Fileless attacks, persistence methods and how to hunt them

Douglas Santos
Security Strategist

Definition of Fileless

What defines fileless attacks ?

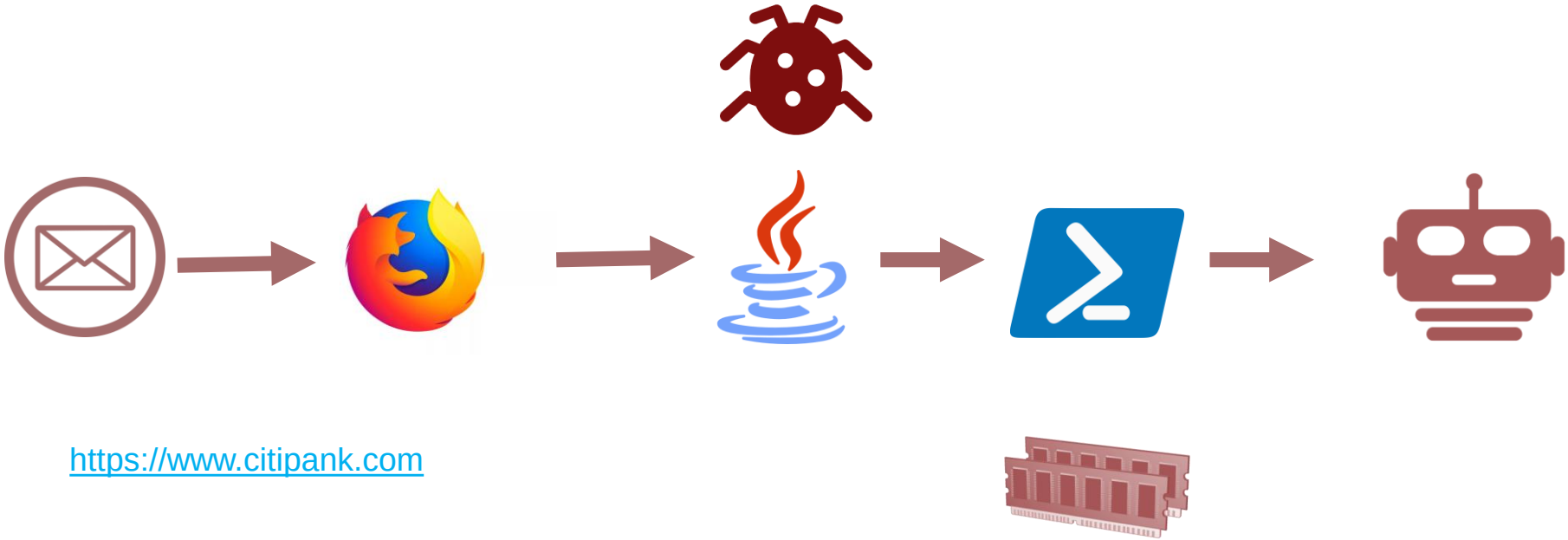
- Malicious code running on a system that …
  - Did not installed anything
  - Did not dropped anything to disk
  - Usually does not have it’s own process
  - Also called ”memory-based”, “living of the land”, “zero-footprint”
  - It uses oldschool techniques for code injection into processes
    - Classic DLL File Injection
    - Reflexive DLL Injection
    - Process Hollowing
    - Thread Execution Hijacking
    - …

Google Searches Trends on “fileless malware”

It’s a new thing right ?

- Not entirely, some tools/features have given the attack a new twist
    - Powershell specifically
    - WMI
- There are types of fileless attacks , some of them are :
    - Memory-Resident Only
    - Fileless Persistence Methods
    - Malicious Use of System tools
    - Non-PE Based (CoffeShot / JScript)

How does it work ?

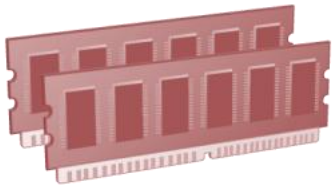


https://www.citipank.com

Early Fileless

Early Fileless Attacks

- Let's take a walk down memory lane …
    - Code Red (July 12th 2001)
        - IIS Vulnerability .ida ISAPI
        - ~6 million systems infected
    - SQL Slammer (January 25th 2003)
        - Microsoft SQL 2000 servers
        - Doubled in size every 8 minutes
        - Took down routers
- They both were ***memory only*** viruses



SQL Slammer and Code Red

- Both leveraged vulnerabilities on software to inject malicious payloads
  - Buffer overflow vulnerabilities
- After exploitation of the vulnerability was done, all injected code :
  - Had functionality to carry on other attacks
  - Finding new systems, checking for vulnerabilities
  - Launching the exploit code against newly find systems
- First versions were non persistent
- Later versions included persistence mechanisms and RAT capabilities

New Fileless

Examples

Poweliks Trojan - 2014

- Initially started as a click fraud trojan (drive-by exploit kits)
- Evolved from being a file-based threat (Wowlinks) to fileless :
  - Shared code included to connect to C2
  - Delete files
  - Hijack CLSID
- Once foothold is gained in a system the malware :
  - Silently visits web pages in a hidden browser window
  - Displays ad on the hidden window as well
  - More malware usually flows through these ad networks
  - Actually installed Windows Updates
  - Starts up watchdog to check if system is being cleaned
  - Persistency with JavaScript loading encoded shellcode from registry
  - Cool trick with the NULL Runkey

Powersniff Trojan - 2016

- Generally arrives in macros in Office documents through Malspam
- In general the emails were targeted
- Macro when enabled and executed calls WMI which :
  - Calls a powershell process
  - With execbypass
  - On a hidden windows
  - Downloads a Powershell file
    - Contains shellcode that is encrypted
    - Same script decode and executes the payload
    - Then perform reconnaissance activities
    - Looking for POS machines

POSHSPY Trojan - 2017

- Research point to APT29 for attribution (Cozy Bear)
- Makes extensive use of native Windows tools (living of the land)
- Use WMI to store and persist the infection
  - Leverages a filter to execute it’s payload
  - WindowsParentalControlsMigration Consumer
    - Upon execution, extracted and executed encoded powershell
- Extensive use of evasion mechanisms
  - Infrequent beaconing
  - Traffic obfuscation
  - Extensive encryption

How to hunt for them

Sysmon

- Process Creation and Termination
- Process changing a file creation time.
- Network Connection
- Driver Load
- Image Load
- CreateRemoteThread
- Raw Access Read of a file
- A process opens another process memory
- File Creation
- Registry Events
- Pipe Events
- WMI Permanent Events

OSQuery

- Exposes operating system details as relational tables
- Allows for deep monitoring of system level details
- Versions exists for MacOS, Windows, Linux and FreeBSD
- Growing community, stable codebase, backed by Facebook
- Allows for scheduled queries to be run
- Differential Logging
- File Integrity Monitoring
- YARA for in Memory Hunting
- Query Packs
- Kolide/Doorman/Fleet are solutions that allows scaling

Powershell Tools and Other Tools

- PSSysmonTools
- PSHunt
- PSReflect (Get-Injected-Thread / GetMemorySegment)
- UpRoot
- PowerForensics
- SeatlBelt
- Flare-WMI / python-cim
- RedLine
- Volatility

Windows Configuration and Logging

- PowerShell constrained Mode
- Script Tracing and Logging
- Powershell Transcripts

Demo Time

- Use Metasploit to serve a web page with an exploit
- Old exploit ms11_003, targeting Windos 7 SP1
- The idea is to just inject shellcode in memory
- Then use powershell to identify suspicious threads
- Dump that thread
- Open that up in IDA


FORTINET