

**WEBINAR**

# Fileless Attack



@nagacyberdefense



ORANGSIBER  
INDONESIA

@orangsiber

# Fileless Attack

## WEBINAR OUTLINE

1. Pengenalan dan Penjelasan singkat
2. Real World Examples
3. Perilaku Umum
4. Proses
5. Kesimpulan



@nagacyberdefense



@orangsiber



# Fileless Attack

## Pengenalan dan Penjelasan Singkat



@nagacyberdefense



@orangsiber



## Pengenalan dan Penjelasan Singkat

- Suatu *Malicious Code* yang tidak perlu membuat *regular file* pada system.
- Berbeda dari cara kerja *malware* yang biasanya.
- Meninggalkan *file* berukuran sangat kecil dan tersembunyi agar persisten.

## *FileLess or MalwareLess?*

Ada 2 cara untuk menginfeksi suatu sistem tanpa adanya sebuah file:

1. Tidak menggunakan malware sama sekali. Hanya membuat *backdoor* dari konfigurasi yang ada pada sistem sehingga tidak bisa mengambil *control* dari sistem setiap saat. (*MalwareLess*)
2. Menggunakan code yang tidak akan disimpan ke *storage disk*. Meninggalkan *first stage* dari code pada sistem agar *control*-nya persisten. (*FileLess*)

# ***Kenapa Digunakan dalam Pentesting?***

- Menghindari deteksi *Anti-Virus*.
- Meninggalkan sedikit jejak untuk forensik digital.
- Environment yang menyulitkan penyerang untuk melakukan *Upload*.
- Membantu bypass Whitelisting Aplikasi.

## Code tanpa File?

1. Seluruh code disimpan di memory. (Tidak persisten)
2. Menyimpan code di non-file atau penyimpanan non-reguler:
  - Di luar *filesystem*: UEFI, HDD Firmware, \$EA, dll.
  - Sistem Network / Eksternal
  - Alternate Data Streams (ADS)
  - Registry

## **Bentuk Lain Penyimpanan Non-Reguler**

1. WMI (*Subscriptions*)
2. Windows events (\*.evt)
3. Di dalam dokumen (\*.doc, \*.xls, \*.pdf)

## Execute Code *Tanpa File*

- *Remote injection ke dalam memory (Remote call atau exploit)*
- *Remote Binaries (EXE, DLL) via SMB, WebDAV, dll.*
- *Scripting Languages (bisa di load secara remote atau melalui command-line)*
  - PowerShell (PowerShell.exe)
  - Javascript / VbScript (regsvr32.exe, rundll32.exe, dll.)
  - .NET assemblies (regasm.exe, ieeexec.exe, InstallUtil.exe)

# Fileless Attack

## EVIDENCES

# Real World Examples

1. Worms (*Slammer*)
2. Poweliks
3. WMIGhost
4. Empire
5. Duqu 2.0 (*Kaspersky*)



@nagacyberdefense



@orangsiber

## Slammer (2003)

1. Menginfeksi ribuan komputer dan berdampak pada *traffic Internet* di beberapa daerah
2. Worm ini melakukan exploit terhadap kerentanan *buffer overflow* dari *Microsoft SQL Server resolution service* (1434/UDP)
3. Hanya sebesar 376 bytes dikemas dalam sebuah *UDP Packet*.



## Poweliks (2014)

1. Infeksi via *word macro*
2. Persisten via Autostart registry key  
(HKLM\Software\Microsoft\Windows\CurrentVersion\Run)
3. Minimal first stage: menggunakan rundll32 untuk menjalankan *Javascript code*
4. Stage berikutnya juga disimpan di *registry* (*encoded*).  
Menjalankan *PowerShell code*.
5. *PowerShell* menginjeksi DLL ke dalam *process memory* lainnya tanpa menyentuh disk.

## WMIGhost (2014)

1. Infeksi via *Word macro*
2. *Dropper* dan *UAC bypass binaries* menyentuh *disk* (sehingga tidak sepenuhnya FileLess)
3. Kemudian melakukan register untuk *WMI Classes* yang diperlukan secara permanen: *event definition*, *event filter*, dan *event consumer*
4. Menggunakan *Javascript* sebagai *payload code* di *script aktif* pada *event consumer*.

## Empire (2015)

1. RAT berbasis *PowerShell*
2. Hanya bekerja melalui *memory*
3. Memiliki banyak pilihan untuk penyimpanan persisten:  
*registry, ADS, eventlog, dan WMI subscriptions.*



ORANGSIBER  
INDONESIA

## Duqu 2.0 (2015)

1. *Infection vector* tidak diketahui
2. Hanya beberapa hosts yang disk-nya digunakan untuk persisten
3. Host-host ini menginjeksi *malware* secara *remote* ke dalam *system memory* lain
4. Memperoleh *privilege* sebagai *domain administrator* dan menjalankan MSI packages (via *new service* atau *scheduled task*)

# Fileless Attack

## Perilaku Umum *Common Fileless Behaviour*



@nagacyberdefense



@orangsiber

## Bagaimana Perilakunya?

1. **Tahap Pertama** : Biasanya sebuah vbs / js berukuran kecil (bukan PowerShell).
2. **Tahap Kedua** : *Main script based on Powershell*. Logika yang lebih kompleks dan *powerful* yang menginjeksi *binary* ke dalam *process*.
3. **Tahap Ketiga** : *Binary*. Biasanya berupa *Portable Executable DLL payload*. Mirip *malware* pada umumnya, namun tidak akan disimpan pada *storage disk*.

# Fileless Attack

Proses

## **Bagaimana ini Bekerja?**

1. *FileLess Infection*
2. *FileLess Backdoor*
3. *FileLess persistence*



@nagacyberdefense



@orangsiber

## FileLess Infection

- Infeksi tanpa mengirim *file* apapun
- Tidak umum. Bahkan operasi *Fileless APT* tetap menggunakan *file* tertentu pada fase ini
- Mengirim *exploit* sebelum *application layer*:
  - Di dalam sebuah *stream*
  - Di *network layer* (contohnya: SMB atau *SSL exploits*)
  - Membuka *network services* (contohnya: *Eternalblue*)



## FileLess Backdoor

- Backdoor hanya berbasis konfigurasi (**tanpa ada code apapun**)
- Beberapa cara yang popular:
  1. *Create user + remote exec (Psexec/Sc, WMI, SchTasks, WinRM, PSRemoting)*
  2. *Binary Image hijack + Remote Desktop*
  3. *Silver/Golden tickets.*
  4. *Proxy + Decrease security*

## FileLess Persistence

- Tahap awal: *Registry Autostart entries*
  1. *run entries*
  2. *Scheduled tasks*
  3. *Image hijacks*
  4. *wmi*
  5. *Services*
- Biasanya **terlalu mencolok** bagi seorang analis, namun **sulit** dideteksi menggunakan *tools* otomatis karena tidak menggunakan *file* apapun.



# Fileless Attack

**Last But Not Least**  
**Kesimpulan**



@nagacyberdefense



@orangsiber

## Kesimpulan

*Fileless Attack* dapat dilakukan hanya dengan melibatkan file berukuran sangat kecil dan dapat disembunyikan dengan mudah agar serangan bersifat persisten tanpa memerlukan penyimpanan pada *storage disk* sehingga sulit untuk dideteksi.



# Fileless Attack

## DEMONSTRASI

Dapat dilihat di Channel Youtube  
Orangsiber



@nagacyberdefense



@orangsiber

# WEBINAR



@nagacyberdefense



ORANGSIBER  
INDONESIA

@orangsiber

# Terima Kasih

Bersumber dari Presentasi Ramon Pinuaga "FileLess Malware Infections : Malware tricks for Pentesters" di Bsides Lisbon 2017