Tracking the attacker’s account activity

Chema García
josemaria.garcia@thiber.org
@sch3m4
https://github.com/sch3m4
Who am I?

Member and co-founder of THIBER, the Spanish cybersecurity think tank.
Independent security researcher & freelance
Open source developer & contributor
SANS Certified
+10 years of experience
- Pentesting
- Development
- DFIR
Incident Response / Threat Hunting

Time!

• Detect
• Identify
• Isolate
• Analyze
• Mitigate
• Report
Scenarios

- Something spreading all over your network
  - Malware campaign
  - Insider script
- Installing backdoors
- Stealing confidential information
  - Business Intelligence
  - Customer’s data
- Insider hijacking user accounts
Sample Scenario

• Monday in the morning
  • Someone found an availability issue within some dozens of computers

• Thursday in the morning
  • Hundreds of computers get affected
  • Lot of affected computers didn’t throw up an alert
  • The scope is unknown.

• IR Team involved
Analysis

- Different malware samples
- Use of “legit” tools
- Different propagation methods
- Common points:
  - WMI
  - PowerShell
  - SMB
- A logon event is generated before each infection
Analysis / Problems

- No SIEM at all
- Default audit policy
- PowerShell v2
  - No logs
Analysis / Problems

- IR Team is required to obtain the attack scope
- Evidences:
  - EVTx log files
  - 22.5 GB!!

Folder containing log files
Analysis / Tracking Logons

• Logon Events:
  • EVENT_WORKSTATION_UNLOCKED = 4801
  • EVENT_SCREENSAVER_DISMISSED = 4803
  • EVENT_LOGON = 4624
  • EVENT_LOGON_EXPLICIT = 4648
  • EVENT_SESSION_RECONNECTED = 4778
Analysis / Tracking Logons

- Logoff Events:
  - EVENT_WORKSTATION_LOCKED = 4800
  - EVENT_SCREENSAVER_INVOKED = 4802
  - EVENT_SHUTDOWN = 4609
  - EVENT_LOGOFF = 4634
  - EVENT_SESSION_DISCONNECTED = 4779
  - EVENT_LOGOFF_INITIATED = 4647
Analysis / Tracking Logons

• Session ID

```xml
<Data Name="TargetLogonId">0x0000000000172355</Data>  
<Data Name="LogonType">2</Data>  
<Data Name="LogonProcessName">User32</Data>  
<Data Name="AuthenticationPackageName">Negotiate</Data>  
<Data Name="WorkstationName"></Data>  
<Data Name="LogonGuid">{31531284-0000-0000-0000-000000000001}</Data>  
<Data Name="TransmittedServices"></Data>  
<Data Name="LnPackageName"></Data>
```

• Not valid for different computers
• Not valid for different domains
Analysis / Tracking Logons

• Generating a new TrackingID across domains:
  • Logon ID
  • Computer
  • Domain
  • User SID

• TrackingID:
  • SHA1( LogonID + ‘|’ + Computer + ‘|’ + Domain + ‘|’ SID)
Analysis / Tracking Logons

• Detecting low-profile hijackers

• SrcTrackingID:
  • SHA1( SrcLogonID + ‘|’ + SrcComputer + ‘|’ + SrcDomain + ‘|’ SrcSID)
Analysis / Findings

- Hijacked accounts
- Targeted computers
- Computers relations
- Domains relations
- Session duration
- ...

[Image of a complex network diagram]
Analysis / HowTo

• Set up the environment

https://github.com/THIBER-ORG/UserLine
Analysis / HowTo

• Index your .evtx log files

https://github.com/THIBER-ORG/UserLine
Analysis / HowTo

• Run UserLine

https://github.com/THIBER-ORG/UserLine
Analysis / HowTo

- Save all logon info

https://github.com/THIBER-ORG/UserLine
• Read the report

https://github.com/THIBER-ORG/UserLine
Analysis / HowTo

• Visualize the data

https://github.com/THIBER-ORG/UserLine
Analysis / HowTo

- Index the data if you need it
Demo Time!

https://github.com/THIBER-ORG/UserLine
Thank you all!

https://github.com/THIBER-ORG/UserLine

Chema García
✉️ javanuki.garcia@thiber.org
🐦 @sch3m4
🔗 https://github.com/sch3m4