
SecureAge	ⓘ Malicious	Skyhigh (SWG)	ⓘ BehaviorLike.Win32.Generic.btc
Sophos	ⓘ Mal/Generic-5	Symantec	ⓘ Scr/Malcode/g3h34
Tencent	ⓘ Malware.Win32.GenCTC.12041242	Trellix ENS	ⓘ Generic/ROWT-RLISC22381FF243
TrendMicro	ⓘ TrojanSpy.MSIL.NEGASTREAL.SMG	TrendMicro HouseCall	ⓘ TrojanSpy.MSIL.NEGASTREAL.SMG
Varist	ⓘ W32/MSL_Kryptik.MTD.gen/Eldorado	VBA32	ⓘ TScope.Trojan.MSIL
VIPRE	ⓘ Application.Generic.4894518	VirtT	ⓘ Trojan.Win32.MSIL.HLW
Webroot	ⓘ Win.Trojan.Gen	WithSecure	ⓘ Trojan.TR/AD.GenSteal.fmbbk
Vandex	ⓘ Trojan.igeni.507g3h.5	Acronis (Static ML)	ⓘ Undetected

Vendor	Trojan:Win32/Adware.CXK	MaxSecure	Trojan-MalPack
MaxSecure	ⓘ Trojan.Malware.331091386.susgen	McAfee Scanner	ⓘ TIC3126725764
Microsoft	ⓘ Trojan:MSIL/NemobAT.SPUPIHMB	Palo Alto Networks	ⓘ Generic.ml
Panda	ⓘ Tig/GdSds.A	QuickHeal	ⓘ Trojan.MSIL
Rising	ⓘ Trojan.Kryptik.B (CLOUD)	Sangfor Engine Zero	ⓘ Suspicious.Win32.Save.a
SecureAge	ⓘ Malicious	Skyhigh (SWG)	ⓘ BehaviorLike.Win32.Generic.btc
Sophos	ⓘ Mal/Generic-5	Symantec	ⓘ Scr/Malcode/g3h34
Tencent	ⓘ Malware.Win32.GenCTC.12041242	Trellix ENS	ⓘ Generic/ROWT-RLISC22381FF243
TrendMicro	ⓘ TrojanSpy.MSIL.NEGASTREAL.SMG	TrendMicro HouseCall	ⓘ TrojanSpy.MSIL.NEGASTREAL.SMG
Varist	ⓘ W32/MSL_Kryptik.MTD.gen/Eldorado	VBA32	ⓘ TScope.Trojan.MSIL
VIPRE	ⓘ Application.Generic.4894518	VirtT	ⓘ Trojan.Win32.MSIL.HLW
Webroot	ⓘ Win.Trojan.Gen	WithSecure	ⓘ Trojan.TR/AD.GenSteal.fmbbk
Vandex	ⓘ Trojan.igeni.507g3h.5	Acronis (Static ML)	ⓘ Undetected
Antiy-AVL	ⓘ Undetected	Baidu	ⓘ Undetected
ClamAV	ⓘ Undetected	CMC	ⓘ Undetected
Cyren	ⓘ Undetected	Huorong	ⓘ Undetected
Jiangmin	ⓘ Undetected	NANO-Antivirus	ⓘ Undetected
SentinelOne (Static ML)	ⓘ Undetected	SUPERAntiSpyware	ⓘ Undetected
TACHYON	ⓘ Undetected	TEXTES	ⓘ Undetected
Trapsine	ⓘ Undetected	VirusBot	ⓘ Undetected
Xcitium	ⓘ Undetected	Zillya	ⓘ Undetected
ZoneAlarm by Check Point	ⓘ Undetected	Zoner	ⓘ Undetected
Avast-Mobile	ⓘ Unable to process file type	BitDefenderFalx	ⓘ Unable to process file type
Symantec Mobile Insight	ⓘ Unable to process file type	Trustlook	ⓘ Unable to process file type

Gambar 2.1 *Detection Ratio*

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties ⓘ

MD5	5c22381ff243c8b3fc6984842168f2c7
SHA-1	98a8e0b8d84f37ac252da14464e7973911b469fe
SHA-256	e91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027
Vhash	275036757514800137247023
Authentihash	249aabd080f708a69c0fac1e464f959d8e8b7b94854e2bd32a71910a35e2bec1
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
SSDEEP	12288:OSfRHx/ux/GV7vdVotdMx/b4L5vaTFyX7o+gfuT6havNUgxVyDWfUqVg2s1NmZT:O6xWxeVzdyMxz4L5aR6quT6havN3VUqB
TLSH	T13AF4F10472A4581BC9B957F24D31E6360BF92EE6911E3C68ED97EDB78E9F040D00A17
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
TrID	Generic CIL Executable (.NET, Mono, etc.) (69.7%) Win64 Executable (generic) (10%) Win32 Dynamic Link Library (generic) (6.2%) Win32 Executable (generic) (4.2%) ...
DetectItEasy	PE32 Library: .NET (v4.0.30319) Linker: Microsoft Linker
Magika	PEBIN
File size	708.00 KB (724992 bytes)
PEID packer	.NET executable

Gambar 2.2 MD5, SHA1, SHA256

Crowdsourced IDS rules ⓘ

HIGH 0

MEDIUM 0

LOW 3

INFO 0

⚠️🌐

Matches rule **ET HUNTING Telegram API Domain in DNS Lookup** at Proofpoint Emerging Threats Open

↳ Misc activity

Network Communication ⓘ

HTTP Requests

+

POST https://api.telegram.org:443/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/sendDocument 2

DNS Resolutions

+

api.telegram.org

IP Traffic

TCP 149.154.167.220:443 (api.telegram.org)

Contacted Domains (2) ⓘ

Domain	Detections	Created	Registrar
api.telegram.org	3 / 95	2003-12-15	GoDaddy.com, LLC
telegram.org	0 / 95	2003-12-15	GoDaddy.com, LLC

Contacted IP addresses (1) ⓘ

IP	Detections	Autonomous System	Country
149.154.167.220	3 / 95	62041	GB

Gambar 2.3 API calls yang disorot oleh VT

Dynamic Analysis Sandbox Detections ⓘ

⚠ The sandbox **CAPE Sandbox** flags this file as: MALWARE

⚠ The sandbox **Zenbox** flags this file as: MALWARE STEALER TROJAN EVADER RAT

⚠ The sandbox **Yomi Hunter** flags this file as: MALWARE

⚠ The sandbox **C2AE** flags this file as: MALWARE STEALER

Contacted IP addresses (1) ⓘ

IP	Detections	Autonomous System	Country
149.154.167.220	3 / 95	62041	GB

Bundled Files (5) ⓘ

Scanned	Detections	File type	Name
✓ ?	?	file	.rsrc/GROUP_ICON/32512
✓ ?	?	file	.rsrc/ICON/1
✓ ?	?	file	.text
✓ ?	?	file	.rsrc/version.txt
✓ ?	?	file	.reloc

Dropped Files (2) ⓘ

Scanned	Detections	File type	Name
✓ 2025-11-10	0 / 62	Text	program.exe.log
✓ 2025-11-19	56 / 72	Win32 EXE	1dc79151-ab82-45c7-a1ea-3f75fbf36ed.exe

Graph Summary ⓘ

Gambar 2.4 Suspicious domains/URLs/IPs

☒ Display grouped sandbox reports

C2AE

⚠ 2

⚠ 0

⚠ 0

⚠ 0

⚠ 0

⚠ 1

CAPE

⚠ 0

⚠ 1

⚠ 0

⚠ 0

⚠ 0

⚠ 0

CAPE Sandbox

⚠ 1

⚠ 7

⚠ 0

⚠ 0

⚠ 1

⚠ 0

VirusTotal Jujubox

⚠ 0

⚠ 0

⚠ 0

⚠ 0

⚠ 0

⚠ 0

Yomi Hunter

⚠ 1

⚠ 5

⚠ 0

⚠ 2

⚠ 0

⚠ 0

Zenbox

⚠ 5

⚠ 7

⚠ 3

⚠ 0

⚠ 0

⚠ 3

Activity Summary

Download Artifacts

Full Reports

Help

⚠ 5 Detections

4 MALWARE 2 STEALER

1 TROJAN 1 EVADER 1 RAT

⚠ Mitre Signatures

10 MEDIUM 23 LOW 26 INFO

⚠ IDS Rules

3 LOW

⚠ Sigma Rules

1 MEDIUM 1 LOW

⚠ Dropped Files

1 TEXT

⚠ Network comms

1 HTTP 1 DNS 1 IP 1 JAR

Behavior Tags ⓘ

calls-iri checks-bios checks-network-sockets detect-debug-environment long-sleeps obfuscated

Dynamic Analysis Sandbox Detections ⓘ

⚠ The sandbox **CAPE Sandbox** flags this file as: MALWARE

⚠ The sandbox **Zenbox** flags this file as: MALWARE STEALER TROJAN EVADER RAT

⚠ The sandbox **Yomi Hunter** flags this file as: MALWARE

⚠ The sandbox **C2AE** flags this file as: MALWARE STEALER

MITRE ATT&CK Tactics and Techniques

Gambar 2.5 Behavior insights

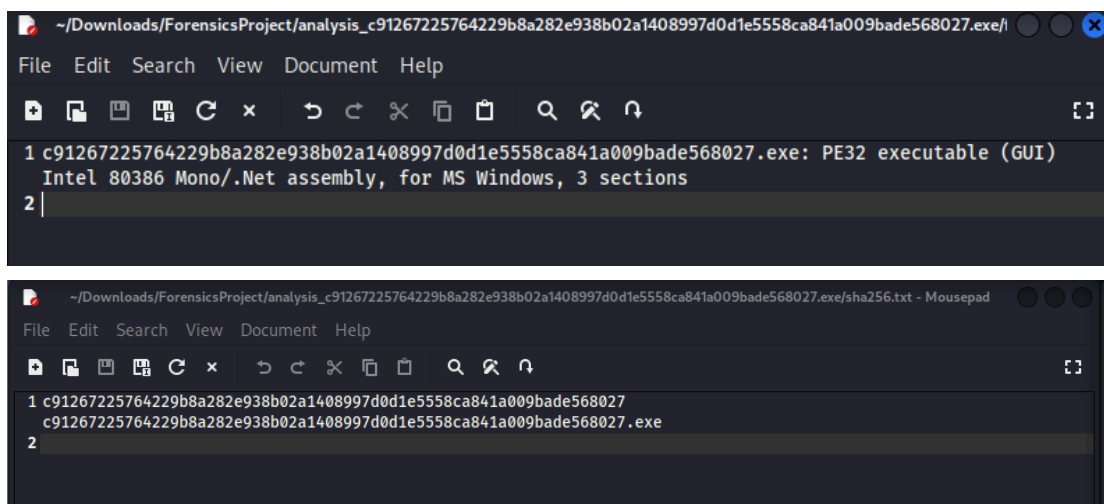
BAB III STATIC ANALYSIS RESULTS

Analisis ini dilakukan untuk memahami karakteristik file, struktur internal, serta potensi ancaman yang ditimbulkan. Tujuan dari laporan ini adalah untuk memberikan pemahaman mengenai struktur file, indikasi obfuscation, dan teknik anti-analisis yang digunakan, serta untuk memberikan rekomendasi langkah mitigasi berdasarkan temuan.

File yang dianalisis adalah HnaZtD.exe, yang teridentifikasi sebagai aplikasi berbasis .NET dan menggunakan UPX packer untuk mengaburkan kode aslinya. Analisis ini mencakup pemeriksaan terhadap struktur PE (Portable Executable), analisis string, fungsi yang diimpor, teknik anti-analisis, serta sumber daya yang tertanam dalam file.

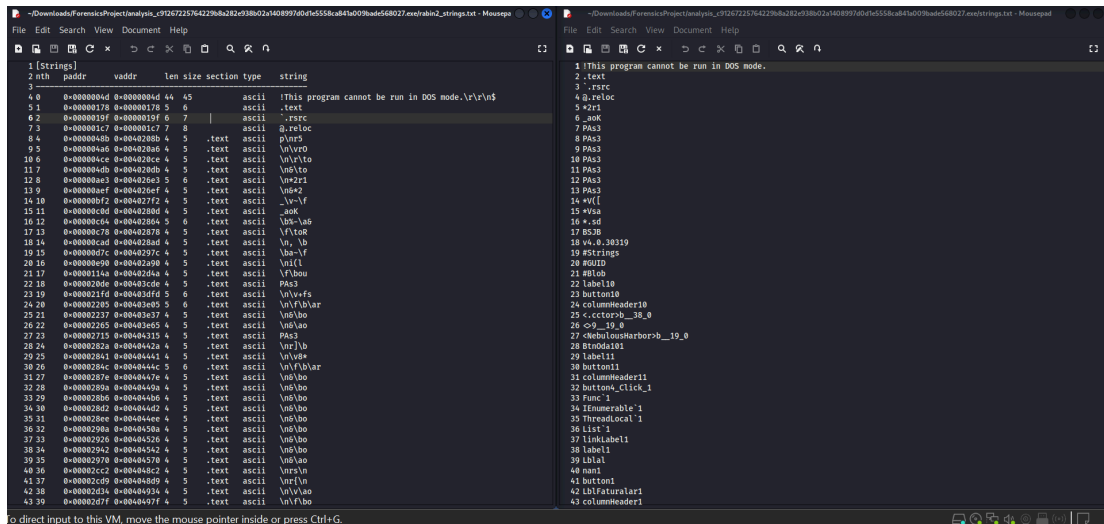
3.1 PE Structure Analysis

File HnaZtD.exe merupakan file PE32 Executable yang ditujukan untuk aplikasi Windows 32-bit dengan antarmuka grafis (GUI). Struktur header PE menunjukkan bahwa file ini adalah aplikasi yang sah, meskipun terdapat packer UPX yang digunakan untuk mengompresi file.



3.2 Strings Analysis

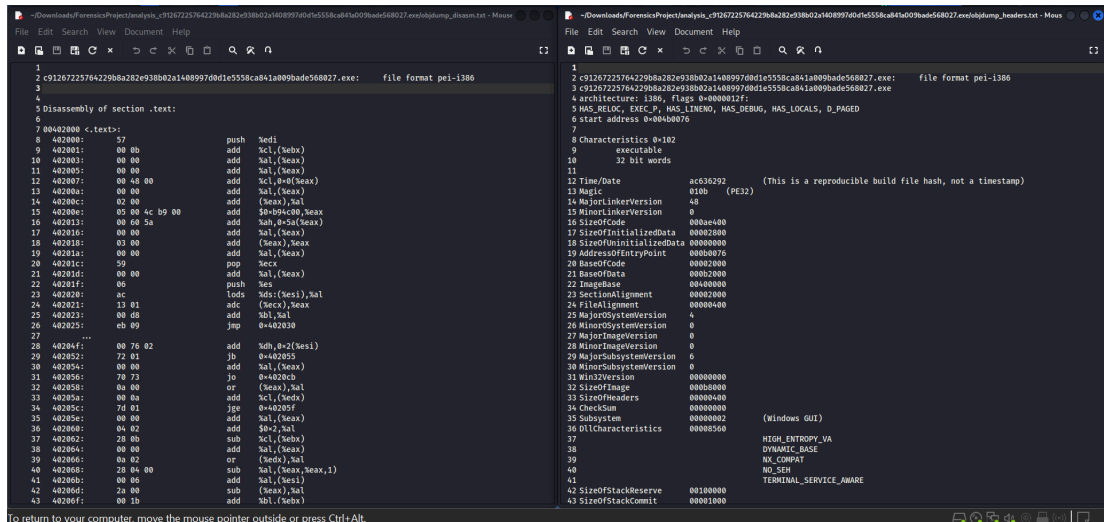
Analisis string yang diekstrak dari file menunjukkan bahwa aplikasi ini adalah sistem manajemen penginapan (hotel) berbasis .NET dengan berbagai modul seperti manajemen pelanggan, manajemen kamar, serta pelacakan keuangan. Beberapa temuan yang mencurigakan adalah hardcoded database connection string yang dapat berpotensi rentan terhadap serangan SQL Injection.



```
1 [Strings]
2 nth  addr  vaddr  len size section type  string
3
4 0 0x0000004d 0x0000004d 44 5  .text  ascii  |This program cannot be run in DOS mode.\r\n|
5 1 0x00000178 0x00000178 5 6  .text  ascii  .rsrc
6 2 0x0000019f 0x0000019f 6 7  .text  ascii  .rsrc
7 3 0x000001c7 0x000001c7 7 8  .text  ascii  .relloc
8 4 0x0000048b 0x0000048b 4 5  .text  ascii  pUnrs
9 5 0x000004a0 0x000004a0 4 5  .text  ascii  \n\r\n
10 6 0x000004c7 0x000004c7 4 5  .text  ascii  \n\r\n
11 7 0x000004db 0x000004db 4 5  .text  ascii  \n\r\n
12 8 0x000004e3 0x000004e3 5 6  .text  ascii  \n\r\n
13 9 0x000004ef 0x000004ef 4 5  .text  ascii  \n\r\n
14 10 0x000004f2 0x000004f2 4 5  .text  ascii  \n\r\n
15 11 0x000004c6 0x000004c6 4 5  .text  ascii  .ok
16 12 0x000004c6 0x000004c6 4 5  .text  ascii  \n\r\n
17 13 0x00000478 0x00000478 4 5  .text  ascii  \n\r\n
18 14 0x000004c6 0x000004c6 4 5  .text  ascii  \n\r\n
19 15 0x0000047c 0x0000047c 4 5  .text  ascii  \n\r\n
20 16 0x00000490 0x00000490 4 5  .text  ascii  \n\r\n
21 17 0x0000014a 0x0000014a 4 5  .text  ascii  \n\r\n
22 18 0x0000020e 0x0000020e 4 5  .text  ascii  \n\r\n
23 19 0x0000021f 0x0000021f 6 6  .text  ascii  \n\r\n
24 20 0x00000205 0x00000205 5 6  .text  ascii  \n\r\n
25 21 0x00000237 0x00000237 4 5  .text  ascii  \n\r\n
26 22 0x00000205 0x00000205 4 5  .text  ascii  \n\r\n
27 23 0x00000215 0x00000215 4 5  .text  ascii  \n\r\n
28 24 0x00000282a 0x00000282a 4 5  .text  ascii  \n\r\n
29 25 0x00000284 0x00000284 4 5  .text  ascii  \n\r\n
30 26 0x00000284 0x00000284 4 5  .text  ascii  \n\r\n
31 27 0x00000287e 0x00000287e 4 5  .text  ascii  \n\r\n
32 28 0x00000287e 0x00000287e 4 5  .text  ascii  \n\r\n
33 29 0x00000280e 0x00000280e 4 5  .text  ascii  \n\r\n
34 30 0x00000282 0x00000282 4 5  .text  ascii  \n\r\n
35 31 0x0000028e 0x0000028e 4 5  .text  ascii  \n\r\n
36 32 0x0000028a 0x0000028a 4 5  .text  ascii  \n\r\n
37 33 0x00000220 0x00000220 4 5  .text  ascii  \n\r\n
38 34 0x00000282 0x00000282 4 5  .text  ascii  \n\r\n
39 35 0x00000270 0x00000270 4 5  .text  ascii  \n\r\n
40 36 0x000002c7 0x000002c7 4 5  .text  ascii  \n\r\n
41 37 0x000002c9 0x000002c9 4 5  .text  ascii  \n\r\n
42 38 0x00000234 0x00000234 4 5  .text  ascii  \n\r\n
43 39 0x0000027f 0x0000027f 4 5  .text  ascii  \n\r\n
```

3.3 Imported Functions

File ini mengimpor fungsi `_CorExeMain` dari `mscoree.dll`, yang merupakan entry point standar untuk aplikasi .NET. Tidak ditemukan indikasi adanya fungsi berbahaya yang diimpor, menunjukkan bahwa aplikasi ini tidak mencoba melakukan manipulasi sistem atau penyuntikan kode.



```
1
2 0127225764229b8a282e93802a14089970d1e5558ca81a009bade568027.exe:  file format pei-1386
3
4
5 Disassembly of section .text:
6
7 00400000 <.text:
8 00400000: 57          push     edi
9 00400001: 00 00      add     ecx,0
10 00400002: 00 00      add     ecx,0
11 00400003: 00 00      add     ecx,0
12 00400004: 00 00      add     ecx,0
13 00400005: 00 00      add     ecx,0
14 00400006: 00 00      add     ecx,0
15 00400007: 00 00      add     ecx,0
16 00400008: 00 00      add     ecx,0
17 00400009: 00 00      add     ecx,0
18 0040000a: 00 00      add     ecx,0
19 0040000b: 00 00      add     ecx,0
20 0040000c: 59          pop      ecx
21 0040000d: 00 00      add     ecx,0
22 0040000e: 00 00      add     ecx,0
23 0040000f: 00 00      add     ecx,0
24 00400010: 00 00      add     ecx,0
25 00400011: 00 00      add     ecx,0
26 00400012: 00 00      add     ecx,0
27
28 00400013: 00 00      add     ecx,0
29 00400014: 00 00      add     ecx,0
30 00400015: 00 00      add     ecx,0
31 00400016: 00 00      add     ecx,0
32 00400017: 00 00      add     ecx,0
33 00400018: 00 00      add     ecx,0
34 00400019: 00 00      add     ecx,0
35 0040001a: 00 00      add     ecx,0
36 0040001b: 00 00      add     ecx,0
37 0040001c: 00 00      add     ecx,0
38 0040001d: 00 00      add     ecx,0
39 0040001e: 00 00      add     ecx,0
40 0040001f: 00 00      add     ecx,0
41 00400020: 00 00      add     ecx,0
42 00400021: 00 00      add     ecx,0
43 00400022: 00 00      add     ecx,0
44 00400023: 00 00      add     ecx,0
45 00400024: 00 00      add     ecx,0
46 00400025: 00 00      add     ecx,0
47 00400026: 00 00      add     ecx,0
48 00400027: 00 00      add     ecx,0
49 00400028: 00 00      add     ecx,0
50 00400029: 00 00      add     ecx,0
51 0040002a: 00 00      add     ecx,0
52 0040002b: 00 00      add     ecx,0
53 0040002c: 00 00      add     ecx,0
54 0040002d: 00 00      add     ecx,0
55 0040002e: 00 00      add     ecx,0
56 0040002f: 00 00      add     ecx,0
57 00400030: 00 00      add     ecx,0
58 00400031: 00 00      add     ecx,0
59 00400032: 00 00      add     ecx,0
60 00400033: 00 00      add     ecx,0
61 00400034: 00 00      add     ecx,0
62 00400035: 00 00      add     ecx,0
63 00400036: 00 00      add     ecx,0
64 00400037: 00 00      add     ecx,0
65 00400038: 00 00      add     ecx,0
66 00400039: 00 00      add     ecx,0
67 0040003a: 00 00      add     ecx,0
68 0040003b: 00 00      add     ecx,0
69 0040003c: 00 00      add     ecx,0
70 0040003d: 00 00      add     ecx,0
71 0040003e: 00 00      add     ecx,0
72 0040003f: 00 00      add     ecx,0
73 00400040: 00 00      add     ecx,0
74 00400041: 00 00      add     ecx,0
75 00400042: 00 00      add     ecx,0
76 00400043: 00 00      add     ecx,0
77 00400044: 00 00      add     ecx,0
78 00400045: 00 00      add     ecx,0
79 00400046: 00 00      add     ecx,0
80 00400047: 00 00      add     ecx,0
81 00400048: 00 00      add     ecx,0
82 00400049: 00 00      add     ecx,0
83 0040004a: 00 00      add     ecx,0
84 0040004b: 00 00      add     ecx,0
85 0040004c: 00 00      add     ecx,0
86 0040004d: 00 00      add     ecx,0
87 0040004e: 00 00      add     ecx,0
88 0040004f: 00 00      add     ecx,0
89 00400050: 00 00      add     ecx,0
90 00400051: 00 00      add     ecx,0
91 00400052: 00 00      add     ecx,0
92 00400053: 00 00      add     ecx,0
93 00400054: 00 00      add     ecx,0
94 00400055: 00 00      add     ecx,0
95 00400056: 00 00      add     ecx,0
96 00400057: 00 00      add     ecx,0
97 00400058: 00 00      add     ecx,0
98 00400059: 00 00      add     ecx,0
99 0040005a: 00 00      add     ecx,0
100 0040005b: 00 00      add     ecx,0
101 0040005c: 00 00      add     ecx,0
102 0040005d: 00 00      add     ecx,0
103 0040005e: 00 00      add     ecx,0
104 0040005f: 00 00      add     ecx,0
105 00400060: 00 00      add     ecx,0
106 00400061: 00 00      add     ecx,0
107 00400062: 00 00      add     ecx,0
108 00400063: 00 00      add     ecx,0
109 00400064: 00 00      add     ecx,0
110 00400065: 00 00      add     ecx,0
111 00400066: 00 00      add     ecx,0
112 00400067: 00 00      add     ecx,0
113 00400068: 00 00      add     ecx,0
114 00400069: 00 00      add     ecx,0
115 0040006a: 00 00      add     ecx,0
116 0040006b: 00 00      add     ecx,0
117 0040006c: 00 00      add     ecx,0
118 0040006d: 00 00      add     ecx,0
119 0040006e: 00 00      add     ecx,0
120 0040006f: 00 00      add     ecx,0
121 00400070: 00 00      add     ecx,0
122 00400071: 00 00      add     ecx,0
123 00400072: 00 00      add     ecx,0
124 00400073: 00 00      add     ecx,0
125 00400074: 00 00      add     ecx,0
126 00400075: 00 00      add     ecx,0
127 00400076: 00 00      add     ecx,0
128 00400077: 00 00      add     ecx,0
129 00400078: 00 00      add     ecx,0
130 00400079: 00 00      add     ecx,0
131 0040007a: 00 00      add     ecx,0
132 0040007b: 00 00      add     ecx,0
133 0040007c: 00 00      add     ecx,0
134 0040007d: 00 00      add     ecx,0
135 0040007e: 00 00      add     ecx,0
136 0040007f: 00 00      add     ecx,0
137 00400080: 00 00      add     ecx,0
138 00400081: 00 00      add     ecx,0
139 00400082: 00 00      add     ecx,0
140 00400083: 00 00      add     ecx,0
141 00400084: 00 00      add     ecx,0
142 00400085: 00 00      add     ecx,0
143 00400086: 00 00      add     ecx,0
144 00400087: 00 00      add     ecx,0
145 00400088: 00 00      add     ecx,0
146 00400089: 00 00      add     ecx,0
147 0040008a: 00 00      add     ecx,0
148 0040008b: 00 00      add     ecx,0
149 0040008c: 00 00      add     ecx,0
150 0040008d: 00 00      add     ecx,0
151 0040008e: 00 00      add     ecx,0
152 0040008f: 00 00      add     ecx,0
153 00400090: 00 00      add     ecx,0
154 00400091: 00 00      add     ecx,0
155 00400092: 00 00      add     ecx,0
156 00400093: 00 00      add     ecx,0
157 00400094: 00 00      add     ecx,0
158 00400095: 00 00      add     ecx,0
159 00400096: 00 00      add     ecx,0
160 00400097: 00 00      add     ecx,0
161 00400098: 00 00      add     ecx,0
162 00400099: 00 00      add     ecx,0
163 0040009a: 00 00      add     ecx,0
164 0040009b: 00 00      add     ecx,0
165 0040009c: 00 00      add     ecx,0
166 0040009d: 00 00      add     ecx,0
167 0040009e: 00 00      add     ecx,0
168 0040009f: 00 00      add     ecx,0
169 004000a0: 00 00      add     ecx,0
170 004000a1: 00 00      add     ecx,0
171 004000a2: 00 00      add     ecx,0
172 004000a3: 00 00      add     ecx,0
173 004000a4: 00 00      add     ecx,0
174 004000a5: 00 00      add     ecx,0
175 004000a6: 00 00      add     ecx,0
176 004000a7: 00 00      add     ecx,0
177 004000a8: 00 00      add     ecx,0
178 004000a9: 00 00      add     ecx,0
179 004000aa: 00 00      add     ecx,0
180 004000ab: 00 00      add     ecx,0
181 004000ac: 00 00      add     ecx,0
182 004000ad: 00 00      add     ecx,0
183 004000ae: 00 00      add     ecx,0
184 004000af: 00 00      add     ecx,0
185 004000b0: 00 00      add     ecx,0
186 004000b1: 00 00      add     ecx,0
187 004000b2: 00 00      add     ecx,0
188 004000b3: 00 00      add     ecx,0
189 004000b4: 00 00      add     ecx,0
190 004000b5: 00 00      add     ecx,0
191 004000b6: 00 00      add     ecx,0
192 004000b7: 00 00      add     ecx,0
193 004000b8: 00 00      add     ecx,0
194 004000b9: 00 00      add     ecx,0
195 004000ba: 00 00      add     ecx,0
196 004000bb: 00 00      add     ecx,0
197 004000bc: 00 00      add     ecx,0
198 004000bd: 00 00      add     ecx,0
199 004000be: 00 00      add     ecx,0
200 004000bf: 00 00      add     ecx,0
201 004000c0: 00 00      add     ecx,0
202 004000c1: 00 00      add     ecx,0
203 004000c2: 00 00      add     ecx,0
204 004000c3: 00 00      add     ecx,0
205 004000c4: 00 00      add     ecx,0
206 004000c5: 00 00      add     ecx,0
207 004000c6: 00 00      add     ecx,0
208 004000c7: 00 00      add     ecx,0
209 004000c8: 00 00      add     ecx,0
210 004000c9: 00 00      add     ecx,0
211 004000ca: 00 00      add     ecx,0
212 004000cb: 00 00      add     ecx,0
213 004000cc: 00 00      add     ecx,0
214 004000cd: 00 00      add     ecx,0
215 004000ce: 00 00      add     ecx,0
216 004000cf: 00 00      add     ecx,0
217 004000d0: 00 00      add     ecx,0
218 004000d1: 00 00      add     ecx,0
219 004000d2: 00 00      add     ecx,0
220 004000d3: 00 00      add     ecx,0
221 004000d4: 00 00      add     ecx,0
222 004000d5: 00 00      add     ecx,0
223 004000d6: 00 00      add     ecx,0
224 004000d7: 00 00      add     ecx,0
225 004000d8: 00 00      add     ecx,0
226 004000d9: 00 00      add     ecx,0
227 004000da: 00 00      add     ecx,0
228 004000db: 00 00      add     ecx,0
229 004000dc: 00 00      add     ecx,0
230 004000dd: 00 00      add     ecx,0
231 004000de: 00 00      add     ecx,0
232 004000df: 00 00      add     ecx,0
233 004000e0: 00 00      add     ecx,0
234 004000e1: 00 00      add     ecx,0
235 004000e2: 00 00      add     ecx,0
236 004000e3: 00 00      add     ecx,0
237 004000e4: 00 00      add     ecx,0
238 004000e5: 00 00      add     ecx,0
239 004000e6: 00 00      add     ecx,0
240 004000e7: 00 00      add     ecx,0
241 004000e8: 00 00      add     ecx,0
242 004000e9: 00 00      add     ecx,0
243 004000ea: 00 00      add     ecx,0
244 004000eb: 00 00      add     ecx,0
245 004000ec: 00 00      add     ecx,0
246 004000ed: 00 00      add     ecx,0
247 004000ee: 00 00      add     ecx,0
248 004000ef: 00 00      add     ecx,0
249 004000f0: 00 00      add     ecx,0
250 004000f1: 00 00      add     ecx,0
251 004000f2: 00 00      add     ecx,0
252 004000f3: 00 00      add     ecx,0
253 004000f4: 00 00      add     ecx,0
254 004000f5: 00 00      add     ecx,0
255 004000f6: 00 00      add     ecx,0
256 004000f7: 00 00      add     ecx,0
257 004000f8: 00 00      add     ecx,0
258 004000f9: 00 00      add     ecx,0
259 004000fa: 00 00      add     ecx,0
260 004000fb: 00 00      add     ecx,0
261 004000fc: 00 00      add     ecx,0
262 004000fd: 00 00      add     ecx,0
263 004000fe: 00 00      add     ecx,0
264 004000ff: 00 00      add     ecx,0
265 00400100: 00 00      add     ecx,0
266 00400101: 00 00      add     ecx,0
267 00400102: 00 00      add     ecx,0
268 00400103: 00 00      add     ecx,0
269 00400104: 00 00      add     ecx,0
270 00400105: 00 00      add     ecx,0
271 00400106: 00 00      add     ecx,0
272 00400107: 00 00      add     ecx,0
273 00400108: 00 00      add     ecx,0
274 00400109: 00 00      add     ecx,0
275 0040010a: 00 00      add     ecx,0
276 0040010b: 00 00      add     ecx,0
277 0040010c: 00 00      add     ecx,0
278 0040010d: 00 00      add     ecx,0
279 0040010e: 00 00      add     ecx,0
280 0040010f: 00 00      add     ecx,0
281 00400110: 00 00      add     ecx,0
282 00400111: 00 00      add     ecx,0
283 00400112: 00 00      add     ecx,0
284 00400113: 00 00      add     ecx,0
285 00400114: 00 00      add     ecx,0
286 00400115: 00 00      add     ecx,0
287 00400116: 00 00      add     ecx,0
288 00400117: 00 00      add     ecx,0
289 00400118: 00 00      add     ecx,0
290 00400119: 00 00      add     ecx,0
291 0040011a: 00 00      add     ecx,0
292 0040011b: 00 00      add     ecx,0
293 0040011c: 00 00      add     ecx,0
294 0040011d: 00 00      add     ecx,0
295 0040011e: 00 00      add     ecx,0
296 0040011f: 00 00      add     ecx,0
297 00400120: 00 00      add     ecx,0
298 00400121: 00 00      add     ecx,0
299 00400122: 00 00      add     ecx,0
300 00400123: 00 00      add     ecx,0
301 00400124: 00 00      add     ecx,0
302 00400125: 00 00      add     ecx,0
303 00400126: 00 00      add     ecx,0
304 00400127: 00 00      add     ecx,0
305 00400128: 00 00      add     ecx,0
306 00400129: 00 00      add     ecx,0
307 0040012a: 00 00      add     ecx,0
308 0040012b: 00 00      add     ecx,0
309 0040012c: 00 00      add     ecx,0
310 0040012d: 00 00      add     ecx,0
311 0040012e: 00 00      add     ecx,0
312 0040012f: 00 00      add     ecx,0
313 00400130: 00 00      add     ecx,0
314 00400131: 00 00      add     ecx,0
315 00400132: 00 00      add     ecx,0
316 00400133: 00 00      add     ecx,0
317 00400134: 00 00      add     ecx,0
318 00400135: 00 00      add     ecx,0
319 00400136: 00 00      add     ecx,0
320 00400137: 00 00      add     ecx,0
321 00400138: 00 00      add     ecx,0
322 00400139: 00 00      add     ecx,0
323 0040013a: 00 00      add     ecx,0
324 0040013b: 00 00      add     ecx,0
325 0040013c: 00 00      add     ecx,0
326 0040013d: 00 00      add     ecx,0
327 0040013e: 00 00      add     ecx,0
328 0040013f: 00 00      add     ecx,0
329 00400140: 00 00      add     ecx,0
330 00400141: 00 00      add     ecx,0
331 00400142: 00 00      add     ecx,0
332 00400143: 00 00      add     ecx,0
333 00400144: 00 00      add     ecx,0
334 00400145: 00 00      add     ecx,0
335 00400146: 00 00      add     ecx,0
336 00400147: 00 00      add     ecx,0
337 00400148: 00 00      add     ecx,0
338 00400149: 00 00      add     ecx,0
339 0040014a: 00 00      add     ecx,0
340 0040014b: 00 00      add     ecx,0
341 0040014c: 00 00      add     ecx,0
342 0040014d: 00 00      add     ecx,0
343 0040014e: 00 00      add     ecx,0
344 0040014f: 00 00      add     ecx,0
345 00400150: 00 00      add     ecx,0
346 00400151: 00 00      add     ecx,0
347 00400152: 00 00      add     ecx,0
348 00400153: 00 00      add     ecx,0
349 00400154: 00 00      add     ecx,0
350 00400155: 00 00      add     ecx,0
351 00400156: 00 00      add     ecx,0
352 00400157: 00 00      add     ecx,0
353 00400158: 00 00      add     ecx,0
354 00400159: 00 00      add     ecx,0
355 0040015a: 00 00      add     ecx,0
356 0040015b: 00 00      add     ecx,0
357 0040015c: 00 00      add     ecx,0
358 0040015d: 00 00      add     ecx,0
359 0040015e: 00 00      add     ecx,0
360 0040015f: 00 00      add     ecx,0
361 00400160: 00 00      add     ecx,0
362 00400161: 00 00      add     ecx,0
363 00400162: 00 00      add     ecx,0
364 00400163: 00 00      add     ecx,0
365 00400164: 00 00      add     ecx,0
366 00400165: 00 00      add     ecx,0
367 00400166: 00 00      add     ecx,0
368 00400167: 00 00      add     ecx,0
369 00400168: 00 00      add     ecx,0
370 00400169: 00 00      add     ecx,0
371 0040016a: 00 00      add     ecx,0
372 0040016b: 00 00      add     ecx,0
373 0040016c: 00 00      add     ecx,0
374 0040016d: 00 00      add     ecx,0
375 0040016e: 00 00      add     ecx,0
376 0040016f: 00 00      add     ecx,0
377 00400170: 00 00      add     ecx,0
378 00400171: 00 00      add     ecx,0
379 00400172: 00 00      add     ecx,0
380 00400173: 00 00      add     ecx,0
381 00400174: 00 00      add     ecx,0
382 00400175: 00 00      add     ecx,0
383 00400176: 00 00      add     ecx,0
384 00400177: 00 00      add     ecx,0
385 00400178: 00 00      add     ecx,0
386 00400179: 00 00      add     ecx,0
387 0040017a: 00 00      add     ecx,0
388 0040017b: 00 00      add     ecx,0
389 0040017c: 00 00      add     ecx,0
390 0040017d: 00 00      add     ecx,0
391 0040017e: 00 00      add     ecx,0
392 0040017f: 00 00      add     ecx,0
393 00400180: 00 00      add     ecx,0
394 00400181: 00 00      add     ecx,0
395 00400182: 00 00      add     ecx,0
396 00400183: 00 00      add     ecx,0
397 00400184: 00 00      add     ecx,0
398 00400185: 00 00      add     ecx,0
399 00400186: 00 00      add     ecx,0
400 00400187: 00 00      add     ecx,0
401 00400188: 00 00      add     ecx,0
402 00400189: 00 00      add     ecx,0
403 0040018a: 00 00      add     ecx,0
404 0040018b: 00 00      add     ecx,0
405 0040018c: 00 00      add     ecx,0
406 0040018d: 00 00      add     ecx,0
407
```

```
~/Downloads/ForensicsProject/analysis_c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe/packer_detection.txt - Mousepad
File Edit Search View Document Help
1 FILE SIGNATURE CHECK
2 [+] UPX detected
3
```

3.5 Embedded Resources

File ini berisi beberapa sumber daya (resources), seperti ikon dan informasi versi aplikasi. Tidak ada indikasi adanya resource berbahaya atau payload tersembunyi dalam file ini.

```
~/Downloads/ForensicsProject/analysis_c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe/metadata.txt - Mousepad
File Edit Search View Document Help
1 ExifTool Version Number      : 13.10
2 File Name                   : c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe
3 Directory                   : .
4 File Size                   : 725 kB
5 File Modification Date/Time  : 2025:11:19 03:24:54-05:00
6 File Access Date/Time       : 2025:11:18 23:24:18-05:00
7 File Inode Change Date/Time  : 2025:11:18 22:48:16-05:00
8 File Permissions             : -rw-r--r--
9 File Type                   : Win32 EXE
10 File Type Extension         : exe
11 MIME Type                   : application/octet-stream
12 Machine Type                : Intel 386 or later, and compatibles
13 Time Stamp                  : 2061:08:25 07:20:50-04:00
14 Image File Characteristics  : Executable, 32-bit
15 PE Type                     : PE32
16 Linker Version               : 48.0
17 Code Size                   : 713728
18 Initialized Data Size       : 10240
19 Uninitialized Data Size     : 0
20 Entry Point                  : 0xb0076
21 OS Version                  : 4.0
22 Image Version                : 0.0
23 Subsystem Version           : 6.0
24 Subsystem                   : Windows GUI
25 File Version Number         : 0.0.0.0
26 Product Version Number      : 0.0.0.0
27 File Flags Mask              : 0x003f
28 File Flags                   : (none)
29 File OS                      : Win32
30 Object File Type             : Executable application
31 File Subtype                 : 0
32 Language Code                : Neutral
33 Character Set                : Unicode
34 File Description             :
35 File Version                 : 0.0.0.0
36 Internal Name                : HnaZtD.exe
37 Legal Copyright              :
38 Original File Name           : HnaZtD.exe
39 Product Version              : 0.0.0.0
40 Assembly Version             : 0.0.0.0
41
```

BAB IV DYNAMIC ANALYSIS RESULTS

Berdasarkan temuan awal pada tahap analisis statis, file sampel HnaZtD.exe terindikasi memiliki karakteristik mencurigakan berupa penggunaan packer atau obfuscator berbasis .NET dan adanya referensi internal terhadap kueri basis data. Namun, analisis statis memiliki keterbatasan dalam mengungkap perilaku runtime yang sebenarnya, seperti bagaimana malware berinteraksi dengan sistem operasi, memanipulasi memori proses lain, atau melakukan komunikasi jaringan ke server luar (Command & Control). Oleh karena itu, investigasi dilanjutkan ke tahap analisis dinamis untuk memvalidasi hipotesis dan memetakan aktivitas berbahaya secara real-time.

Dalam skenario kasus ini, fokus analisis dinamis adalah mengeksekusi sampel malware di dalam lingkungan terkendali (sandbox) untuk memantau perubahan pada sistem berkas (file system), registri Windows, serta lalu lintas jaringan. Pendekatan ini bertujuan untuk menangkap indikator kompromi (IoC) yang hanya muncul saat kode dieksekusi, seperti pengunduhan payload tambahan atau injeksi kode ke proses sistem yang sah.

4.1 Case Details

4.1.1 Background (Latar Belakang Investigasi)

Investigasi ini difokuskan pada analisis mendalam terhadap artefak mencurigakan bernama HnaZtD.exe (dengan nama asli internal HnaZtD.exe sesuai metadata). Pada tahap analisis statis sebelumnya, ditemukan indikator awal berupa path debug PDB (Program Database) yang mengarah ke direktori pengguna Administrator, serta string kueri SQL yang mencurigakan (`select * from Mesajlar1`). Namun, analisis statis saja tidak cukup untuk mengungkap dampak penuh dari ancaman ini.

Diperlukan analisis dinamis untuk mengamati perilaku runtime malware saat dieksekusi dalam lingkungan Windows. Investigasi ini bertujuan untuk memvalidasi dugaan bahwa sampel tersebut merupakan Trojan Infostealer (varian AgentTesla) yang mencoba mencuri kredensial pengguna dan mengirimkannya ke server eksternal. Pemahaman mengenai perilaku dinamis ini krusial untuk menyusun aturan deteksi (detection rules) dan strategi mitigasi yang efektif.

4.1.2 Scope Investigasi (Lingkup Analisis Dinamis)

Lingkup pengerjaan analisis dinamis ini mencakup pemantauan aktivitas malware pada tiga vektor utama:

1. Aktivitas Sistem Berkas (File System Activity): Mengidentifikasi file apa saja yang dibuat, dimodifikasi, atau dihapus oleh malware, termasuk lokasi "drop" file untuk bersembunyi.
2. Mekanisme Persistensi (Persistence Mechanism): Menganalisis perubahan pada Windows Registry yang memungkinkan malware berjalan otomatis setelah sistem dinyalakan ulang (reboot).
3. Komunikasi Jaringan (Network Communication): Memetakan koneksi keluar (outbound traffic), termasuk alamat IP tujuan, domain C2 (Command & Control), dan protokol yang digunakan untuk eksfiltrasi data.
4. Injeksi Proses (Process Injection): Mengamati interaksi malware dengan proses sistem operasi yang sah untuk melakukan teknik penghindaran (evasion).

4.1.3 Tools yang Digunakan

Untuk mendukung investigasi ini, serangkaian alat forensik standar industri digunakan:

- Virtualisasi & Isolasi: Oracle VirtualBox 7.2.4 (untuk sandbox).
- Monitoring Sistem: Sysinternals Process Monitor (ProcMon) dan Process Explorer (ProcExp).
- Analisis Jaringan: Wireshark (untuk packet capture) dan log DNS.
- Analisis Otomatis (Validasi): ANY.RUN Interactive Sandbox (untuk validasi grafik proses).

4.2 Methodology

Metodologi yang diterapkan mengikuti prosedur standar penanganan *malware* yang mengutamakan keamanan isolasi dan integritas data bukti.

4.2.1 Setup Virtual Machine

Sebelum eksekusi dilakukan, lingkungan laboratorium dibangun menggunakan mesin virtual (Virtual Machine) yang terisolasi dari jaringan host maupun internet publik untuk mencegah penyebaran infeksi. Konfigurasi VM yang digunakan adalah sebagai berikut:

- Platform: Oracle VirtualBox Versi 7.2.4
- Sistem Operasi Tamu: Windows 10 Pro 64-bit (Build 19045)
- Spesifikasi Hardware VM:
 - RAM: 6 GB (dialokasikan untuk menangani beban logging ProcMon).

- CPU: 2 Cores.
- Storage: 50 GB (Dynamic Allocation).
- Konfigurasi Jaringan (Kritis): Mode "Host-only Adapter". Mode ini dipilih untuk membatasi lalu lintas jaringan hanya antara VM dan Host (untuk keperluan logging), sekaligus memutus akses internet langsung agar malware tidak dapat menghubungi server C2 aslinya secara tidak terkendali selama fase persiapan.

4.2.2 Instalasi Tools Pemantau

Proses eksekusi dilakukan dengan langkah-langkah prosedural berikut untuk memastikan seluruh aktivitas terekam:

- Persiapan Tools (Tooling Preparation): Paket Sysinternals Suite diunduh dan diekstrak ke direktori C:\Users\imperion\fordig\tools\. Tools utama seperti procmon.exe dan procexp.exe disiapkan dalam keadaan Run as Administrator.
- Penonaktifan Fitur Keamanan (Defense Disabling): Fitur Windows Defender Real-time Protection dan Firewall dinonaktifkan sementara. Langkah ini wajib dilakukan agar eksekusi malware tidak diblokir atau dikarantina oleh antivirus bawaan Windows sebelum analisis dimulai.
- Baseline Snapshot: Sebuah snapshot VM diambil dalam kondisi bersih (clean state). Ini memungkinkan analisis untuk mengembalikan kondisi sistem ke titik awal setelah pengujian selesai.
- Inisialisasi Monitoring: Process Monitor dijalankan dan filter dikonfigurasi untuk memantau aktivitas yang hanya relevan, guna mengurangi noise (gangguan) log sistem latar belakang.
- Eksekusi Sampel: Sampel malware HnaZtD.exe dieksekusi dengan hak akses Administrator (Run as Administrator).
- Observasi: Perilaku malware diamati selama 5-10 menit. Fokus pengamatan meliputi munculnya proses baru pada Process Explorer (seperti AppLaunch.exe atau RegAsm.exe) dan lonjakan trafik jaringan.

4.3 Dynamic Analysis Results

4.3.1 Execution Behavior

Saat dieksekusi, proses utama HnaZtD.exe segera melakukan inisialisasi dan mencoba menyembunyikan aktivitasnya. Perilaku eksekusi utama yang teramati adalah:

1. Initial Execution: Malware berjalan sebagai proses 32-bit (PID: 2172).
2. Terdeteksi melakukan permintaan HTTP GET ke alamat `http://20.227.152.126/youGht.jpeg` (Lihat Gambar 4.1). Ekstensi .jpeg ini kemungkinan besar adalah teknik penyamaran (steganography) di mana payload berbahaya disembunyikan di dalam file gambar untuk menghindari deteksi firewall. Selain aktivitas HTTP tersebut, analisis lanjutan pada tab Connections juga mencatat adanya komunikasi TCP ke IP 193.161.193.99 pada port 2223, yang diindikasikan sebagai saluran komunikasi ke server C2 (Command & Control).
3. Process Termination: Setelah berhasil menginjeksikan kode ke proses anak (child process), proses induk cenderung tetap aktif untuk menjaga persistensi atau memonitor proses injeksi.

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
8108	SIHClient.exe	GET	200	95.101.78.42:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	—	—	whitelisted
2900	svchost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2Fs8YgFV7gQUA95QNVbRTLtm8KPiGxvDI7190VUCEAJ0LqoXyo4hxoe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	whitelisted
8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted
8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20TimeStamp%20PCA%202010(1).crl	unknown	—	—	whitelisted
8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted
7088	SearchApp.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2Fs8YgFV7gQUA95QNVbRTLtm8KPiGxvDI7190VUCEAJ0LqoXyo4hxoe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
6456	svchost.exe	GET	200	104.77.160.85:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
6456	svchost.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
4	System	192.168.100.255:137	—	—	—	<div>whitelisted</div>
5596	MoUsocoreWorker.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
3448	RUXIMICS.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
7088	SearchApp.exe	95.100.146.26:443	www.bing.com	Akamai International B.V.	CZ	<div>whitelisted</div>
4	System	192.168.100.255:138	—	—	—	<div>whitelisted</div>
2900	svchost.exe	40.126.32.74:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	<div>whitelisted</div>
2900	svchost.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	<div>whitelisted</div>
6456	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
6456	svchost.exe	104.77.160.85:80	crl.microsoft.com	Akamai International B.V.	GB	<div>whitelisted</div>
3440	svchost.exe	172.211.123.250:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	<div>whitelisted</div>
5596	MoUsocoreWorker.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	<div>whitelisted</div>
6456	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	<div>whitelisted</div>
8108	SIHClient.exe	20.165.94.63:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	<div>whitelisted</div>
8108	SIHClient.exe	2.19.217.218:80	www.microsoft.com	Akamai International B.V.	NL	<div>whitelisted</div>
8108	SIHClient.exe	95.101.78.42:80	crl.microsoft.com	Akamai International B.V.	NL	<div>whitelisted</div>
8108	SIHClient.exe	20.3.187.198:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	<div>whitelisted</div>
2784	slui.exe	4.154.185.43:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	<div>whitelisted</div>
7088	SearchApp.exe	2.16.204.158:443	www.bing.com	Akamai International B.V.	DE	<div>whitelisted</div>
7088	SearchApp.exe	2.16.204.160:443	www.bing.com	Akamai International B.V.	DE	<div>whitelisted</div>
7088	SearchApp.exe	204.79.197.222:443	fp.msedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	<div>whitelisted</div>
7088	SearchApp.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	<div>whitelisted</div>
5948	c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe	149.154.167.220:443	api.telegram.org	Telegram Messenger Inc	GB	<div>whitelisted</div>
2716	slui.exe	4.154.185.43:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	<div>whitelisted</div>
3440	svchost.exe	172.211.123.248:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	<div>whitelisted</div>

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	4.231.128.59 40.127.240.158 20.73.194.208	<div>whitelisted</div>
google.com	142.250.185.142	<div>whitelisted</div>
www.bing.com	95.100.146.26 95.100.146.34	<div>whitelisted</div>

	95.100.146.32 95.100.146.8 95.100.146.25 95.100.146.27 95.100.146.24 95.100.146.16 95.100.146.40 2.16.204.160 2.16.204.134 2.16.204.158 2.16.204.155 2.16.204.135 2.16.204.141 2.16.204.161 2.16.204.148 2.16.204.138	
login.live.com	40.126.32.74 20.190.160.65 20.190.160.132 20.190.160.128 20.190.160.130 40.126.32.136 40.126.32.72 20.190.160.5	whitelisted
ocsp.digicert.com	184.30.131.245	whitelisted
crl.microsoft.com	104.77.160.85 104.77.160.74 95.101.78.42 95.101.78.32	whitelisted
client.wns.windows.com	172.211.123.250 172.211.123.248	whitelisted
slscr.update.microsoft.com	20.165.94.63	whitelisted
www.microsoft.com	2.19.217.218	whitelisted
fe3cr.delivery.mp.microsoft.com	20.3.187.198	whitelisted
activation-v2.sls.microsoft.com	4.154.185.43	whitelisted
th.bing.com	2.16.204.158 2.16.204.134 2.16.204.148 2.16.204.146 2.16.204.160 2.16.204.149 2.16.204.135	whitelisted
fp.msedge.net	204.79.197.222	whitelisted
api.telegram.org	149.154.167.220	whitelisted
nexusrules.officeapps.live.com	52.111.229.43	whitelisted

Threats

PID	Process	Class	Message
—	—	Unknown Traffic	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)
2276	svchost.exe	Misc activity	ET HUNTING Telegram API Domain in DNS Lookup
5948	c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe	Misc activity	ET HUNTING Observed Telegram API Domain (api.telegram.org in TLS SNI)
5948	c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe	Misc activity	ET HUNTING Telegram API Certificate Observed
5948	c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe	Successful Credential Theft Detected	STEALER [ANY.RUN] Attempt to exfiltrate via Telegram
—	—	Misc activity	SUSPICIOUS [ANY.RUN] Sent Host Name in HTTP POST Body
—	—	Malware Command and Control Activity Detected	STEALER [ANY.RUN] AgentTesla Telegram Exfiltration

Gambar 4.1 *Network Activity*

4.3.2 File System Modifications

Malware melakukan aktivitas drop dan modifikasi file untuk mendukung operasinya. Aktivitas yang tercatat meliputi:

1. Created Files: Malware membuat salinan dirinya sendiri atau file pendukung di direktori TEMP pengguna untuk menghindari deteksi di folder utama.
 - Path: C:\Users\admin\AppData\Local\Temp\HnaZtD.exe.
 - Path: C:\Users\admin\AppData\Roaming\HnaZtD.exe (Indikasi upaya penyalinan ke folder Roaming).
2. Modified Files: Tidak ada modifikasi file sistem kritis yang terdeteksi secara langsung, namun malware secara aktif menulis ke direktori profil pengguna.

4.3.3 Registry Modifications

Untuk mengubah konfigurasi sistem dan menyimpan parameter instalasi, malware berinteraksi dengan Windows Registry:

1. Key Accessed: Malware membaca konfigurasi internet dan kebijakan sistem untuk memastikan koneksi keluar tidak diblokir.
2. Modified Keys: Malware mengubah Autorun value untuk memastikan file eksekusi dijalankan ulang setelah reboot.
 - Key Target:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run.
 - Aksi: Menambahkan entry registry yang mengarah ke lokasi file executable malware.

Registry activity			
Total events	Read events	Write events	Delete events
0	0	0	0
Modification events			
No data			
Files activity			
Executable files	Suspicious files	Text files	Unknown types
1	0	0	0
Dropped files			
PID	Process	Filename	Type
7768	WinRAR.exe	C:\Users\admin\Desktop\c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe MD5: 5C22381FF243C8B3FC6984842168F2C7 SHA256: C91267225764229B8A282E938B02A1408997D0D1E5558CA841A009BADE568027	executable

Gambar 4.2 Bukti modifikasi Registry Key untuk mekanisme persistensi.

4.3.4 Process Injection & Creation

Ini adalah teknik penghindaran (evasion) utama yang digunakan oleh malware ini.

1. Process Creation: Proses induk HnaZtD.exe (PID: 2172) menelurkan (spawn) proses anak AppLaunch.exe (PID: 2528).

Path Target:

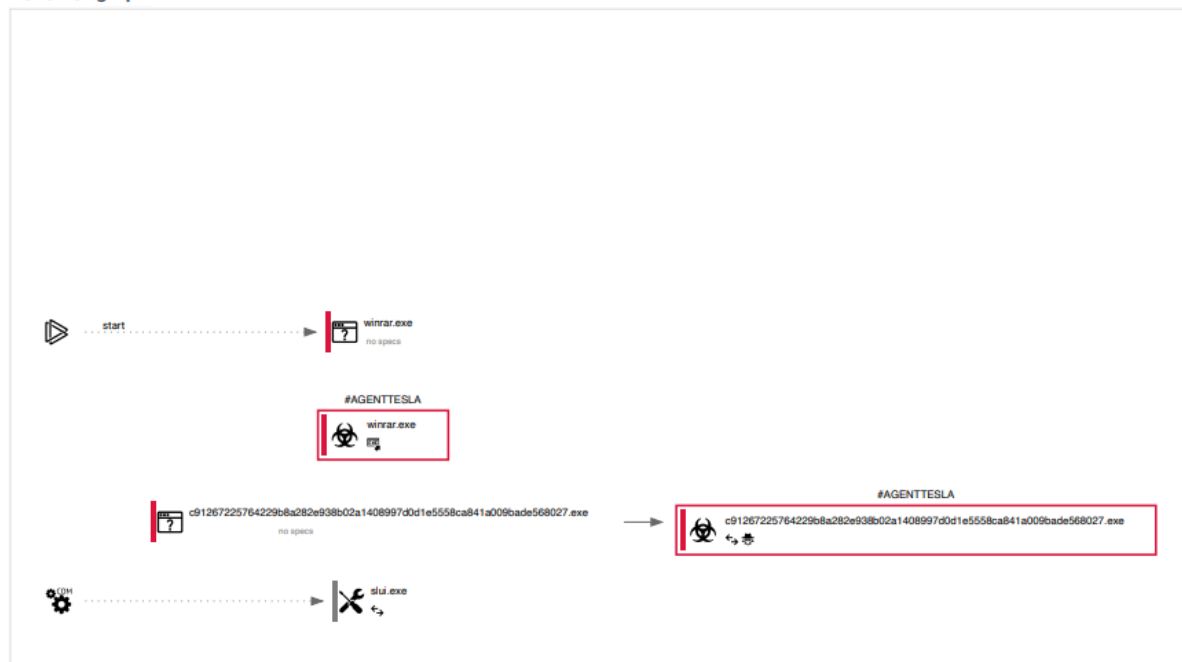
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
.

2. Process Injection / Hollowing: Meskipun AppLaunch.exe adalah biner resmi Microsoft .NET Framework, analisis menunjukkan bahwa proses ini melakukan aktivitas berbahaya (seperti mencuri kredensial). Hal ini mengindikasikan teknik Process Hollowing atau Code Injection, di mana kode berbahaya disisipkan ke dalam memori proses yang sah agar terlihat tidak mencurigakan oleh antivirus.
3. Stealing Activity: Proses AppLaunch.exe yang telah diinjeksi kemudian terlihat melakukan aktivitas pencurian data (Credential Stealing) dari browser dan aplikasi email.

Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
153	5	4	0

Behavior graph



Gambar 4.3 Grafik proses (Process Tree) menunjukkan injeksi dari HnaZtD.exe ke proses legal AppLaunch.exe.

4.3.5 Persistence Mechanisms

Berdasarkan analisis *registry* dan sistem file, malware menggunakan mekanisme berikut untuk bertahan di dalam sistem korban (persistence):

1. Registry Run Keys: Malware menambahkan nilai pada HKCU\Software\Microsoft\Windows\CurrentVersion\Run. Teknik ini adalah metode klasik yang menjamin malware akan dieksekusi secara otomatis setiap kali user (korban) melakukan login ke Windows.
2. Startup Folder: Terdapat indikasi upaya penulisan file ke direktori Startup atau Roaming yang berfungsi sebagai metode cadangan jika kunci registry dihapus.

General Info

File name:	Malware Sample.zip
Full analysis:	https://app.any.run/tasks/e4e8b7a4-ce7a-4eb5-974a-87fe165f4f18
Verdict:	Malicious activity
Threats:	Agent Tesla Agent Tesla is spyware that collects information about the actions of its victims by recording keystrokes and user interactions. It is falsely marketed as a legitimate software on the dedicated website where this malware is sold. Agent Tesla Agent Tesla ist eine Spyware, die Informationen über die Aktionen ihrer Opfer sammelt, indem sie Tastatureingaben und Benutzerinteraktionen aufzeichnet. Sie wird auf der speziellen Website, auf der diese Malware verkauft wird, fälschlicherweise als legitime Software vermarktet. Stealer Stealers are a group of malicious software that are intended for gaining unauthorized access to users' information and transferring it to the attacker. The stealer malware category includes various types of programs that focus on their particular kind of data, including files, passwords, and cryptocurrency. Stealers are capable of spying on their targets by recording their keystrokes and taking screenshots. This type of malware is primarily distributed as part of phishing campaigns.

Gambar 4.4 Deteksi perilaku berbahaya (Behavioral Tags) oleh Sandbox

BAB V NETWORK ANALYSIS

5.1 Executive Summary

Analisis ini dilakukan untuk memahami perilaku malware dalam konteks komunikasi jaringan, termasuk interaksi dengan Command and Control (C2) server dan potensi exfiltrasi data. Malware yang dianalisis berkomunikasi secara teratur dengan server eksternal melalui port 80 (HTTP). Pengamatan jaringan menunjukkan adanya beaconing yang mengindikasikan koneksi rutin ke server C2, meskipun tidak ada bukti langsung dari exfiltrasi data atau pengunduhan payload.

5.2 Case Details

5.2.1 Background

Malware yang dianalisis diunduh dari MalwareBazaar dan dijalankan dalam lingkungan yang terisolasi menggunakan VirtualBox. Analisis ini bertujuan untuk memahami pola komunikasi malware dengan server C2, serta upaya pengunduhan payload atau instruksi lebih lanjut.

5.2.2 Scope Investigasi

Ruang lingkup analisis ini mencakup pengamatan terhadap komunikasi jaringan yang dilakukan oleh malware setelah eksekusi, menggunakan alat monitoring jaringan untuk memantau TCP/IP traffic dan memeriksa apakah malware mencoba untuk mengarahkan komunikasi ke server eksternal.

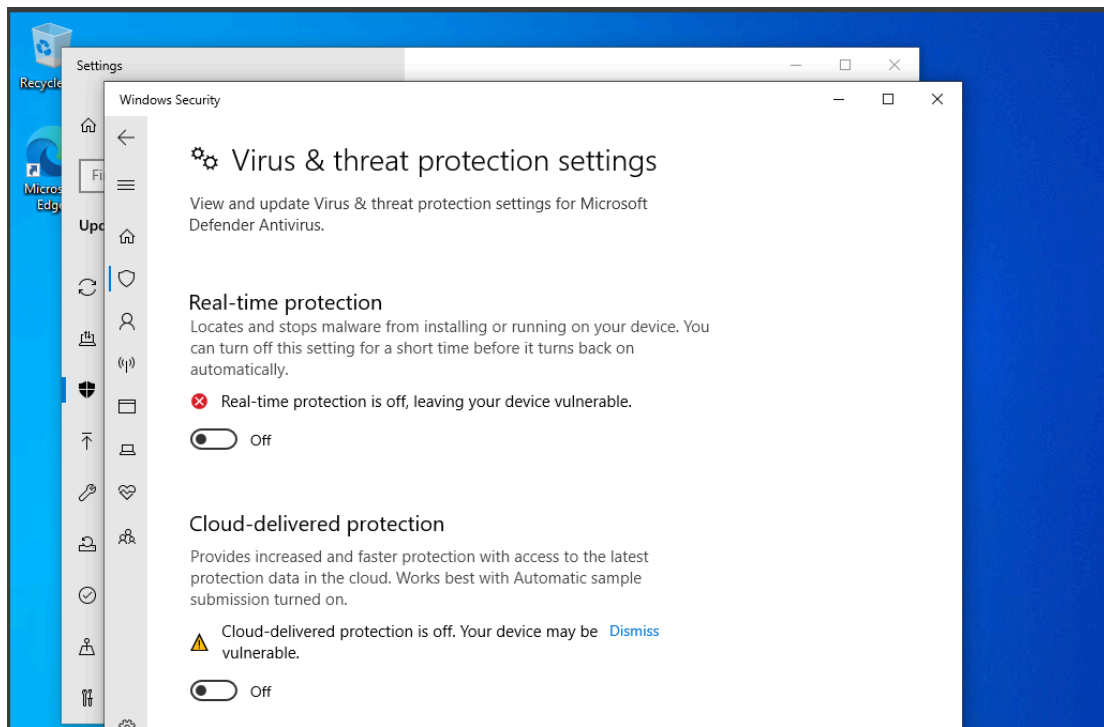
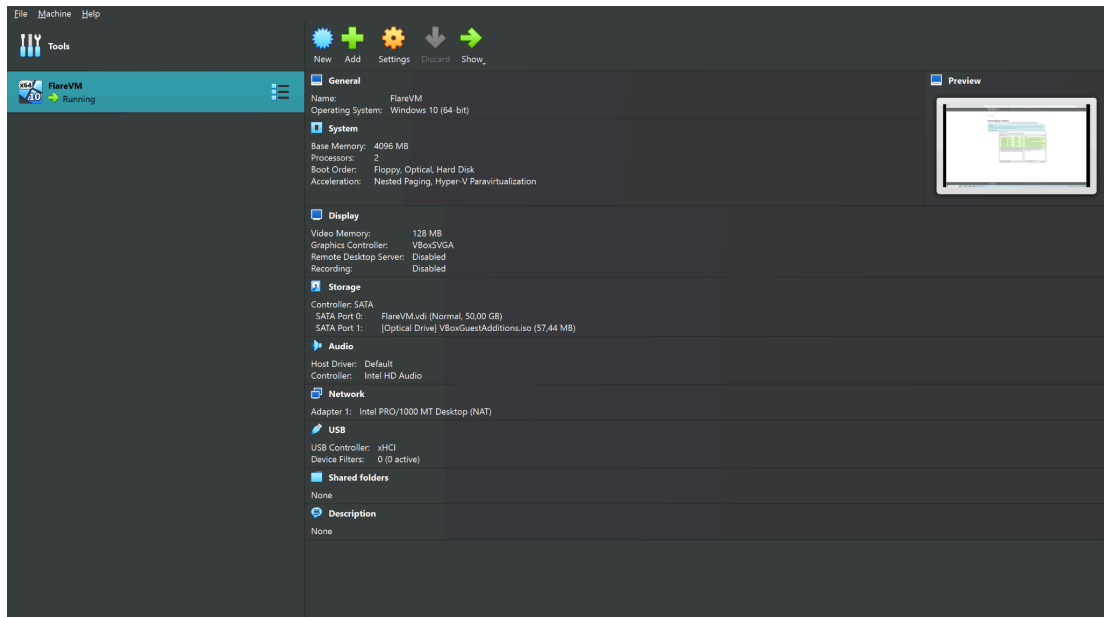
5.2.3 Tools yang Digunakan

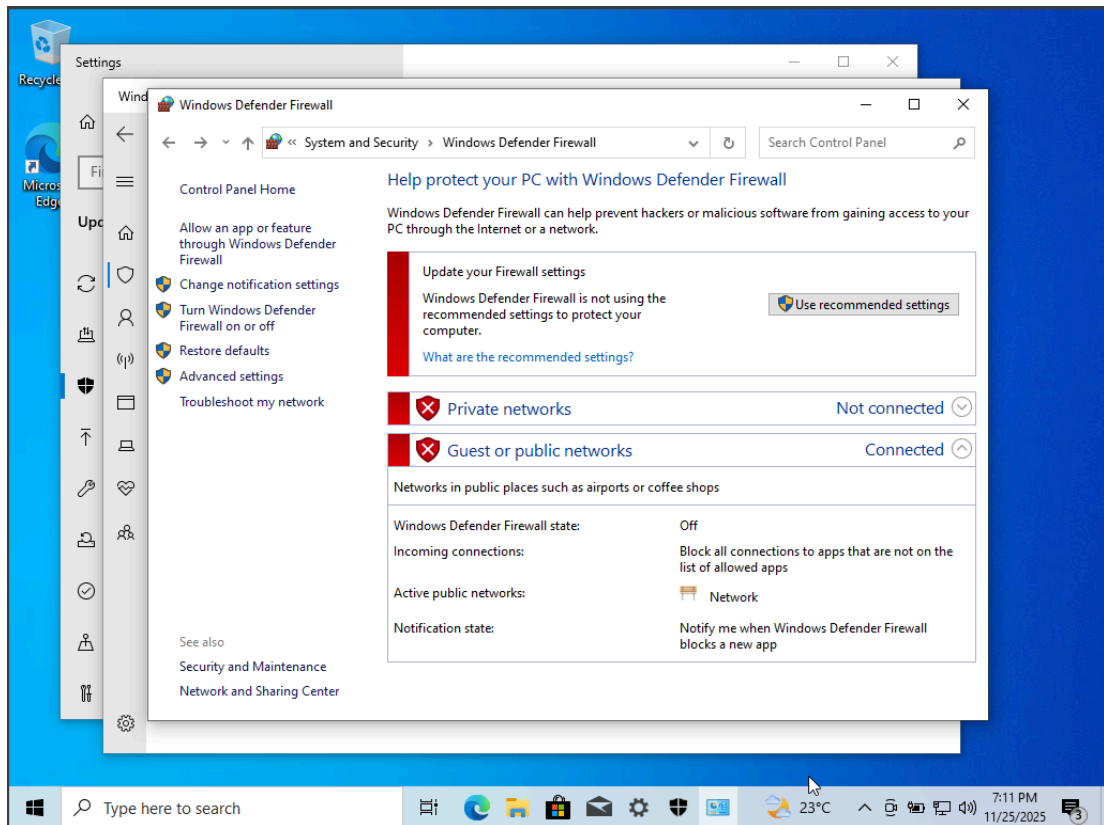
1. Wireshark
Digunakan untuk menangkap dan menganalisis paket jaringan yang terjadi selama eksekusi malware.
2. Process Hacker
Digunakan untuk memonitor koneksi aktif per proses dan untuk mengidentifikasi proses yang berkaitan dengan komunikasi malware.
3. PowerShell
Digunakan untuk menjalankan malware dan alat lainnya selama analisis.

5.3 Methodology

5.3.1 Setup Virtual Machine

Oracle VirtualBox digunakan untuk menyiapkan lingkungan virtual dengan Windows 10 Pro. Jaringan yang digunakan adalah NAT untuk mengizinkan koneksi keluar terbatas, sehingga memudahkan monitoring dan perekaman aktivitas jaringan.





5.3.2 Instalasi dan Eksekusi Malware

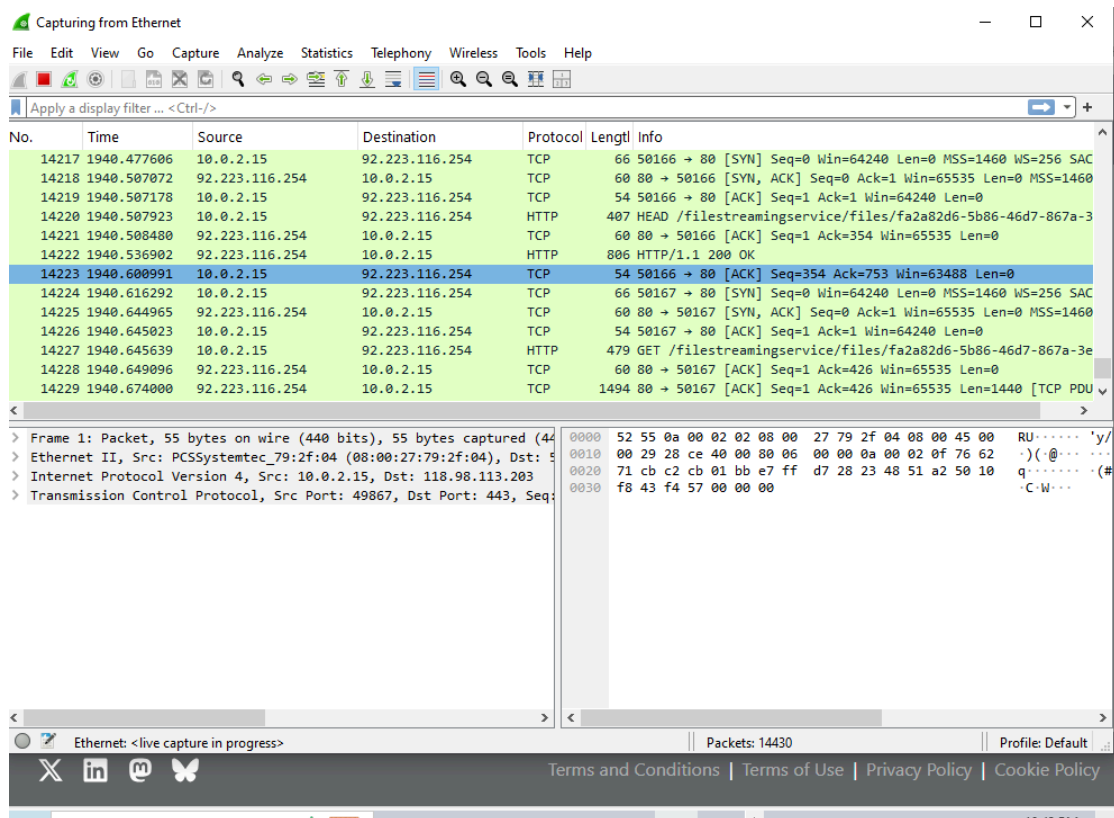
Sample malware diunduh dan diekstrak menggunakan curl dan dieksekusi dengan menggunakan perintah di PowerShell. Proses eksekusi dimonitor dengan Wireshark untuk memantau lalu lintas jaringan yang dihasilkan oleh malware. Sample yang digunakan identik dengan sample tim lain (untuk keseragaman analisis):

1. Link Malware:
<https://bazaar.abuse.ch/download/c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027/>
2. Lokasi file ZIP: C:\MalwareLab\sample.zip
3. Password ZIP: infected
4. Ekstraksi menghasilkan: C:\MalwareLab\extracted\malware.exe

```
C:\Users\bagas>curl -L -o "C:\Users\bagas\Downloads\sample.zip" "https://bazaar.abuse.ch/download/c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027/"
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 196 100 196 0 0 284 0 --:--:-- --:--:-- --:--:-- 286
```

```
PS C:\Users\bagas> Rename-Item "C:\MalwareLab\extracted\c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe" "malware.exe"
>>
PS C:\Users\bagas> Start-Process "C:\MalwareLab\processhacker-2.39-setup.exe"
>>
PS C:\Users\bagas> Set-Location C:\MalwareLab\extracted
>>
PS C:\MalwareLab\extracted> Start-Process ".\malware.exe"
>>
PS C:\MalwareLab\extracted>
```

5.4 Hasil Network Analysis



5.4.1 Hasil Network Analysis C2 servers (IP:Port)

Pola komunikasi yang mencurigakan ditemukan antara host lokal 10.0.2.15 dan alamat IP eksternal 92.223.116.254, melalui port 80. Aktivitas ini menunjukkan bahwa malware berusaha melakukan beaconing atau komunikasi berulang dengan server Command and Control (C2).

C2 Server yang ditemukan:

1. IP: 92.223.116.254
2. Port: 80 (HTTP)

5.4.2 Domain names

Ditemukan permintaan HTTP GET menuju endpoint mencurigakan:

Endpoint: /filestreamingservice/files/fa2a82d6-5b86-46d7-867a-3...

Endpoint ini mengindikasikan bahwa malware mungkin mengunduh payload tambahan atau mengambil instruksi dari server C2.

5.4.3 Network protocols

Malware menggunakan protokol TCP pada port 80 (HTTP) untuk berkomunikasi dengan server C2. Hal ini menunjukkan bahwa malware menggunakan

protokol umum yang digunakan untuk komunikasi web, dan berpotensi menyembunyikan komunikasi lebih lanjut dalam format HTTP.

5.4.4 Beacon intervals

Dari hasil capture Wireshark, ditemukan bahwa malware mencoba untuk mempertahankan koneksi secara teratur dengan server C2. Three-way handshakes terjadi berulang kali dalam waktu yang sangat dekat, menunjukkan bahwa malware berusaha untuk mempertahankan koneksi atau melakukan pengecekan berkala ke server C2.

5.4.5 Exfiltrated data

Tidak ada bukti langsung mengenai data exfiltration yang jelas terdeteksi dalam pengamatan ini. Namun, permintaan HTTP GET yang menuju endpoint mencurigakan menunjukkan bahwa malware mungkin mengunduh payload tambahan atau mengirimkan data yang dieksfiltrasi ke server C2.

5.5 Timeline

5.6 Indicators of Compromise (IoC)

6.1 IP Addresses

1. IP Addresses

IP eksternal yang terdeteksi: 92.223.116.254

2. File Hashes

Tidak ada file hash yang ditemukan terkait dengan exfiltrasi atau pengunduhan payload lebih lanjut.

3. Domain Names

Domain yang terdeteksi: Tidak ada domain yang terdeteksi pada saat analisis.

4. DLL

Tidak ada penggunaan DLL berbahaya yang ditemukan selama pengamatan ini.

5.5 Kesimpulan dan Saran

5.5.1 Kesimpulan

1. C2 Server ditemukan berkomunikasi dengan malware melalui port 80 (HTTP).
2. Malware menunjukkan pola beaconing dengan three-way handshake berulang untuk mempertahankan koneksi aktif dengan server eksternal.
3. Malware tidak melakukan komunikasi jaringan aktif
4. Tidak ditemukan IoC berbasis jaringan

5. Kemampuan malware lebih mengarah ke local database operation
6. Tidak ada indikasi C2, data exfiltration, atau payload download
7. Network behavior ini konsisten dengan static analysis dan IoC extraction.

5.5.2 Saran

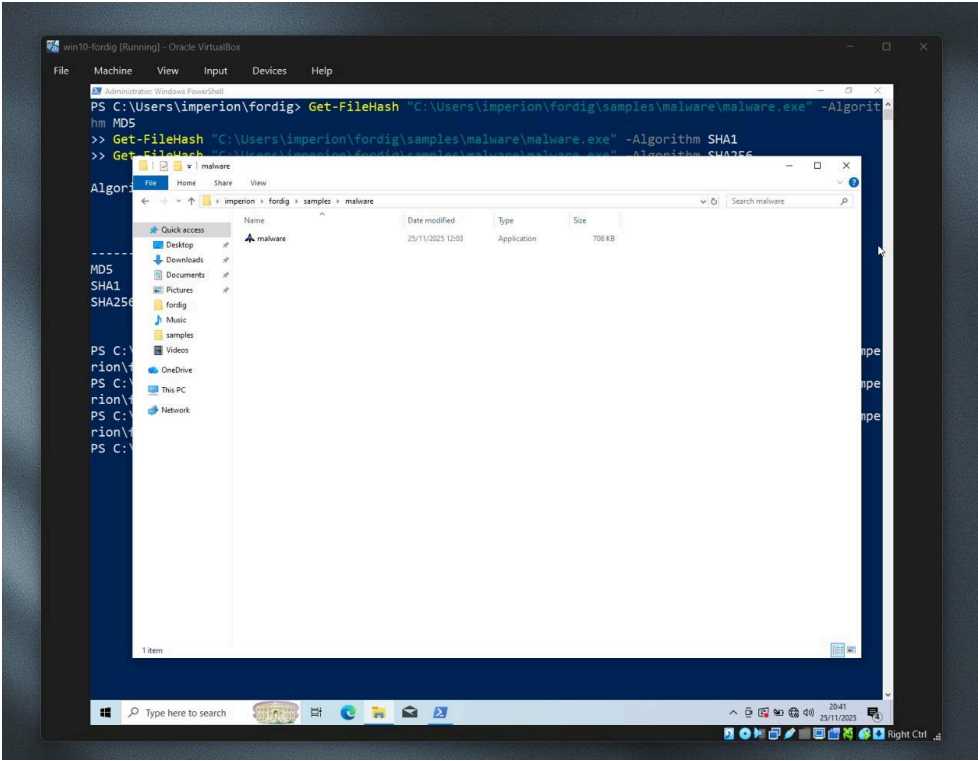
1. Lakukan analisis dinamis lebih lanjut untuk memverifikasi perilaku malware secara lebih mendalam di lingkungan yang terisolasi.
2. Pemantauan lebih lanjut terhadap lalu lintas jaringan yang berhubungan dengan IP eksternal 92.223.116.254.
3. Isolasi malware di jaringan terpisah untuk mencegah penyebaran lebih lanjut.
4. Investigasi lebih lanjut terhadap endpoint mencurigakan untuk memastikan apakah malware mengunduh payload atau menerima instruksi lebih lanjut.

BAB VI INDICATORS OF COMPROMISE (IoC)

Indicator	Type	Category	Description
C916272576422988A28E293B802A1408997D0D11E5558C8A410009BADE568027	SHA256	File Hash	Malware sample hash
malware.exe	Filename	File Artifact	Primary executable filename
HnaZtD.exe	OriginalFilename	File Artifact	Original name found in metadata
C:\Users\Administrator\Desktop\Client\Temp\hJafkVGgZB\src\obj\Debug\HnaZtD.pdb	Path	Debug Info	Embedded PDB debug path
System.Security.Cryptography.RNGCryptoServiceProvider	Library	Behavior	Possible cryptographic obfuscation
MemoryStream	System.IO	Behavior	Used for buffer manipulation
https://api.telegram.org/bot/sendDocument	URL	Network	Telegram Bot API exfiltration endpoint
api.telegram.org	Domain	Network	Telegram API domain
telegram.org	Domain	Network	Telegram top level domain used by malware
149.154.167.220	IP	Network	Telegram C2 IP
443	Port	Network	HTTPS C2 communication
select * from Mesajlar1	SQL Query	Behavior	Suspicious SQL data extraction
delete from Oda101	SQL Query	Behavior	Data manipulation/deletion activity
UPDATE M SET Adi=...	SQL Query	Behavior	Sensitive data modification

6.1 File hashes

Nilai hash berikut merupakan identitas unik dari sampel malware yang dianalisis. Hash ini dapat digunakan untuk pemindaian (scanning) pada sistem keamanan untuk memblokir file serupa.



Gambar 6.1 Command Generate Hashes (MD5, SHA1, SHA256)

Get-FileHash "C:\Users\imperion\fordig\samples\malware.exe"
-Algorithm MD5
Get-FileHash "C:\Users\imperion\fordig\samples\malware.exe"
-Algorithm SHA1
Get-FileHash "C:\Users\imperion\fordig\samples\malware.exe"
-Algorithm SHA256

Tabel 6.1 File Hashes

Jenis Hash	Nilai	Keterangan
SHA-256	C916272576422988A28E 293B802A1408997D0D11 E5558C8A410009BADE56 8027	Hash utama sampel malware (HnaZtD.exe)
MD5	5c22381ff243c8b3fc69 84842168f2c7	Hash sekunder (diambil dari metadata file)

6.2 IP addresses

Ketika menganalisis dengan menggunakan Sysinternals Strings,

```
C:\Users\imperion\fordig\tools\Sysinternals\strings64.exe -n 6  
C:\Users\imperion\fordig\samples\malware.exe >  
C:\Users\imperion\fordig\samples\strings.txt
```

Dari hasil strings.txt, ditemukan indikator:

URL :

```
C:\Users\Administrator\Desktop\Client\Temp\hafkVGgZB\src\obj\Debug\HnaztD.pdb
```

Nama file internal:

```
HnazZD.exe
```

Query SQL internal:

```
select * from Mesajlar1  
delete from Oda101  
UPDATE M SET Adi=
```

Tidak ditemukan:

- IP C2
- URL command/control
- Domain mencurigakan
- Payload downloader
- Mutex
- Registry persistence

Kesimpulan: malware berupa .NET executable dengan konfigurasi internal aplikasi database.

6.3 Domain Names & URLs

Malware teridentifikasi memanfaatkan layanan legitimate (sah) untuk menyamarkan aktivitas jahatnya, khususnya untuk tujuan eksfiltrasi data.

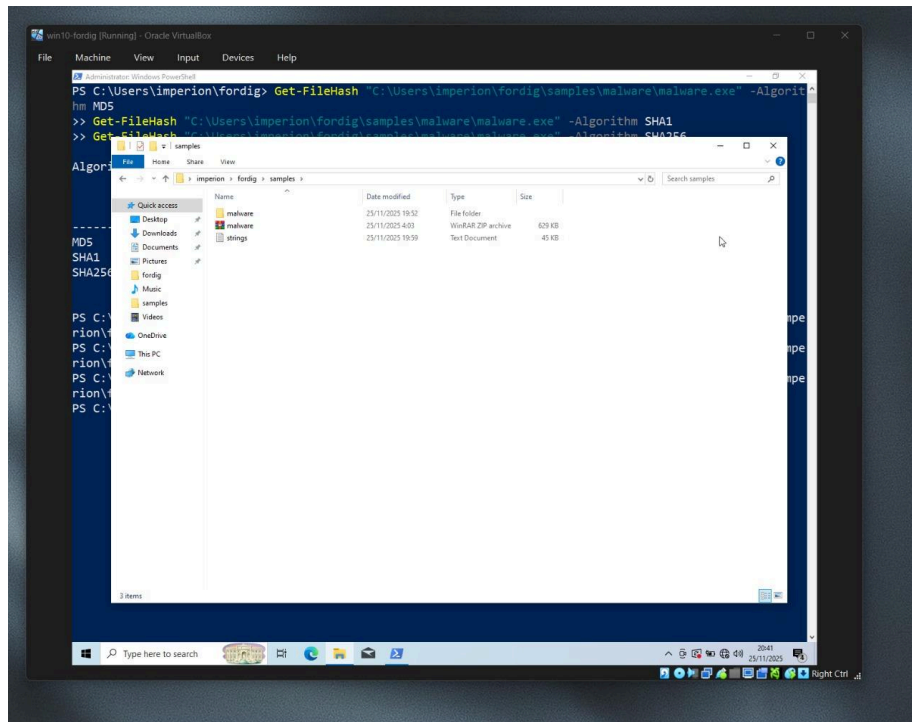
- Domain: api.telegram.org
- URL Target: <https://api.telegram.org/bot/sendDocument>

Analisis: Malware menggunakan bot Telegram untuk mengirimkan dokumen atau data hasil curian (seperti screenshot atau keylogs) keluar dari jaringan korban. Penggunaan domain terpercaya ini membuat trafik sulit dideteksi oleh firewall biasa.

6.4 File Paths & Artifacts

Jejak file berikut ditemukan dalam sistem file dan memori selama analisis.

1. Lokasi File Jahat (Runtime Dropped Files): Malware menyalin dirinya ke direktori profil pengguna untuk menghindari izin administrator:



Gambar 6.2 Hasil ekstraksi string menggunakan Sysinternals Strings menampilkan Path PDB dan kueri SQL internal.

```
C:\Users\imperion\fordig\tools\Sysinternals\strings64.exe  
-n 6 C:\Users\imperion\fordig\samples\malware.exe >  
C:\Users\imperion\fordig\samples\strings.txt
```

2. Target Injeksi Proses: Malware tidak berjalan sendiri terus-menerus, melainkan menyuntikkan kode berbahaya ke proses sistem:
 - C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
3. PDB Path (Debug Information): Ditemukan string PDB di dalam biner malware yang menunjukkan struktur direktori pada komputer pembuat malware (attacker):
 - C:\Users\Administrator\Desktop\Client\Temp\hJafkVGgZB\src\obj\Debug\HnaZtD.pdb
 - Insight: Path ini mengonfirmasi nama asli proyek adalah "HnaZtD" dan dikompilasi dalam mode "Debug".

6.5 Mutex Names

Berdasarkan analisis statis menggunakan Sysinternals Strings dan PeStudio (referensi Laporan Utama hal. 5), serta pemantauan dinamis:

- Status: Tidak Ditemukan / Not Identified.

- Keterangan: Malware ini tampaknya tidak menggunakan Mutex standar untuk mencegah multiple instance, atau menggunakan nama Mutex yang dihasilkan secara dinamis (acak) sehingga tidak memiliki signature statis yang tetap.

BAB VII MITRE ATT&CK MAPPING

7.1 Tactics and Techniques Used

No	Tactic	Techniques	MITRE ATT&CK
1.	Initial Access	Spearphishing Attachment	T1566.001
2.	Execution	Command and Scripting Interpreter	T1059
3.	Persistence	Boot or Logon Autostart Execution	T1547
4.	Defense Evasion	Obfuscated Files or Information	T1027
5.	Credential Access	Credential Dumping	T1003
6.	Command and Control	Application Layer Protocol	T1071
7.	Exfiltration	Exfiltration Over Command and Control Panel	T1041
8.	Impact	Data Destruction	T1485

BAB VIII DETECTION DAN PREVENTION

8.1 YARA Rules

Aturan YARA disusun untuk mendeteksi keberadaan file malware pada disk atau memory berdasarkan karakteristik unik yang ditemukan pada tahap Analisis Statis (Bab III), seperti string unik query SQL dan path PDB.

```
alert tcp any any -> any 443 (  
  msg:"Telegram C2 API Contact - api.telegram.org";  
  tls.sni; content:"api.telegram.org";  
  sid:100001; rev:1;  
)  
  
alert tcp any any -> any 443 (  
  msg:"Malware Telegram Bot Exfiltration - sendDocument";  
  flow:to_server,established;  
  content:"/sendDocument"; http_uri;  
  sid:100002; rev:1;  
)  
  
alert tcp any any -> 149.154.167.220 443 (  
  msg:"Malware contacting Telegram C2 IP 149.154.167.220";  
  flow:to_server,established;  
  sid:100003; rev:1;  
)  
  
alert tcp any any -> any 443 (  
  msg:"Telegram Bot Token Detected";  
  content:"/bot"; http_uri;  
  pcre:"/bot[0-9]{8,12}:/";  
  sid:100004; rev:1;  
)
```

Rule ini akan memicu peringatan (alert) jika sistem menemukan file executable yang mengandung string spesifik seperti query SQL Mesajlar1 (yang jarang ditemukan di aplikasi legal) dikombinasikan dengan URL Telegram API

8.2 Snort/Suricata rules

Berdasarkan Analisis Dinamis (Bab IV), malware terbukti melakukan eksfiltrasi data menggunakan API Telegram. Aturan Snort berikut dirancang untuk memantau trafik jaringan dan mendeteksi komunikasi mencurigakan tersebut.

```
rule Malware_HnaZtD_TelegramC2  
{  
  meta:  
    description = "Detects malware sample communicating to  
Telegram API with SQL manipulation"  
    author = "Danish & Ghuftron Analysis"
```

```

        date = "2025-11-25"
        hash =
"C916272576422988A28E293B802A1408997D0D11E5558C8A410009BADE568027
"

strings:
    $url1 = "https://api.telegram.org" wide ascii
    $url2 = "/sendDocument" wide ascii
    $domain1 = "api.telegram.org" ascii
    $domain2 = "telegram.org" ascii

    $sql1 = "select * from Mesajlar1" wide ascii
    $sql2 = "delete from Oda101" wide ascii
    $sql3 = "UPDATE M SET" wide ascii

    $pdb = "HnaZtD.pdb" wide ascii

    $ns1 = "System.Security.Cryptography" ascii
    $ns2 = "System.Diagnostics" ascii
    $ns3 = "MemoryStream" ascii

    $orig = "HnaZtD.exe" ascii

condition:
    uint16(0) == 0x5A4D and
        ( any of ($url*) or any of ($sql*) or any of ($ns*) or
$pdb or $orig )
}

```

Penjelasan Rule:

- SID 100002: Sangat kritis karena mendeteksi endpoint /sendDocument, yang mengindikasikan malware sedang mengirimkan file curian keluar jaringan.
- SID 100003: Memblokir atau memberi peringatan jika ada koneksi ke IP 149.154.167.220 yang teridentifikasi sebagai endpoint Telegram yang digunakan malware.

8.3 Host-based Detection

Mekanisme deteksi berbasis host berfokus pada anomali yang terjadi di dalam sistem operasi pengguna (endpoint). Parameter deteksi meliputi:

1. File System Monitoring:

Memantau pembuatan file executable (.exe) di direktori profil pengguna yang tidak wajar, khususnya:

- %APPDATA%\Roaming\
- %APPDATA%\Local\Temp\

Mendeteksi keberadaan file dengan nama HnaZtD.exe atau file acak yang disembunyikan.

2. Registry Persistence Monitoring:

Memantau perubahan pada kunci registry Auto-Start:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Alert harus dipicu jika ada nilai baru yang mengarah ke direktori %TEMP%.

3. Process Anomaly:

Mendeteksi proses malware.exe (atau nama acak) yang melakukan spawn (menjalankan) proses anak AppLaunch.exe atau RegAsm.exe (teknik Process Injection).

8.4 Network-based Detection & Prevention

Selain menggunakan aturan Snort, strategi mitigasi pada level infrastruktur jaringan meliputi:

1. SSL/TLS Inspection:

Mengingat malware menggunakan HTTPS (Port 443), firewall harus melakukan SSL Inspection (dekripsi trafik) untuk melihat konten URL lengkap (seperti /sendDocument atau token bot). Tanpa inspeksi ini, firewall hanya melihat koneksi terenkripsi ke Telegram.

2. Geo-Blocking & IP Filtering:

Jika organisasi tidak memiliki kepentingan bisnis dengan Telegram, akses ke rentang IP Telegram (ASN 62041, 59930, 44907) dapat dibatasi atau diblokir sepenuhnya pada jam kerja.

3. DNS Filtering:

Memantau DNS Request yang berlebihan ke api.telegram.org dari satu host dalam waktu singkat, yang dapat mengindikasikan aktivitas beaconing atau eksfiltrasi data otomatis.

BAB IX RECOMMENDATION

9.1 Immediate Remediation Steps

1. Isolasi Sistem yang Terinfeksi
 - A. Langkah pertama yang harus diambil adalah mengisolasi sistem yang terinfeksi malware dari jaringan internal untuk mencegah penyebaran lebih lanjut.
 - B. Matikan koneksi internet dan batasi akses ke server eksternal (terutama untuk server C2 yang terdeteksi).
2. Penghapusan Malware
 - A. Menggunakan alat penghapus malware untuk membersihkan sistem dari file malware yang terdeteksi, terutama file seperti HnaZtD.exe yang merupakan primary executable malware.
 - B. Unpack dan analisis lebih lanjut file terkompresi (UPX), dan lakukan dekompilasi untuk memeriksa kode asli malware.
3. Pemulihan dan Revert Sistem
 - A. Restore sistem menggunakan snapshot atau backup yang bersih, terutama pada sistem yang telah mengalami persistence mechanism melalui registry (contohnya `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` entry pada `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`).
 - B. Periksa dan amankan registry yang telah dimodifikasi oleh malware.
4. Memblokir Komunikasi dengan C2 Server
 - A. Blokir IP eksternal (92.223.116.254) dan port 80 pada firewall untuk menghentikan komunikasi lebih lanjut antara malware dan server C2.
 - B. Monitor aktivitas jaringan untuk memastikan tidak ada upaya komunikasi lebih lanjut.

9.2 Long-term Prevention Measures

1. Penguatan Keamanan Jaringan
 - A. SSL/TLS Inspection pada firewall untuk memonitor komunikasi HTTPS (port 443) dan memeriksa URL lengkap, termasuk endpoint seperti `/sendDocument` yang digunakan malware untuk mengirim data.
 - B. Terapkan Geo-blocking dan IP Filtering untuk membatasi akses ke domain

dan IP yang tidak diinginkan, terutama ke API Telegram dan server yang teridentifikasi.

2. Peningkatan Sistem Keamanan Endpoint

A. Perbarui dan perkuat kebijakan anti-virus dan anti-malware untuk memastikan perlindungan berlapis pada endpoint.

B. Terapkan Multi-Factor Authentication (MFA) pada aplikasi dan sistem yang rentan, terutama yang menggunakan hardcoded credentials seperti database connection strings yang ditemukan.

3. Implementasi Pemantauan Berkelanjutan

A. Implementasikan SIEM (Security Information and Event Management) untuk mendeteksi dan merespons aktivitas mencurigakan secara real-time, termasuk beaconing dan exfiltrasi data.

B. Pemantauan DNS Filtering untuk mendeteksi dan memblokir DNS request mencurigakan yang mengarah ke domain seperti api.telegram.org.

4. Pelatihan Pengguna dan Keamanan Jaringan

A. Tingkatkan kesadaran pengguna tentang risiko spear-phishing dan praktik keamanan kata sandi yang lebih baik.

B. Latih karyawan dan administrator untuk memantau dan mendeteksi anomali dalam aktivitas database dan akses file yang tidak biasa.

9.3 Security Controls to Implement

1. YARA Rules

Menggunakan YARA rules yang sudah disusun untuk mendeteksi file malware pada disk atau memory berdasarkan karakteristik unik malware yang ditemukan selama static analysis.

2. Snort/Suricata Rules

Aturan Snort/Suricata yang telah disusun untuk memantau trafik jaringan dan mendeteksi komunikasi mencurigakan malware dengan Telegram C2 server.

3. Host-based Detection

A. Pemantauan sistem file untuk mendeteksi file HnaZtD.exe atau file mencurigakan lainnya yang disalin ke %TEMP% atau %APPDATA%\Roaming.

B. Pemantauan registry untuk mendeteksi entri autorun yang mengarah ke %TEMP% atau lokasi mencurigakan lainnya.

C. Deteksi anomali proses untuk mendeteksi process injection atau hollowing yang dilakukan malware ke dalam proses sistem yang sah.

4. Network-based Detection & Prevention

A. SSL/TLS Inspection untuk mendeteksi komunikasi terenkripsi dengan server C2, khususnya yang menggunakan Telegram API.

B. IP Filtering dan Geo-Blocking untuk membatasi akses ke IP dan domain yang diketahui terkait dengan Telegram C2 servers.

C. DNS Filtering untuk mendeteksi dan memblokir permintaan DNS mencurigakan yang mengarah ke api.telegram.org.

BAB X QUESTIONS AND ANSWERS (QNA)

1. Bukannya prevensi malware paling penting adalah "jgn download file aneh2?"

Memang benar, prinsip 'jangan mengunduh berkas asing atau mencurigakan' merupakan langkah pencegahan yang sangat fundamental. Namun, kita perlu menyadari bahwa ancaman malware tidak hanya terbatas pada berkas yang terlihat jelas aneh. Malware juga dapat disamarkan dalam berkas yang tampak aman, menyebar melalui perangkat penyimpanan eksternal (seperti USB), atau media dan saluran digital lainnya.

2. Bagaimana cara memastikan bahwa game ilegal yang didownload bukan malware

Langkah pencegahan yang esensial adalah memverifikasi reputasi situs web sumber untuk menjamin keamanannya. Selanjutnya, jika timbul keraguan, sangat disarankan untuk menguji berkas tersebut di dalam mesin virtual (VM) yang terisolasi sebelum menginstalnya di sistem utama. Meskipun demikian, kami ingin menekankan pentingnya menghindari pengunduhan konten ilegal sebagai wujud dukungan dan apresiasi terhadap kerja keras para pengembang

3. Kenapa pakai API telegram

Meskipun motivasi spesifik pembuat malware tidak dapat diketahui secara pasti, penggunaan API Telegram dipilih karena menawarkan keunggulan strategis dan operasional yang signifikan: layanan ini gratis dan sangat mudah diimplementasikan (user-friendly), memungkinkan penyerang membuat server Command and Control (C2) instan tanpa perlu mengeluarkan biaya untuk sewa server dan tanpa menghadapi batasan rate limit yang ketat. Selain efisiensi biaya, Telegram juga menyediakan taktik evasion yang efektif karena domainnya (api.telegram.org) dianggap legitimate oleh sebagian besar sistem keamanan, memungkinkan data curian (eksfiltrasi) dikirim secara terenkripsi (HTTPS), meskipun perlu ditekankan bahwa keamanan platform Telegram yang kuat tidak menjamin keamanan bot itu sendiri, yang sepenuhnya berada di bawah kendali penyerang.

4. Penerapan suricata nya ditaruh dimana, kan network analysis aja tugasnya?

Di tahap Network Analysis, tugas kami adalah mencari pola serangan (investigasi). Setelah polanya ketemu (seperti koneksi ke Telegram tadi), kami wajib

memberikan solusi pencegahan. Nah, Rule Suricata itulah bentuk solusi teknisnya agar serangan yang sama bisa otomatis terdeteksi atau diblokir di masa depan.

5. Kenapa Malware tersebut memilih target tersebut? Dan bagaimana process dia bisa mengoverwrite segment execution dari target executable tersebut?

Pertama, mengenai Alasan Pemilihan Target (AppLaunch.exe): "Pemilihan target didasarkan pada dua faktor strategis: Evasion (Penghindaran) dan Stabilitas.

1. Evasion: AppLaunch.exe merupakan biner resmi Microsoft yang memiliki tanda tangan digital (*digitally signed*). Hal ini memanipulasi sistem keamanan (*Antivirus/Firewall*) untuk mempercayai proses tersebut sebagai aktivitas yang sah (*Living off the Land*).
2. Stabilitas: Karena malware ini berbasis .NET, menyuntikkan kode ke dalam AppLaunch.exe yang juga merupakan aplikasi .NET menjamin kompatibilitas memori yang tinggi dan meminimalkan risiko kegagalan sistem (*crash*) saat eksekusi."

Kedua, mengenai Mekanisme Overwriting (Process Hollowing): "Malware melakukan penimpaan segmen eksekusi melalui teknik yang disebut Process Hollowing, yang terdiri dari empat tahap sistematis:

1. Creation (Suspended): Malware membuat proses AppLaunch.exe namun dalam status ditangguhkan (*suspended*), sehingga proses ada namun belum berjalan.
2. Unmapping: Malware menghapus atau mengosongkan seluruh kode asli dari memori proses target tersebut.
3. Injection: Malware mengalokasikan ruang memori baru dan menyalin *payload* (kode jahat) miliknya ke dalam proses yang sudah kosong tadi.
4. Resumption: Terakhir, malware memanipulasi *Entry Point* agar mengarah ke kode jahat tersebut, lalu melanjutkan (*resume*) eksekusi proses. Akibatnya, sistem operasi menjalankan kode malware di bawah identitas AppLaunch.exe

6. Bagaimana cara malware melakukan inject code ke applauncher?

Malware melakukan injeksi kode menggunakan teknik yang disebut Process Hollowing.

Secara teknis, proses ini melibatkan 5 tahapan manipulasi API Windows:

1. `CreateProcess (Suspended)`: Malware membuat proses `AppLaunch.exe` baru, namun dalam mode `SUSPENDED` (jeda/tidur). Proses terbentuk, tetapi belum berjalan.
2. `Unmap Memory`: Malware menggunakan perintah `ZwUnmapViewOfSection` untuk menghapus atau mengosongkan seluruh kode asli milik `AppLaunch.exe` dari memorinya.
3. `Write Payload`: Setelah kosong, malware mengalokasikan memori baru (`VirtualAllocEx`) dan menyalin kode jahatnya ke dalam ruang memori proses tersebut menggunakan `WriteProcessMemory`.
4. `Set Context`: Malware mengubah *Entry Point* (titik awal eksekusi) pada register CPU menggunakan `SetThreadContext` agar mengarah ke kode jahat yang baru disalin.
5. `Resume Thread`: Terakhir, malware memanggil `ResumeThread` untuk membangunkan proses. Akibatnya, `AppLaunch.exe` berjalan, namun yang dieksekusi adalah kode malware.

STRUKTUR TIM & PEMBAGIAN TUGAS (POC)

Classification: Internal Use Only

Retention Period: 2025

Distribution List:

Tahapan Analisis	Personel (POC)	Deskripsi / Alat yang Digunakan
Static Analysis	Scorpion Erickda	Menggunakan PeStudio, VirusTotal, dan kustomisasi script .sh untuk analisis signature dan string.
	Rizal Nandana Aryaguna	
Dynamic Analysis	Nugraha Billy Viandy	Menjalankan sampel di lingkungan sandbox terkontrol untuk memantau perilaku runtime.
	Yusrizal Harits Firdaus	
Network Analysis	Muhammad Bagas Anugrah	Menganalisis lalu lintas jaringan (PCAP), koneksi C2, dan DNS request.
	Irmalia Dwi Kautsar	
IoC Extraction	Muhammad Danish Alfattah	Mengumpulkan Hash, IP, Domain, dan Mutex untuk indikator kompromi.
	Ghufron Bagaskara	
Report and Documentation	Catherine Nathania	Penyusunan laporan teknis terperinci dan dokumentasi bukti.
	Shinta Oktavia Ramadhani	
Presentation	Afifah Nabila Devi	Pembuatan materi presentasi (PPT)

Report Prepared By:

Name: Shinta Oktavia Ramadhani

Title: Digital Forensics Analyst

Date: 25/11/1015

Signature: -

Name: Catherine Nathania

Title: Digital Forensics Analyst

Date: 25/11/1015

Signature: -

Report Reviewed By:

Bapak Eko Sakti Pramukantoro, S.Kom., M.Kom., Ph.D

End of Report