POWERED BY
BLACK HILLS
Information Security

RAPID ENDPOINT INVESTIGATIONS

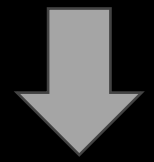
Linux and Mac Edition

AGENDA

[Session Length: 1 Hour]

- Introduction
- Context
- Causality
- Tools and Techniques
- Contact/Q&A

“close enough for horseshoes and hand grenades”



...simple, effective, repeatable...

Patterson Cake

IR Contrarian

The future of security...

ENDPOINT & IDENTITY

everything we care about happens on an endpoint, in the context of an identity

ENDPOINT & IDENTITY

ENDPOINT = ?

- Operating System
- User Interface
- Apps/Services/Data
- Hardware (Compute/Storage)
- Network Attached*

ENDPOINT = ?

- Operating System
- User Interface
- Apps/Services/Data
- Hardware (Compute/Storage)
- Network Attached*

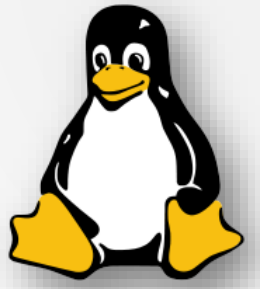
OS = Windows vs Linux vs Mac?

By the (approx.) numbers...

- Business Desktops = Windows (85%)
- Servers = Linux (75%)
- Other = Mac (Business Desktops 10%)

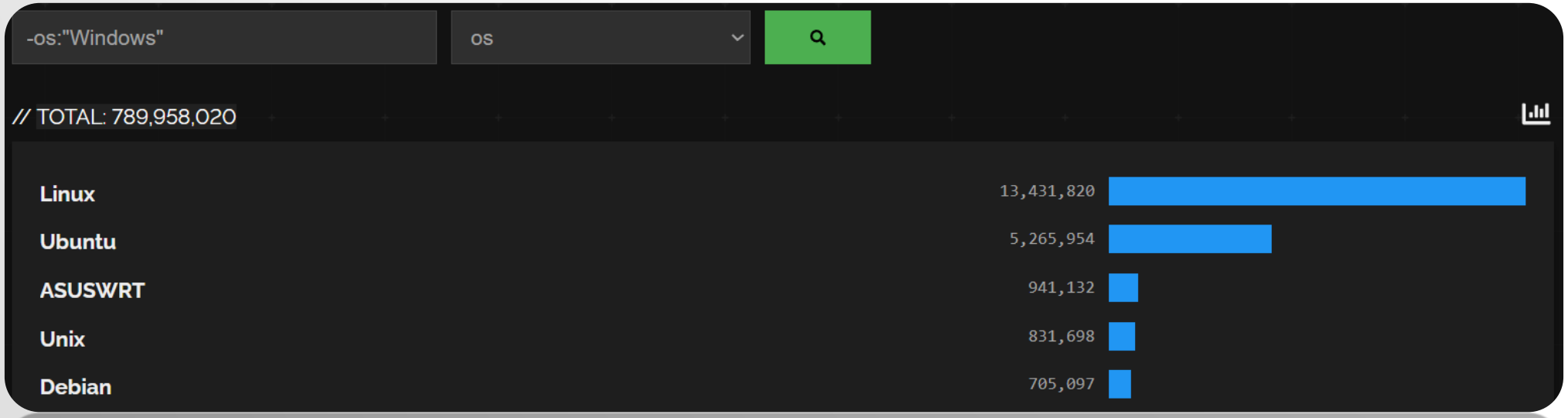
[...prevalence and primary use case...]

Linux “Use Cases”



Approximately…

- Web Servers = 75%
- Cloud Infra = 90%+
- Supercomputers = 100%



Endpoint Investigations: Linux

Approximately…

- 50 million+ lines of code
- 229,438 man pages
- 10K-50K Configuration Files
- 1M – 5M forensic artifacts
- A gazillion needles

Rapid Endpoint Investigations: Linux

Approximately…

- 50 [illegible]n+ [illegible] of code
- 229,4[illegible] pages
- 10K [illegible]uration Files
- 1M – 5M forensic artifacts
- A gazillion needles

10 ARTIFACTS

Initial Access: ssh

Network Communications: Outbound TCP/IP - HTTP/HTTPS

Detection Evasion: n/a, “doppelgangers?”

Actions on Objective: resource utilization
crypto mining – outbound ssh attacks – other outbound attacks

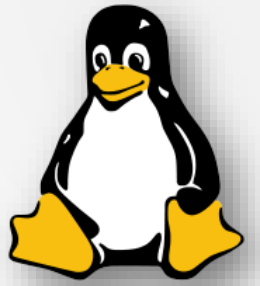
Persistence: cron – config – ssh

THREAT COMMONALITIES*

how & where threats impact endpoints

[causality: cause and effect]

ENDPOINT ATTACK SURFACE



50+ MILLION LINES OF CODE

Initial Access: ssh

Network Communications: Outbound TCP/IP - HTTP/HTTPS

Actions on Objective: resource abuse

Persistence: cron – config – ssh

MEMORY – IDENTITY – NETWORK - DISK

PROCESSES – SOCKETS – WRITEABLE DIRS – CRON – SERVICES – SSH CONFIG

"prioritized assessment of need and allocation of [limited] resources for maximum effect"

RAPID TRIAGE WORKFLOW

- What questions are you trying to answer?
- What artifacts will help you answer those questions?
- How will you perform CPR [collect-parse-reduce/refine] to derive actionable intelligence?

RAPID TRIAGE WORKFLOW

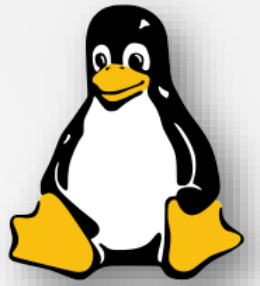
"do what you can, with what you have, where you are" ~T Roosevelt

- Select Artifacts [prioritized]
- Acquire Artifacts [point of impact]
- Parse Artifacts [rapidly]
- Analyze Artifacts [start from event context]
- Identify IOCs [m...i...n...d]
- Expand Context [find attack extents]
- Contain [from attack extents]

COLLECT...PARSE...REDUCE/REFINE

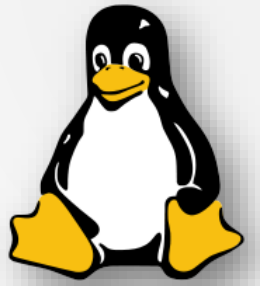
"rapid triage = performing CPR"

Linux Artifacts



- running processes
- network sockets
- shell history
- critical config files
- crontab
- systemdlist/init.d/services
- executable files
- ssh auth/access
- writable/executable dirs.
- executable files w/hashes

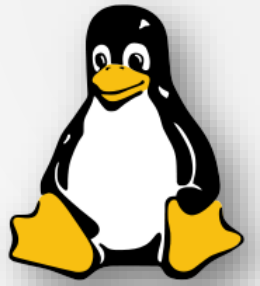
“These are the artifacts you’re looking for.”



- Collect:
  - Velociraptor Offline
  - Unix-Like Artifact Collector (UAC)*
- Parse: [..]
- Reduce/Refine: Excel/Calc...Text Editor...WSL(grep)

COLLECT...PARSE...REDUCE/REFINE

"rapid triage = performing CPR"

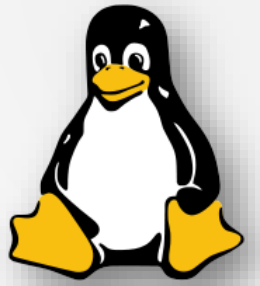


- Velociraptor Offline Collector :
  - Linux.Collection.CatScale
  - Misc (optional)
- Features/Functions:
  - Broadly Compatible “MUSL” executable
  - Local ZIP creation w/cloud upload option
  - Easy to pre-stage/test/pre-deploy [no infra required]
- Execution:
  - Execute as “root” (sudo)
  - Run via ssh/RMM (“Expect Script”)

COLLECT ARTIFACTS

[MUSL = C Standard Library for OS’s based on Linux Kernel]

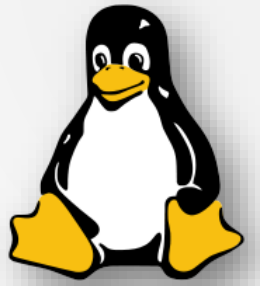
- Velociraptor Offline Collector :
  - Linux.Network.NetstatEnriched
  - Linux.Sys.Pslist
  - Linux.Sys.BashHistory*
  - Linux.Sys.Crontab
  - Linux.Sys.LastUserLogin
  - Linux.Sys.SSHLogin
  - Linux.Collection.CatScale
    - timeline
    - executables
    - log files
    - config files



COLLECT ARTIFACTS

[MUSL = C Standard Library for OS's based on Linux Kernel]

Reduce/Refine: Excel/Calc...Text Editor...WSL(grep)

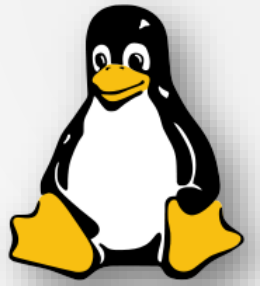


- Running Process
- Network Sockets
- SSH Logins
- Scheduled Jobs [cron]
- Executable content in world-writeable dirs [hash]

ANALYSIS WORKFLOW

TTPs: *Initial Access, Priv Esc, Persistence, C2/Lateral Movement, Actions on Objective*

Reduce/Refine: Excel/Calc...Text Editor...WSL(grep)



- Running Process
- Network Sockets
- SSH Logins
- Scheduled Jobs [cron]

"rtw-vr-linux-catscale.sh"

hostname-cron-tab.txt
hostname-established-connections.txt
hostname-pslist-unique-hashes.txt
hostname-ssh-auth-successes.txt

OUTPUT REVIEW

GitHub "Rapid Endpoint Investigations": *linux-mac*

OUTPUT REVIEW

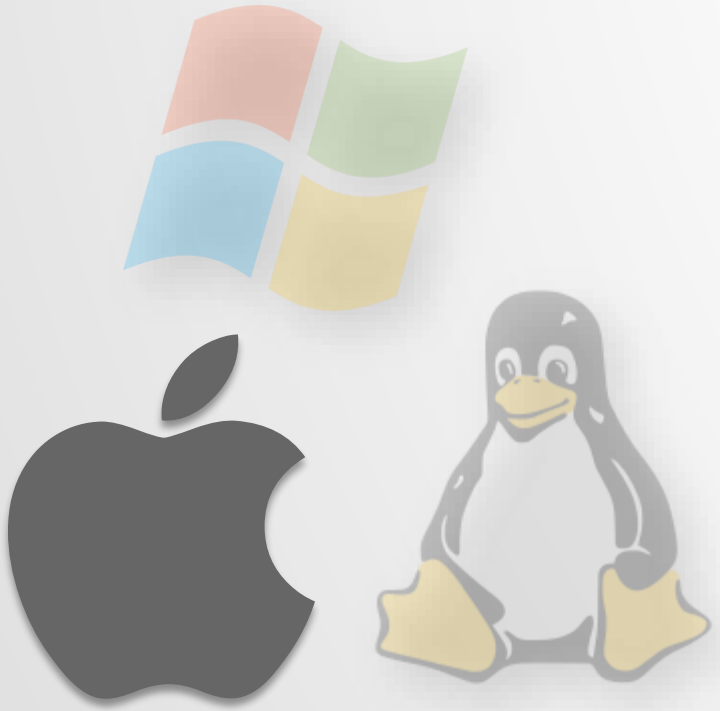
PSList JSON: 2,145 lines

User/binary/path/hash: 98 lines

```
"admin","(sd-pam)","/usr/lib/systemd/systemd-executor","fd0c6736f66c4d32a5342ad5ceb5d4f7536f155e"
"admin",".bisis","/var/tmp/.update-logs/.bisis","7940c6e29ab9cf6abe5e570f73eed93265962e1a"
"admin",".system3d","/tmp/.est1/.system3d","0f4b32d5374ef4efdfe015b8087bcda61b409494"
"admin","Update","/var/tmp/.update-logs/Update","a2101ec53fb0934b23f83c582d3a0bed9f66fd13"
"admin","bash","/usr/bin/bash","7ec5ea0b9805b4f43c7be78d27f262a5f51eddc0"
"admin","sshd","/usr/sbin/sshd","5464030446875a9d3342483dea9441768ae62c01"
"admin","systemd","/usr/lib/systemd/systemd","f7f2e64bd57370bdf3f9bf34f849460481bc415e"
"messagebus","dbus-daemon","/usr/bin/dbus-daemon","3ec52b7e768590dbd57c0bd4e76845970f84c1d4"
"polkitd","polkitd","/usr/lib/polkit-1/polkitd","949ce2a6badb45171e67bb2575255aeff03d97b0"
"root","(sd-pam)","/usr/lib/systemd/systemd-executor","fd0c6736f66c4d32a5342ad5ceb5d4f7536f155e"
"root","/usr/bin/python3","/usr/bin/python3.12 (deleted)",
"root","Collector-no-upload_v0.72.0-linux-amd64-musl","/root/utils/Collector-no-upload_v0.72.0-linux-amd64-
"root","ModemManager","/usr/sbin/ModemManager","aad36a970eee9d222ed8cbee14e91182b237d038"
"root","agetty","/usr/sbin/agetty","33a2[illegible]45d4fd8fa80549dfb194a4cd7ea15d11c34"
"root","bash","/usr/bin/bash","7ec5ea0b9[illegible]05b4f43c7be78d27f262a5f51eddc0"
"root","cpuhp/0","","da39a3ee5e6b4b0d325[illegible]bfef95601890afd80709"
"root","cron","/usr/sbin/cron","fa067730[illegible]65d3b788e719cba50c870aa43c22a27"
"root","droplet-agent","/opt/digitalocean/bin/droplet-agent","27448ff83d9ecd53968fbbb46c31df22d2c0fd57"
"root","ecryptfs-kthread","","da39a3ee5e[illegible]b4b0d3255bfef95601890afd80709"
"root","idle_inject/0","","da39a3ee5e6b4[illegible]0d3255bfef95601890afd80709"
"root","irq/9-acpi","","da39a3ee5e6b4b0d[illegible]255bfef95601890afd80709"
"root","jbd2/vda1-8","","da39a3ee5e6b4b0[illegible]3255bfef95601890afd80709"
"root","jbd2/vda13-8","","da39a3ee5e6b4b[illegible]d3255bfef95601890afd80709"
"root","kauditd","","da39a3ee5e6b4b0d323[illegible]bfef95601890afd80709"
```

".bisis","/var/tmp/.update-logs/.bisis", "7940c6e29ab9cf6abe5e570f73eed93265962e1a"
".system3d","/tmp/.est1/.system3d", "0f4b32d5374ef4efdfe015b8087bcda61b409494"
"Update","/var/tmp/.update-logs/Update", "a2101ec53fb0934b23f83c582d3a0bed9f66fd13"

OS = Windows vs Linux vs Mac?



By the (approx.) numbers...

- Business Desktops = Windows (85%)
- Servers = Linux (75%)
- Other = Mac (Business Desktops 10%)

Mac “Threat-Actor SoP”

- Initial Compromise = web lures/malvertising, supply chain, insider threat*
- Actions on Objective = info-theft (passwords, cookies, files)
- TTPs = AppleScript, osascript, dscl (LOOBin)

*NOTE: most common (IR Consulting “scope”)

Mac Artifacts

- running processes
- network sockets
- shell history (zsh, bash)
- critical config files
- launchd/crontab
- services/launchctl
- private:
  - web history (safari)
  - unified log
  - logs

Admin + “Full Disk” access required
(Remote Login = ssh)

- UAC:
  - Unix-Like Artifact Collector
- Features/Functions:
  - Broadly Compatible ~~executable~~
  - Local ZIP creation w/cloud upload option
  - Easy to pre-stage/test/pre-deploy
- Execution:
  - Execute as “root” (sudo)
  - Best with “Full Disk” permissions

COLLECT ARTIFACTS

[Mostly Scripts and YAML Files – though you can customize!]

Mac UAC Execution

UAC Workflow:

- Download UAC
- Copy the "uac-main.zip" to your target HOST
- Unzip "uac-main.zip" to your desired directory
- Set "uac" to executable
- Execute "uac" specifying profile, output naming, and output directory
- Copy the "uac" output to your analyst system

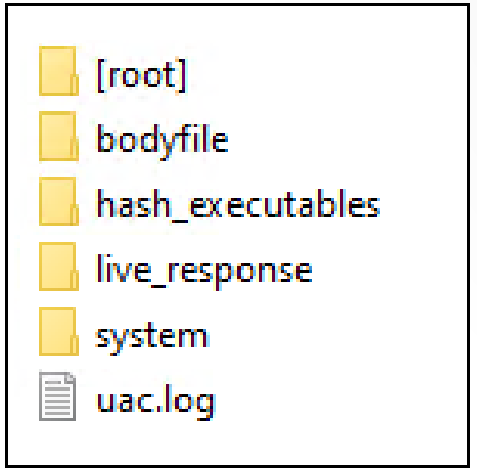
OPTIONS:

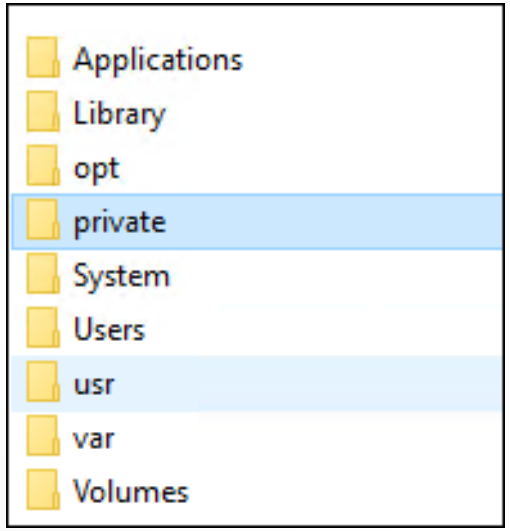
- You can also auto-upload results to S3
- You can use my “run_uac_full_upload.sh” script

https://github.com/secure-cake/malware-investigations/wiki

Mac UAC Artifacts

- running processes (live_response)
- network sockets (live_response)
- shell history (zsh, bash) [root]
- critical config files [root]
- launchd/crontab (live_response
- services/launchctl (live_response)
- private: [root]
  - web history (safari)
  - unified log
  - logs





Mac Artifacts

Web History (Safari)

UAC:

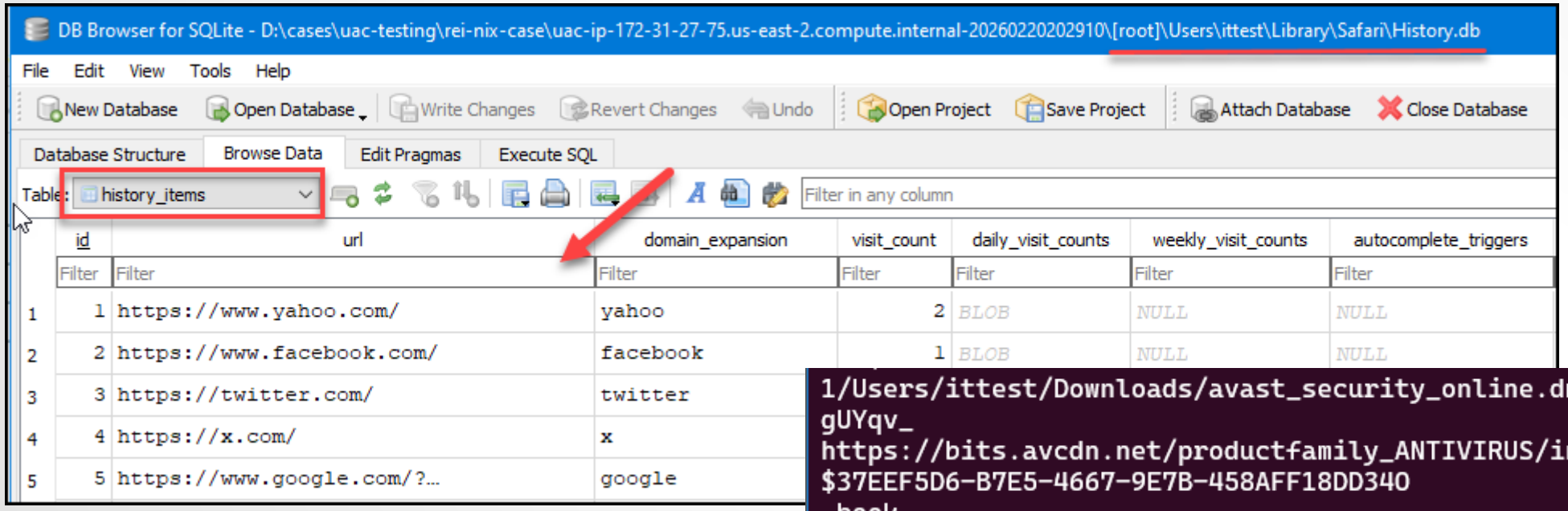
- [root]\Users\%username\Library\Safari:
  - History.db (DB Browser for SQLite)
    - History_items
    - History_visit
  - ..\Downloads.plist (strings)
- [root]\Users\%username\Downloads\?

NOTE: Admin + "Full Disk" access required (Remote Login = ssh)

Mac Artifacts

Web History (Safari): History.db\history_items

DB Browser (SQLite): ..\[root]\Uses\username\Library\Safari\History.db




```
1/Users/ittest/Downloads/avast_security_online.dmg3A
gUYqv_
https://bits.avcdn.net/productfamily_ANTIVIRUS/insttype_
$37EEF5D6-B7E5-4667-9E7B-458AFF18DD340
 book
0000000000
Users
ittest
Downloads
avast_security_online.dmg
```

strings: \[root]\Uses\username\Library\Safari\Downloads.plist

Mac Artifacts

Apple Unified Log

- UAC:
  - [root]\private\var\db\
    - uuidtext
    - diagnostics
      - Persist
      - Special
      - Signpost
      - HighVolume
      - Timesync

NOTE: Admin + “Full Disk” access required (Remote Login = ssh)

Mac Artifacts

Apple Unified Log

- UAC:
  - Mandiant Unified Log Iterator (download)

```
.\unifiedlog_iterator.exe -m log-archive -i ..\uac-collection-folder\ -o hostname-unified-log.csv -f csv
```

NOTE: Be patient (10-15 minutes)…several hundred MB of output!

https://cloud.google.com/blog/topics/threat-intelligence/reviewing-macos-unified-logs/

Mac Artifacts

Other (UAC)

- bodyfile:
  - uac-output\bodyfile\bodyfile.txt

```
log2timeline.py --parsers=mactime --storage_file output.plaso `
./uac-output/bodyfile/bodyfile.txt

psort.py -o dynamic output.plaso --slice "2026-02-20T19:00:00“ `
--slice_size 30  -w timeline-slice20260220-1904.csv
```

NOTE: Requires installation of “plaso-tools”

Mac Artifacts

- grep “all” – keyword list (uac-output parent folder):

echo keyword >> keywords.txt

grep -r -o -i -a --color=always --file=keywords.txt | sort | uniq –c | sort

```
  1 [root]/private/var/db/uuidtext/DF/ACD128E66B3C2F9795CD03311B4004:Monero
  1 live_response/packages/brew_list.txt:xmrig
  1 live_response/packages/brew_list_--formula.txt:xmrig
  2 [root]/private/var/db/diagnostics/Persist/0000000000000007.tracev3:xmrig
  2 system/hidden_directories.txt:xmrig
  3 [root]/private/var/db/uuidtext/DF/ACD128E66B3C2F9795CD03311B4004:XMRig
  3 [root]/private/var/db/uuidtext/DF/ACD128E66B3C2F9795CD03311B4004:monero
  4 hash_executables/hash_executables.md5:xmrig
  4 hash_executables/hash_executables.sha1:xmrig
 12 [root]/private/var/db/uuidtext/DF/ACD128E66B3C2F9795CD03311B4004:XMRIG
 17 [root]/private/var/db/uuidtext/DF/ACD128E66B3C2F9795CD03311B4004:xmrig
 63 bodyfile/bodyfile.txt:xmrig
118 bodyfile/uac-timeline-filtered.csv:xmrig
145 uac-timeline-slice1.csv:xmrig
```

Example Keywords: monero, xmrig, mindergate, ccminer, cryptotab, moneroocean

everything we care about happens on an endpoint, in the context of an identity

ENDPOINT & IDENTITY

how & where threats impact endpoints

[causality: cause and effect]

ENDPOINT ATTACK SURFACE

50+ MILLION LINES OF CODE

Initial Access: _____

Network Communications: _____

Actions on Objective: _____

Persistence: _____

MEMORY – IDENTITY – NETWORK - DISK

[ATTACK SURFACE – ARTIFACTS]

PROCESSES – SOCKETS – WRITEABLE DIRS – TASKS – SERVICES - RMM

RESOURCES

https://cake-labs.com/rtw (Rapid Triage Workflow)
https://cake-labs.com/rtw-nix (RTW Wiki - CatScale/UAC)
https://cake-labs.com/nixneedles (Linux CLI Reference)
https://cake-labs.com/needles (PowerShell One-Liners)

Patterson Cake

@SecureCake

github.com/secure-cake

patterson@blackhillsinfosec.com