NOAH – NO AGENT HUNTING
UNCOVER THE EVIL WITHIN
About Me

- I’m Belgian working in Montréal - Canada.
- Manager / researcher
  - Doing offensive and defensive work
- Previous talks
  - BlackHat USA, Asia and Europe, BSidesDC, Sector, Hackfest, NorthSec, Infosecurity Europe...
- I eat passwords and I’m bad at managing them

https://github.com/giMini

**PowerMemory**
Exploit the credentials present in files and memory

- PowerShell
  - ⭐️ 520
  - 🌐 142
So you want to be a hunter?
L2P noob

Hunting
You're doing it wrong
@pabraeken
So you want to be a hunter?

L2P noob
Spearfishing != Spearphishing

Knowledge is important

- Behavior of the shark
- Pattern of the attack
- Don’t let a bloody fish ruin your day
The CYBER™ kill chain

In theory

Phases of the Intrusion Kill Chain

- **Reconnaissance**
  - Research, identification, and selection of targets
  - Pairing remote access malware with exploit into a deliverable payload (e.g., Adobe PDF and Microsoft Office files)

- **Weaponization**
  - Transmission of weapon to target (e.g., via email attachments, websites, or USB drives)

- **Delivery**
  - Once delivered, the weapon’s code is triggered, exploiting vulnerable applications systems

- **Exploitation**
  - Outside server communicates with the weapons providing “hands on keyboard access” inside the target’s network.

- **Installation**
  - The weapon installs a backdoor on a target’s system allowing persistent access

- **Command & Control (C2)**
  - Command channel for remote manipulation of victim

- **Actions on Objective**
  - With hands on keyboard access, attacker accomplishes their original goal

Lockheed Martin’s Cyber Kill Chain® and Intelligence Driven Defense™ services identify and prevent cyber incursions. The services monitor what the adversaries must complete in order to achieve their objective.

In theory
The CYBER TM kill chain

In theory

Carbon Black.

STOPS MIMIKATZ
Persistence

- Startup folder LoL / Logon
- Registry (Run/RunOnce...)
- Scheduled tasks
- Services
- WMI subscription
- Drivers
- LSA providers
- Explorer
- Internet Explorer
- AppInit_DLL
- Network Providers
- Boot Execute
- Print Monitors
Persistence tricks
Hiding persistence

• Make sample inaccessible
  • ADS
  • Special folders (CLSIDs or this trick →
• Make registry keys inaccessible
• Make registry keys hard to spot
• Hide behind legitimate applications
• Hide code in the registry

Remember?
CON, PRN, NUL, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9, COM1, COM2, COM3, COM5, COM6, COM7, COM8, COM9)
Persistence
That escalates quickly

• Abusing shim databases
• COM hijacking
• User-triggered persistence
  • Spora
  • shortcut hijacking
  • handler hijacking
Attackers think in graph

Change your mindset

“Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.”

John Lambert
GM, Microsoft Threat Intelligence Center

@pabraeken
The CYBER™ kill chain @xme

In real life: incidents are non linear, they make mistakes

@pabraeken
The CYBER™ kill chain @xme

In real life: incidents are non-linear, they make mistakes
How to hunt?
A typical hunting day

- Find suspicious activity
- Search for suspicious activities
- Filter out legitimate activities
- Figure out the threat
- A threat is discovered
- Scoping the attacks
- Remediate the threat
- Update defenses

Hunt | Deep analysis | Investigate | Respond | Improve

@pabraeken
You think you have a life?
Getting ready for the week-end?

@pabraeken
Skype first meeting
Skype never works

<table>
<thead>
<tr>
<th>Hi, Who just joined?</th>
<th>Can You email that to everyone?</th>
<th>____ are you there?</th>
<th>Uh, ______, you’re still sharing...</th>
<th>Hi guys, I have to jump on another call</th>
</tr>
</thead>
<tbody>
<tr>
<td>(sound of someone typing, possibly with a hammer)</td>
<td>(Loud, painful echo/feedback)</td>
<td>(child or animal noises)</td>
<td>Hi, can you hear me?</td>
<td>No. It’s still loading</td>
</tr>
<tr>
<td>Next Slide. Please</td>
<td>Can Everyone go on mute?</td>
<td>I’m sorry. I was on mute.</td>
<td>(for overtalkers) Sorry, go ahead with what you wanted to say</td>
<td>Hello? Hello?</td>
</tr>
<tr>
<td>So ... (faded out) I can ... (undistinguishable) By... (cuts out) Ok?</td>
<td>Sorry I’m late (insert lame excuses)</td>
<td>I have a hard stop at ...</td>
<td>I’m sorry, you cut out there</td>
<td>Can we take this offline?</td>
</tr>
<tr>
<td>I’ll have to get back to you</td>
<td>Can everyone see my screen?</td>
<td>Sorry, I was having connection issues.</td>
<td>I think there’s a lag</td>
<td>Sorry, didn’t catch that. Can you repeat?</td>
</tr>
</tbody>
</table>

@pabraeken
Skype first meeting
Skype never works

Hello ?

Hello ?
And now it happens

...
Oh they have a SIEM?

Do you feel more secure now?
Got in a security incident?

Ok bro, let’s start the agent installation process...

@pabraeken
Got in a security incident?
Ok bro, let’s start the agent installation process...

ONE MILLION DOLLARS

@pabraeken
Wake up
Hunt without an agent

• Objectives
  • Hunt from the get-go
  • Quick answers
  • No installation, minimal impact to hunted systems
  • No uninstallation
  • Nice output
1. The victim clicks on a http link
2. Macro LULZ
3. In memory, PowerShell drop the malware

- Attempt local privileges *escalation*
- Domain reconnaissance
- Lateral movement

To persist on the infected system, the malware creates a WMI subscription

@pabraeken
BRACE YOURSELF

IT'S A LIVE DEMO

@pabraeke
Take away

1. https://github.com/giMini/NOAH
2. Installation is EZ (Docker)
3. It’s hunting without the pain of agent deployment
Thank you!

Pierre-Alexandre Braeken
@pabraeken
https://github.com/giMini