



FORENSIK DIGITAL

Laporan Analisis Malware Case 2: AgentTesla

Start Now



ANGGOTA

- Nugraha Billy Viandy
- Yusrizal Harits Firdaus
- Muhammad Danish Alfattah
- Ghufon Bagaskara
- Scorpion Erickda
- Catherine Nathania

- Irmalia Dwi Kautsar
- Muhammad Bagas Anugrah
- Shinta Oktavia Ramadhani
- Afifah Nabila Devi
- Rizal Nandana Arya Guna



SKENARIO INSIDEN (LATAR BELAKANG)

SecureBank Indonesia mengalami insiden keamanan di mana beberapa workstation karyawan menunjukkan aktivitas yang mencurigakan. Antivirus mendeteksi file executable yang suspicious namun tidak dapat mengidentifikasi jenis malware dengan pasti.

Security Operations Center (SOC) telah mengisolasi sample dari sistem yang terinfeksi dan meminta Digital Forensics Team untuk melakukan analisis mendalam.



SKENARIO INSIDEN (LATAR BELAKANG)

Tujuan Analisis:

- Identifikasi karakteristik malware (Static Analysis).
- Memetakan perilaku malware (Dynamic Analysis).
- Behavior & Capabilities
- Mendapatkan Indicators of Compromise (IoC) untuk mitigasi.





LINGKUNGAN ANALISIS (LAB SETUP)

Prinsip Keamanan: Safety First - Isolasi total menggunakan Virtual Machine.

Spesifikasi Lab:

1. VM Korban: Windows 10 Pro (Jaringan: Host-Only, Defender Disabled).
2. VM Analisis: Kali Linux (Tools: Radare2, Exiftool, Objdump).

Tools Utama: VirusTotal (Cloud analysis), PEStudio (Static), Wireshark (Network), Process Monitor (Behavior).



HASIL ANALISIS DINAMIS (BEHAVIOR)

Awal Eksekusi:

1. Malware dieksekusi melalui WinRAR.exe setelah payload diekstrak dari file ZIP.
2. Payload utama mulai berjalan dan langsung melakukan enumerasi awal terhadap sistem.

Aktivitas Sistem:

1. Malware membaca Machine GUID, hostname, serta sejumlah entri registry penting sebagai fingerprinting.
2. Payload memunculkan proses turunan dan menyiapkan data untuk eksfiltrasi sebelum membangun koneksi jaringan.



HASIL ANALISIS STATIS (STATIC ANALYSIS)



Identitas File:

➤ File Name:

c91267...68027.exe

➤ Tipe:

PE32 Executable (GUI) Intel 80386
Mono/.Net assembly.

➤ Hash (SHA256):

c91267225764229b8a282e938b0
2a1408997d0d1e5558ca841a009
bade568027

➤ Temuan Anomali:

1. Packer Detection: Terdeteksi menggunakan UPX (teknik untuk mengompres/menyembunyikan kode).
2. Timestamp: Tercatat tahun 2061, indikasi kuat manipulasi metadata (timestomping).
3. VirusTotal: Rasio deteksi tinggi, diklasifikasikan sebagai Malware/Trojan/Stealer.

ANALISIS JARINGAN (NETWORK IOC)



➤ Komunikasi C2 (Command & Control):

Malware membangun koneksi TLS (Port 443) ke domain publik.

➤ Destinasi:

api.telegram.org

➤ Ransomware

149.154.167.220

➤ Aktivitas Berbahaya:

1. Menggunakan API Telegram (getMe, sendDocument) untuk mengirim data curian ke bot penyerang.
2. Status respon "ok true" menandakan pengiriman data berhasil.

Process Injection (Process Hollowing): ◀

Temuan: Malware induk (HnaZtD.exe) tidak bekerja sendirian

Teknik: Menyuntikkan kode berbahaya ke dalam proses legal Windows: AppLaunch.exe

Path Target:

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

Tujuan: Mengelabui antivirus agar mengira aktivitas pencurian data dilakukan oleh aplikasi resmi Microsoft.

Mekanisme Persistensi (Agar Malware "Awet"): ◀

Target Registry:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

Aksi: Menambahkan nilai registry agar malware berjalan otomatis saat Windows startup.

Lokasi File: Malware menyalin dirinya ke %APPDATA%\Roaming\ dan %TEMP%.

TEKNIK EVASION & PERSISTENCE

Teknik Penghindaran & Mekanisme Persistensi



INDICATORS OF COMPROMISE (IOC)

Tabel ini berisi artefak digital untuk mendeteksi serangan serupa:

Type Indikator	Nilai / Detil	Keterangan
File Hash (SHA-256)	C916272576422988A28E293 B802A1408997D0D11E5558 C8A410009BADE568027	Identitas unik malware
Filename	HnaZtD.exe, malware.exe	Nama file saat dieksekusi
C2 Domain	api.telegram.org	Server tujuan eksfiltrasi
C2 IP Address	92.223.116.254, 149.154.167.220	Alamat IP Server Telegram
PDB Path	...\obj\Debug\HnaZtD.pdb	Jejak direktori komputer pembuat malware
SQL Query	select * from Mesajlar1	Query unik pencurian data

MITRE ATT&CK FRAMEWORK

Pemetaan Teknik Serangan (MITRE ATT&CK)

➤ **Malware AgentTesla ini menggunakan teknik standar industri berikut:**

1. Initial Access (T1566): Spearphishing Attachment (Metode masuk awal).
2. Execution (T1059): Command and Scripting Interpreter (Menjalankan perintah).
3. Persistence (T1547): Registry Run Keys / Startup Folder (Bertahan saat reboot).
4. Defense Evasion (T1027 & T1055): Obfuscated Files (UPX) & Process Injection (Sembunyi di AppLaunch).
5. Credential Access (T1003): Credential Dumping (Mencuri password).
6. Command & Control (T1071): Web Service (Menggunakan API Telegram).

ATURAN DETEKSI (DETECTION RULES)



Strategi Deteksi (YARA & Snort)

YARA Rule (Deteksi File): <

1. Fokus mendeteksi string unik di dalam memori/disk.
2. Signature: String select * from Mesajlar1 (Indikasi pencurian database) dan Path PDB HnaZtD.pdb.

Snort/Suricata Rule (Deteksi Jaringan): <

1. Fokus memonitor lalu lintas jaringan.
2. Signature: Mendeteksi paket HTTPS menuju api.telegram.org dengan URI /sendDocument (Indikasi pengiriman file curian).

Host-Based Detection: <

1. Alert jika ada file .exe baru muncul di folder %TEMP%.
2. Alert jika ada proses AppLaunch.exe yang melakukan koneksi internet (seharusnya jarang terjadi).

REKOMENDASI

Tindakan Remediasi (Segera):

- Isolasi: Putuskan koneksi jaringan host yang terinfeksi.
- Blokir: Blokir IP C2 92.223.116.254 di perimeter firewall.
- Pembersihan: Hapus file di %APPDATA% dan bersihkan Registry HKCU\...\Run.

Pencegahan Jangka Panjang:

- SSL/TLS Inspection: Aktifkan di Firewall untuk mendekripsi trafik HTTPS (agar payload Telegram terlihat).
- Endpoint Protection (EDR): Implementasi EDR yang mampu mendeteksi perilaku Process Injection.
- Geo-blocking: Batasi akses IP dari negara yang tidak relevan dengan operasional bisnis.

KESIMPULAN

Identifikasi: Sampel dikonfirmasi sebagai AgentTesla (Spyware/RAT) berbasis .NET yang dipacking dengan UPX.

Anomali Utama: Manipulasi timestamp menjadi tahun 2061 (Timestomping).

Perilaku Kunci:

1. Melakukan Process Injection ke sistem legal.
2. Mencuri kredensial dan data database lokal.
3. Menggunakan Telegram API sebagai sarana C2 untuk menghindari deteksi firewall konvensional.

Dampak: Risiko tinggi terhadap kerahasiaan data otentikasi dan integritas sistem perbankan.



THANK YOU

IZIINN