Windows Malware Investigations

[no assembly required]

BLACK HILLS
Information Security

“We were targeted by a sophisticated, advanced persistent threat.”

~Recently Breached Company [press release]

[for sale...“ocean front property” in Arizona]

“Most hackers suck.”

~A Reynolds [VP of IT]

[“You still want to buy our AI/ML, next-gen EDR...right?”]

Agenda/Schedule

[Session Length: 1 hour]

- Introduction
- Presuppositions & Context
- Investigative Workflow
- Technical Possibilities
- References/Contact
- Q&A

“it is futile to do with more things that which can be done with fewer”

~W Occam

Patterson Cake

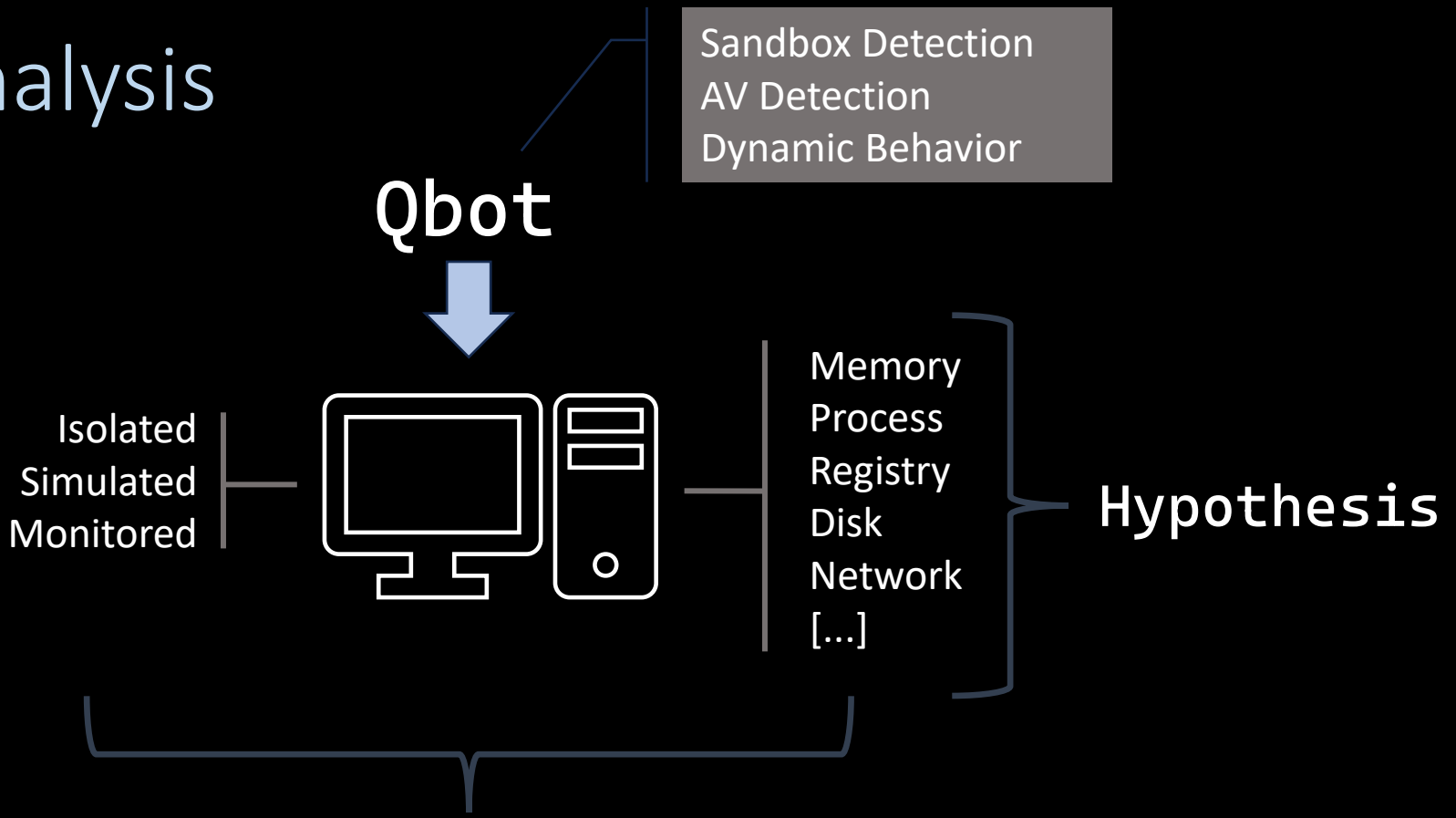
DFIR Consultant

Win-Mal Investigations:

- Why? = ACTIONABLE INTELLIGENCE
- When? = Alert/Event Investigations
- Where?

[...horses not zebras...]

Malware Analysis



["this is not a virtual machine...no, seriously"]

Malware Analysis

["the world, as it is, is vexing enough"]

Malware Commonalities

- Initial Access (point of impact)
- Actions on Objective (do something)
- Network Communications (command and control)
- Evade detection (obfuscation, LOL, etc.)
- Persistence (survive a reboot)

[...horses not zebras...]

Most Common Threats (Recent)

- Qbot
- SocGholish
- Raspberry Robin
- Gootloader
- Spongy Weasel
- Yellow Cockatoo

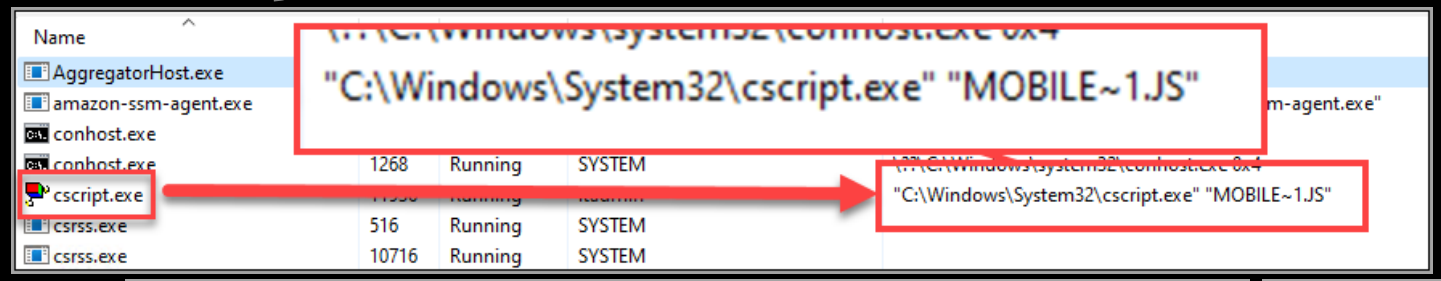
“Red Canary – Intelligence Insights & Threat Intelligence Reports”

Malware Commonalities

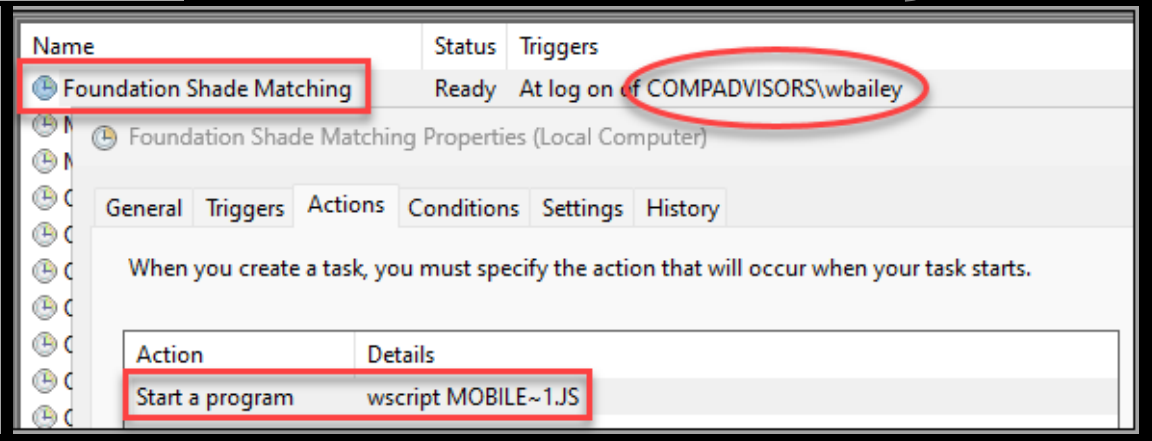
- Initial Access: SEO Poisoning, Malvertising, Drive-By's
  - File Types: .zip, .rar, .iso, .vhd, .lnk, .msi
- Actions on Objective: staging & initial enumeration
  - Execution: wsript, cscript, powershell, cmd, rundll32
- Network Communications: outbound tcp/https
- Evade detection: LOLBINS, disable endpoint protections
- Persistence: scheduled tasks, registry, startup folder

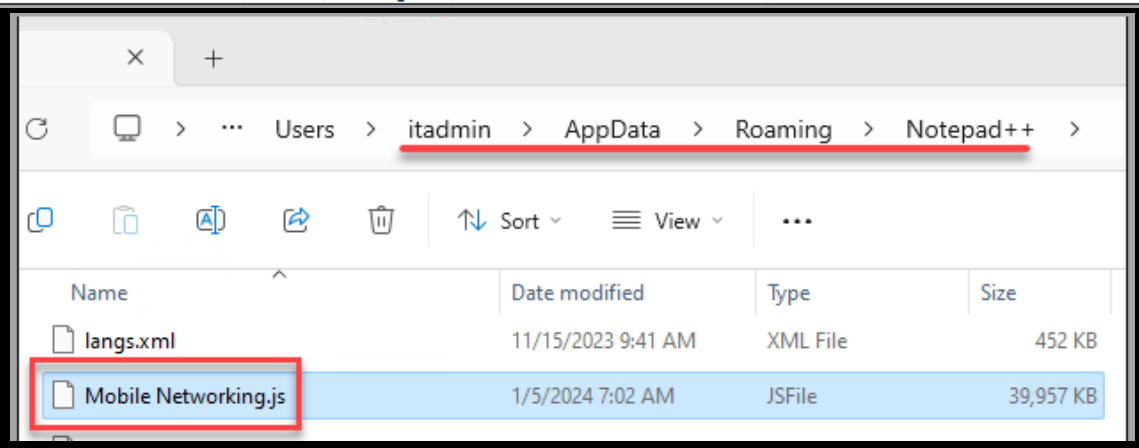
[defenders must be right 100% of the time...attackers only once]

[memory]

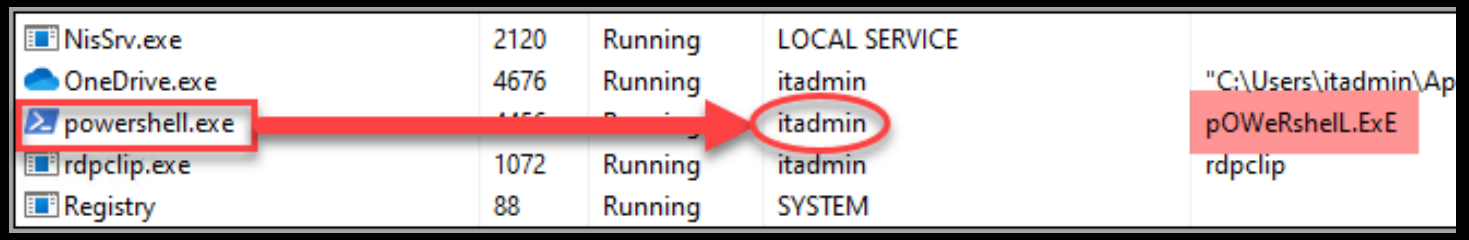


[identity]





[disk]




```
PS C:\Users\itadmin> netstat -ano | findstr /i "4456"
  TCP    172.31.47.48:56308     89.42.211.237:443      ESTABLISHED     4456
PS C:\Users\itadmin> netstat -ano | findstr /i "4456"
  TCP    172.31.47.48:56308     89.42.211.237:443      ESTABLISHED     4456
PS C:\Users\itadmin> netstat -ano | findstr /i "4456"
  TCP    172.31.47.48:56308     89.42.211.237:443      ESTABLISHED     4456
```

[network]

Technical Possibilities…

- PowerShell One-Liners [EDR?]
- PowerShell One-Liners w/Excel Diff
- Velociraptor Offline [parsed]*
- Velociraptor Offline w/Excel Diff*

*[small but mighty...and easy to transfer]

Windows Malware Investigation - Artifacts

- Select Artifacts {actionable intelligence!}
  - Network Connections (netstat, dns)
  - Disk (MFT)
  - Running Processes (pslist)
  - Persistence (services, tasks, startup items)

[collect...parse...reduce/refine]

Network Communications (C2) *

[gootloader]

```
oc.php","https://t        .tr/xmlrpc.php","https://bukhara-
php") | GeT-rANdom)}cATCH{};SleeP -S 20}
```

```
$timespan = New-TimeSpan -Minutes 1
$timer = [diagnostics.stopwatch]::startnew()
while ($timer.elapsed -lt $timespan){
$gettcpconnections = Get-NetTCPConnection | Where-Object state -ne "Bound" |`
Select-Object localaddress,localport,remoteaddress,remoteport,state,owningprocess,`
@{Name="process";Expression={(Get-Process -id $_.OwningProcess).ProcessName}} |`
 Export-Csv c:\users\security\Desktop\net-connect.csv -NoTypeInformation -Append
$gettcpconnections
start-sleep -seconds 3
```

[See https://github.com/secure-cake/win-mal-investigations/misc-powershell]

Disk (“Writeable”)*

```
    Directory: C:\ProgramData

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d----          11/15/2023  5:52 PM                Microsoft OneDrive
d----          11/15/2023  6:30 PM                Microsoft Visual Studio
d----           5/7/2022  5:24 AM                USOShared
d----          11/15/2023  7:12 PM                VMware

    Directory: C:\Users

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d----           2/2/2024  9:45 PM                Security
```

%userprofile$\appdata\..

```
Get-ChildItem -Directory -Recurse -Depth 1 -Force  C:\ -ErrorAction SilentlyContinue |`
where {(get-acl $_.fullname).access | where {($_.identityreference -eq 'rtw-win11-02022\security')`
-or ($_.identityreference -eq 'nt authority\authenticated users') -or`
($_.identityreference -eq 'builtin\users') -or ($_.identityreference -eq 'rtw-win11-02022\Users')`
-and ($_.filesystemrights -eq 'FullControl') -or ($_.filesystemrights -eq 'Modify')`
-or ($_.filesystemrights -eq 'Write')}}
```

[See https://github.com/secure-cake/win-mal-investigations/misc-powershell]

Running Processes (Memory)

```
name            : services.exe
executablepath  :
processid       : 748
parentprocessid : 628
commandline     :

name            : lsass.exe
executablepath  : C:\Windows\system32\lsass.exe
processid       : 796
parentprocessid : 628
commandline     : C:\Windows\system32\lsass.exe
```

Pid	Ppid	Name	CommandLine	Exe
4456	11936	powershell.exe	pOWeRshelL.ExE	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
Get-Wmiobject win32_process | select name,executablepath,processid,parentprocessid,commandline |`
export-csv c:\users\security\desktop\pslist.csv -NoTypeInformation
```

[See https://github.com/secure-cake/win-mal-investigations/misc-powershell]

Services

Name	State	DisplayName	ProcessId	StartMode	PathName
AJRouter	Stopped	AllJoyn Router Service	0	Manual	C:\Windows\system32\svchost.exe -k Loca
ALG	Stopped	Application Layer Gateway Service	0	Manual	C:\Windows\System32\alg.exe
AppIDSvc	Stopped	Application Identity	0	Manual	C:\Windows\system32\svchost.exe -k Loca

```
get-wmiobject win32_service | select name,state,displayname,processid,startmode,pathname,startname |`
export-csv c:\users\security\desktop\target-services.csv -NoTypeInformation
```

[See https://github.com/secure-cake/win-mal-investigations/misc-powershell]

Scheduled Tasks

HostName	TaskName	Author	Task To Run
RTW-WIN11-02022	\MicrosoftEdgeUpdateTaskMachineCore	N/A	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe /c
RTW-WIN11-02022	\MicrosoftEdgeUpdateTaskMachineCore	N/A	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe /c

```
schtasks /query /V /FO csv | convertfrom-csv | where taskname -ne "TaskName" |`
select hostname,taskname,'next run time',status,'logon mode','last run time',`
author,'task to run','start in',comment,'scheduled task state','run as user' |`
export-csv c:\users\security\desktop\baseline-tasks.csv -NoTypeInformation
```

[See https://github.com/secure-cake/win-mal-investigations/misc-powershell]

Running Processes [DIFF]

A	B	D	E	F
Pid	Ppid	Name	CommandLine	Exe
3496	728	vm3dservice.exe	C:\Wi…xe	C:\Windows\System32\vm3dservice.exe
3520	728	wlms.exe	C:\Wi…xe	C:\Windows\System32\wlms\wlms.exe
3528	728	Sysmon64.exe	C:\Wi…	C:\Windows\Sysmon64.exe
3544	728	svchost.exe	C:\Windows\System32\svchost.exe -k netsvcs -p -s WpnService	C:\Windows\System32\svchost.exe
3732	728	svchost.exe	C:\Windows\System32\svchost.exe -k netsvcs -p -s SharedAccess	C:\Windows\System32\svchost.exe
2396	856	unsecapp.exe	C:\Windows\system32\wbem\unsecapp.exe -Embedding	C:\Windows\System32\wbem\unsecapp.exe
4668	3336	AggregatorHost.exe	AggregatorHost.exe	C:\Windows\System32\AggregatorHost.exe
4372	728	svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -s RmSvc	C:\Windows\System32\svchost.exe

Green = Match
Yellow = Unique

Target | Baseline

I ♥ Excel

Conditional Formatting Rules Manager

Show formatting rules for: This Worksheet

New Rule... | Edit Rule... | Delete Rule | Duplicate Rule

Rule (applied in order shown)	Format	Applies to
Formula: =COUNTIF(Baseline!$D$1:$D$250,D1)=0	AaBbCcYyZz	=$D:$D
Formula: =COUNTIF(Baseline!$D$1:$D$250,D1)>0	AaBbCcYyZz	=$D:$D

Windows Malware Investigation - Artifacts

- Select Artifacts {actionable intelligence!}
  - Network Connections (netstat, dns)
  - Disk (MFT)
  - Running Processes (pslist)
  - Persistence (services, tasks, startup items)

[collect...parse...reduce/refine]

Windows Malware Investigation Collection

- **Velociraptor Offline Collector**
  - Artifacts
    - KAPE [MFT, AV Logs, PowerShell Console/Transcripts]
    - Netstat Enriched
    - DNS Cache
    - Services
    - TaskScheduler (w/upload)
    - StartupItems
    - PSList

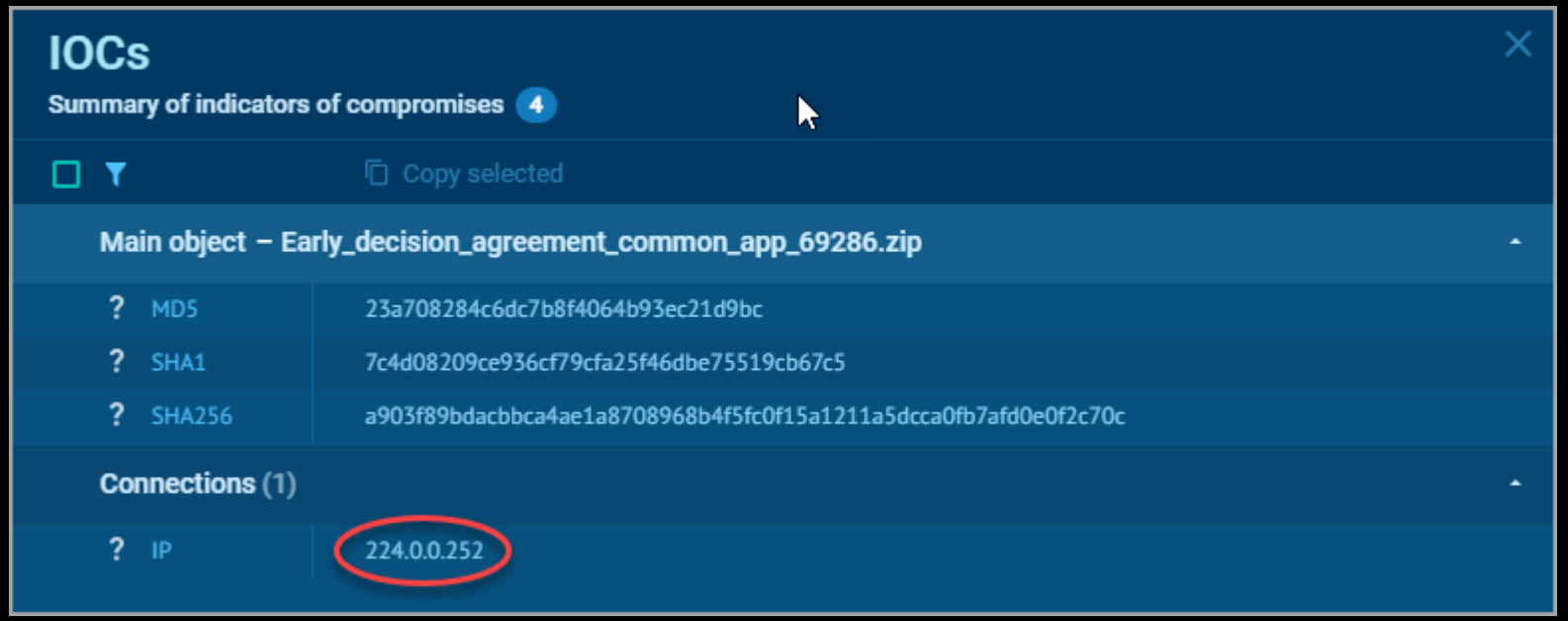
[See https://github.com/secure-cake/win-mal-investigations]

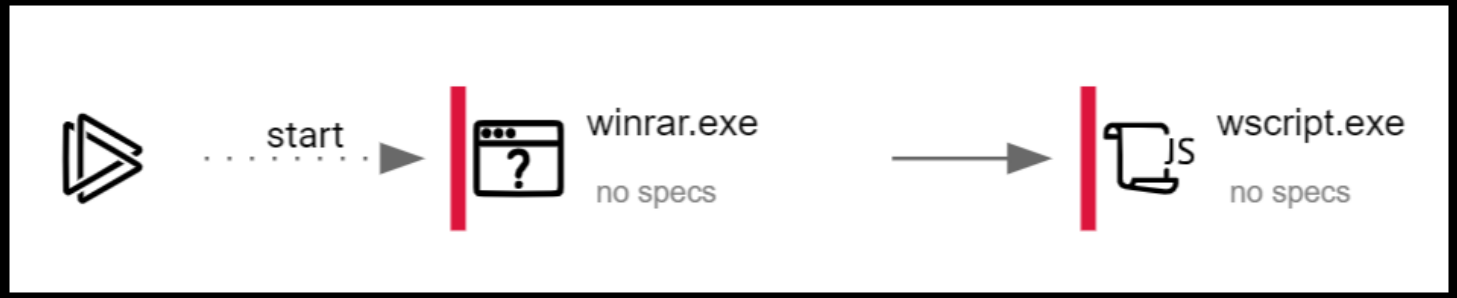
Win-Mal Investigation - WORKFLOW

- Create “win-mal” Velociraptor Collector*
- Distribute/execute “win-mal” collector on “baseline” system*
- Distribute/execute “win-mal” collector on “target” system
- Stage “win-mal” data on analysis system
- Run “WinMal_Target_Baseline_Excel.ps1” script
- Open Excel combined workbook
- Create Excel “automations”*
- Review “unique” artifacts from “target” system

[See https://github.com/secure-cake/win-mal-investigations]

Sandbox Analysis #1 [FINDINGS]



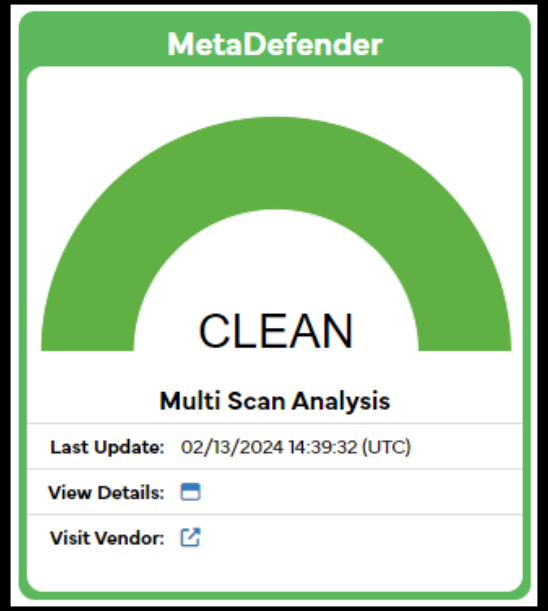


[224.0.0.252?]

Sandbox Analysis #2 [FINDINGS]

Last update: 02/13/2024 14:39:20 (UTC)

Huorong	✓	Bitdefender	✓
Avira	✓	Zillya!	✓
Sophos	✕ Troj/DrodZp-CL	Vir.IT eXplorer	✓
VirusBlokAda	✓	K7	✓
McAfee	✓	NETGATE	✓
TACHYON	✓	Varist	✓
Kaspersky	✓	Antiy	✓
AhnLab	✓	Lionic	✓
Webroot SMD	✓	Emsisoft	✓
NANOAV	✓	RocketCyber	✓
Comodo	✓	ESET	✓
ClamAV	✓	Cylance	✓



`Indicators = encoded JavaScript`

`["malicious"]`

Win-Mal Investigations [FINDINGS]

- Netstat: x1 IP [suspicious]
- Pslist: x1 process [malicious]
- Services: x0
- Startup: x0
- Tasks: x1 task [malicious]
- DNS: x4 A Record [malicious/suspicious]

x7 IOC's – "malware is not magic" ~Cake

WinMal Technical Possibilities...

- Collect:
  - PowerShell
  - EDR
  - Velociraptor
  - Other...
- Parse (Process):
  - Excel (Automate)
  - OpenOffice Calc
- Reduce/Refine:
  - Diff w/baseline (Excel)

[See https://github.com/secure-cake/win-mal-investigations]

Q&A

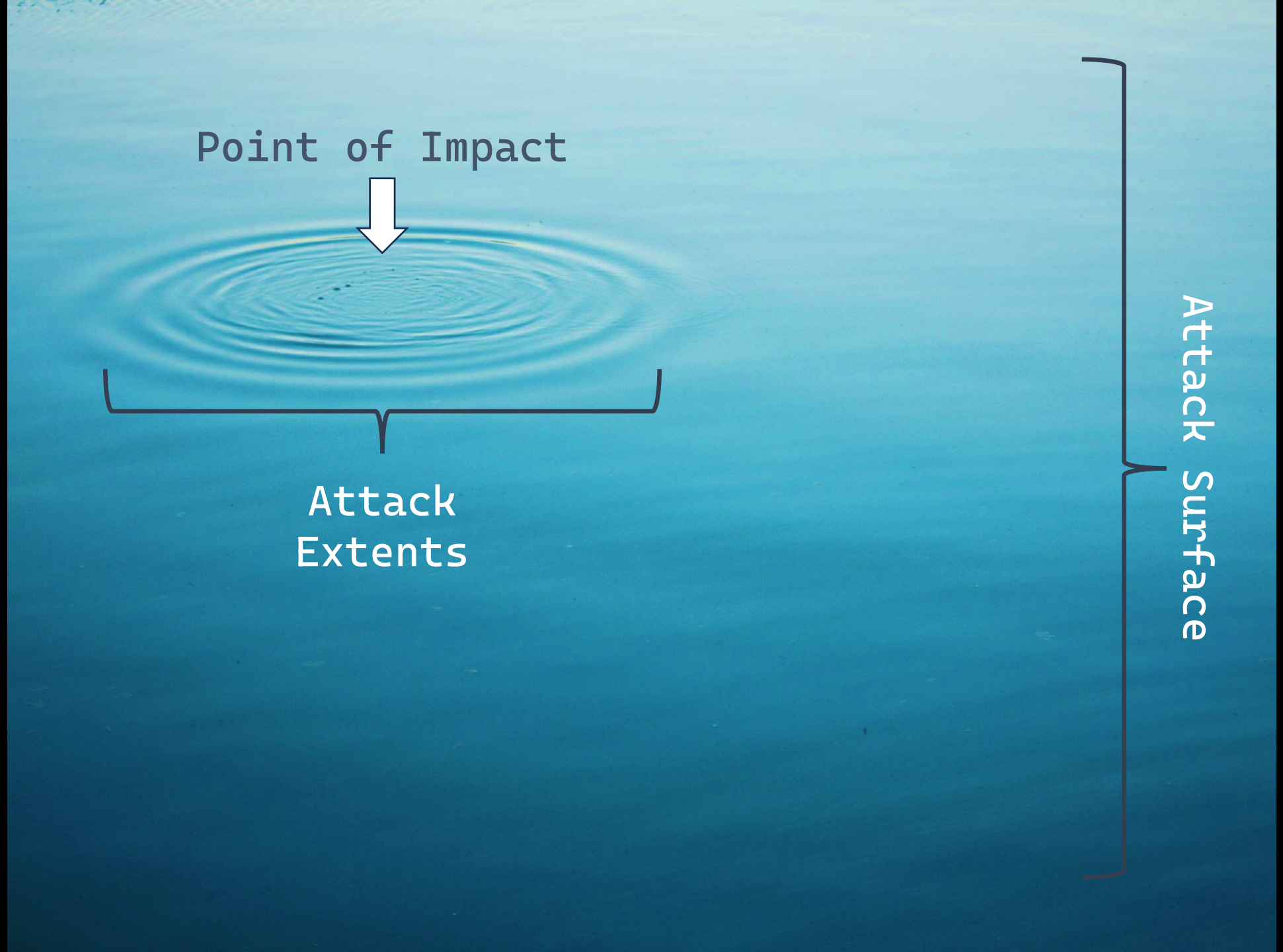
Patterson Cake

@SecureCake

github.com/secure-cake

patterson@blackhillsinfosec.com

Thank you!


Point of Impact
Attack
Extents
Attack Surface

Detection → Analysis → Containment → Eradication → Recovery

Attack Surface → Indicators → Capabilities

Point of Impact

- [application]
- [identity]
- [endpoint]
- [network]
- [third party]
- [other]

- [memory]
- [identity]
- [network]
- [disk]

- [EDR]
- [Antivirus]
- [Proxy]
- [SIEM]
- [Firewalls]
- [Azure/M365]
- [OS Tools]
- [..]

Visibility & Containment

[frameworks: broadly-applicable guidelines upon which to build something useful]