Unveiling shadows: key tactics for tracking cyber threat actors, attribution, and infrastructure analysis

Hossein Jazi

Senior Threat Intelligence Specialist

Hossein Jazi

@h2jazi

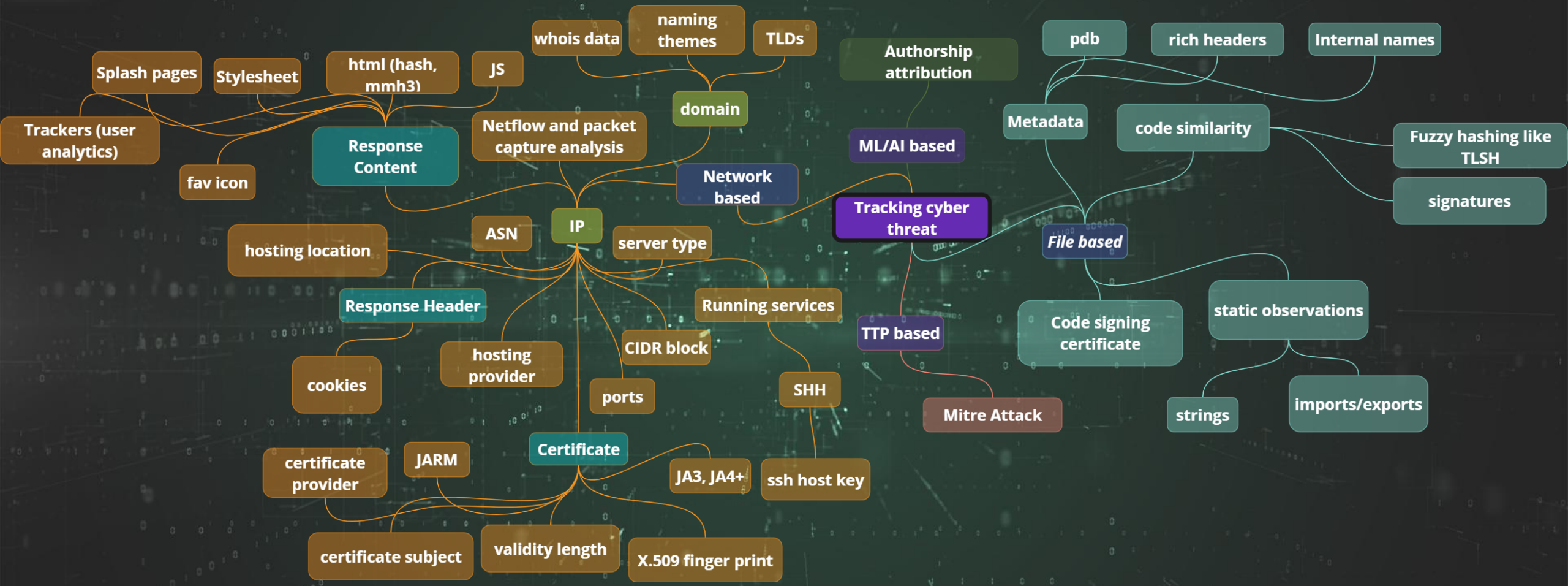
THREAT INTELLIGENCE SPECIALIST

- APT researcher
- Malware reverse engineer
- Threat Hunter
- Cyber crime investigator

APT Tracking

APT Tracking

High Level Detail



File-based Tracking

File-based Tracking

Static Indicators – Strings

DACLS RAT

- **Static Indicators:**
  - Extracted from static analysis of a toolset or malware used by threat actors.
- **Key use:**
  - Identifying and tracking malware variants associated with specific threat actors.
- **Specific Strings:** Unique strings within the malware can serve as indicators to detect and link new variants to known threats.
- **DACLS RAT:**
  - Certificate name and private key
  - “c_2910.cls” and “k_3872.cls,”

File-based Tracking

Static Indicators – Imports/Exports

IMPORTS/EXPORTS

- Examining import/export names in malware to uncover new malware families linked to the same threat actor.
- **Imphashing for Malware Tracking:**
  - Generates a hash from the Import Address Table (IAT) of an executable file.
  - Comparing imphashes reveals related malware samples and variants.
- **Benefits:**
  - Identifies new malware variants by detecting similar or identical imphashes.
  - Useful in tracking malware with code reuse by threat actors.

- **LocalPotato Exploit (FIN11):**
  - Imphash analysis helps track different variants of this NTLM exploitation tool, which exploits CVE-2023-21746 for privilege escalation.

File-based Tracking

Code Similarity

LAZARUS APT

- **Code similarity:**
  - Compares malware samples to identify commonalities and relationships between different threats.
- **Key concepts:**
  - Code Reuse: Malware authors often reuse snippets or entire modules, linking malware to specific authors or groups.
  - Structural Analysis: Examining control flow graphs and function calls reveals hidden similarities.
  - Behavioral Patterns: Techniques for persistence, evasion, or exploitation may indicate a common origin.
- **APT Tracking:**
  - APTs reuse encryption keys, algorithms, API hashing, and C2 communications.
  - Reverse Engineering: Advanced techniques identify unique patterns for tracking via YARA rules.

```
signed_int64 __fastcall String decoder(int64 a1, int64 a2, Int64a3)
(
__int64 v3; // r10
char v4; // r11
signed __int64 result; // rax
unsigned int v6; // er9
__int64 v7; //rbx
char v8; // cl

a1 = (signed int)a3;
v3 = a2;
v4 = -124;
result = 1461817411164;
v6 = 162112194;
if ((signed int)a3 > 0i64)
{
    v7 = a1 - a2;
    do
    {
        v8 = *(_BYTE *)(v7 + v3++);
        *(BYTE )(v3 - 1) = v4 ^ result ^ v6 ^ v8;
        v4 = v4 & result ^ v6 & (v4 ^ result);
        v6 = (v6 >> 8) | ((((unsigned int16)v6 ^ (unsigned int16)(8 * v6)) & 0x7F8) << 20);
        result = ((unsigned int)result >> 8) | ((((_DWORD)result << 7) ^ ((unsigned int)result ^ 16
        •((unsigned int)result ^ 2 * (_DWORD) result)) & 0xFFFFFF80) << 17);

        --a3;
    }
    while ( 43 );
}
return result;
}
```

File-based Tracking

VT diff and content search

APT SIDECOPY- LINUX VARIANTS

content:"#+,/5=LMOS[hm{} + , @ P [\t%v(\")){}\n*., ->-c-u//000X0b0o0s0x255380: ; =#> ??A3A4CNCcCfCoCsLlLmLoLtLuMcMeMnNdNlNoOKOUPcPdPePfPiPoPsSTScSkSmSoTZTeToV1V2V3V5V6YiZlZpZs\")\"\n\\\"\\\\\\n \x0D\n\t]]:][[\nh2i)idipivmsn=nss us|0|1}\n"

Smart search

FILES - 9

Sort by | Filter by | Export | Tools | Help

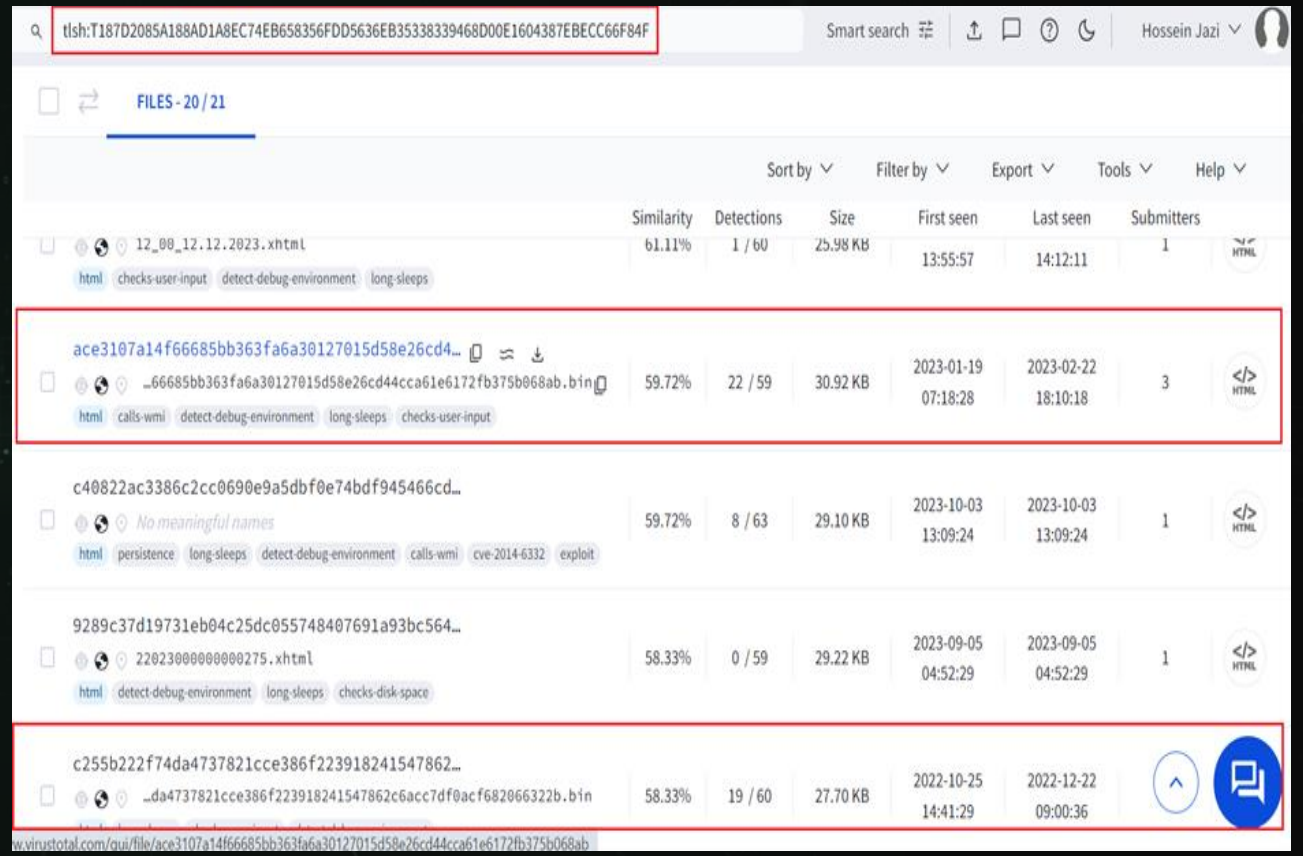
	Detections	Size	First seen	Last seen	Submitters
03888813079d01e1ba2d2675cf35724e529d58a78b9efd8161c746e8e33c64… D:\tmp\03888813079d01e1ba2d2675cf35724e529d58a78b9efd8161c746e8e33c643d.elf elf persistence detect-debug-environment sets-process-name	37 / 68	4.38 MB	2024-01-02 09:23:15	2024-01-08 06:11:33	5
c2ce338a7128bfe3909e9647c1f82bd9fea7220f063afd5c698512973d76a6… 61b898f4254d8c6d3d375584a1109367f9e86d221e2d404bf6768fb81b1b48b5.elf.rewr elf detect-debug-environment persistence	6 / 63	5.16 MB	2024-02-22 14:10:21	2024-02-22 14:10:21	1
9a9cd695f2aeb986e084c96f03ce433eda9c520f19a0d59c0e6a224984d243… 9645299e58c7521d811fbdcdbd57db45160191db7c7b73eae5d97e4530136da8.elf.rewr elf detect-debug-environment persistence	6 / 62	5.16 MB	2024-02-23 02:45:26	2024-02-23 02:45:26	1
9645299e58c7521d811fbdcdbd57db45160191db7c7b73eae5d97e4530136d… DocScanner_AUG_2023.pdf elf sets-process-name persistence detect-debug-environment	35 / 67	4.38 MB	2023-08-28 11:57:00	2023-11-17 14:28:57	3
61b898f4254d8c6d3d375584a1109367f9e86d221e2d404bf6768fb81b1b48… Homosexuality - Indian Armed Forces/Homosexuality - Indian Armed Forces .pdf elf persistence sets-process-name detect-debug-environment	39 / 68	4.38 MB	2023-08-29 09:33:23	2024-03-01 06:21:57	9
7efea614cd6eaf338da6d788029fff8b7a62e17ca8dcf58c5932db045c358d… Meeting_Notice-reg.pdf elf detect-debug-environment sets-process-name persistence	34 / 66	6.51 MB	2023-10-26 08:34:01	2023-11-15 21:08:25	3
db403abf7dcc5bccbedbb53eceef76bd02b440c1114a0b64e665eac1e44fa9… draft_letter_nov_2023.docx elf detect-debug-environment persistence sets-process-name checks-cpu-name	33 / 66	6.51 MB	2023-10-31 04:18:40	2023-11-17 13:56:12	3
a9407fdee890615e8e4f4927deb0c32795e848ce58e66dab56bf3b7188bc0b… DocScanner_Updated_letter.pdf elf detect-debug-environment persistence	33 / 67	6.51 MB	2023-10-31 04:18:40	2023-11-21 10:02:53	3
57e72c7c81df7d971db2977b51bc37447b641466917e7ed8f92efa3b0eb23f… updated_draft_PPT.pptx elf checks-cpu-name detect-debug-environment sets-process-name persistence	33 / 67	6.51 MB	2023-10-31 04:18:39	2023-11-17 13:55:01	4

File-based Tracking

Fuzzy hashing

GAMAREDON APT

- Fuzzy Hashing:
  - Identifies similarities between files or data, even when they are not identical.
  - Unlike traditional hashing, fuzzy hashes reflect degrees of similarity, useful for detecting variations of malicious files.
- Key Fuzzy Hashing Algorithms:
  - ssdeep: Detects similarities in spam emails and malware.
  - sdhash: Generates similarity digests for digital forensics, useful for file comparison.
  - TLSH: Robust against minor changes, used for clustering similar malware samples and identifying new variants.
- APT Tracking:
  - Links common tools used by APTs across incidents.
  - Compares hashes of files/scripts to track shared infrastructure and identify common servers/resources.



File-based Tracking

Fuzzy Hashing

OILRIG –SAITAMA BACKDOOR

tlsh:T1B9454B3BD722FDDAD7BF3D7090142D621C883D57A7714768FA4829EA26B7200DF1A168

Smart search

FILES - 9 / 9

Sort by | Filter by | Export | Tools | Help

	Similarity	Detections	Size	First seen	Last seen	Submitters
26884f872f4fae13da21fa2a24c24e963ee1eb66da47e270246d6… Confirmation Receive Document.xls xls handle-file run-dll auto-open environ powershell macros create-ole write-file exe-pattern …	100%	41 / 66	1.17 MB	2022-04-26 10:21:39	2022-04-26 10:21:39	1
e008a45aa0abaf3fe0a6553af81caf8fcfc7d11ff3ac4645016b4… dttcodexgigas.d57ff42e1e53341cd34ded32960dfe902168c8ce xls open-file auto-open create-dir exe-pattern handle-file url-pattern macros enum-windows environ …	97.22%	34 / 61	1.17 MB	2022-05-11 02:46:30	2022-05-11 02:46:30	1
84ca7cdceed0cc0731f7cf6af3d19d87c49331fc19aae65db444b… 84ca7cdceed0cc0731f7cf6af3d19d87c49331fc19aae65db444b73bab76fc0a.bin doc open-file create-dir exe-pattern handle-file malware macros run-dll environ calls-wmi write-file …	83.33%	32 / 60	1.16 MB	2021-04-02 07:09:38	2021-07-27 09:50:31	2
8206e02ba9150243ba4783ec7e8b613c518620f6d2b6f03cd6489… ~DF375B2D178C55641E.TMP doc write-file run-dll environ create-dir exe-pattern create-ole handle-file open-file macros	83.33%	36 / 62	1.16 MB	2023-09-30 17:48:48	2023-09-30 17:48:48	1
93e1eae55d96ea9282974be97aa2d637577d659142238975a4285… ~WRF{82955F2B-CB09-406B-BD5A-4CBB4024BAB1}.tmp doc	81.94%	2 / 61	1.16 MB	2023-09-30 17:48:48	2023-09-30 17:48:48	1
866a45cb8bf063c02496da35cf8d0e70a6de71964e96fb7891493… ~DF1BD5D0DA62810725.TMP doc	73.61%	1 / 61	1.06 MB	2023-09-30 17:48:48	2023-09-30 17:48:48	1
11dae9f628d35e003d6c08669cf9f4f35ce6e00fdd376bd757942… 11dae9f628d35e003d6c08669cf9f4f35ce6e00fdd376bd7579423cecfe0279c.bin doc open-file create-dir exe-pattern handle-file runtime-modules malware checks-network-adapters …	73.61%	39 / 62	1.26 MB	2021-04-02 07:32:03	2021-07-27 09:50:38	3
b8325b436df4745ccb57f9ba8765225c48e8517a4ee687b31ee80… M0.xls xls obfuscated open-file auto-open handle-file create-file detect-debug-environment macros calls-wmi …	59.72%	29 / 62	1.86 MB	2021-09-29 12:51:57	2021-09-29 12:51:57	1
8c60a7dd6cb293343c5a283fca635d447a1760a3928f6903213c1… MailFirst.txt vba obfuscated handle-file run-dll write-file anti-analysis	50%	13 / 59	1.82 MB	2021-09-29 12:57:22	2021-09-29 12:57:22	1

File-based Tracking

Signature – YARA rules

YARA RULES

- What are YARA Rules?
  - A powerful tool used to identify and classify malware based on patterns.
  - **Features:**
    - **Patterns**: Matches textual or binary patterns within files.
    - **Formats**: Includes plain text, hexadecimal strings, regular expressions, and wildcards.
    - **Conditions**: Incorporates complex conditions and boolean logic for precise targeting.
    - **Modularity**: Reusable and effective for various tasks.
- Applications of YARA Rules
  - **Detection**: Identify unique encryption algorithms or code reuse.
  - **Tracking**: Link malware samples to APT groups like Lazarus.
  - **Variants**: Detect and respond to known malware variants.

TURLA APT

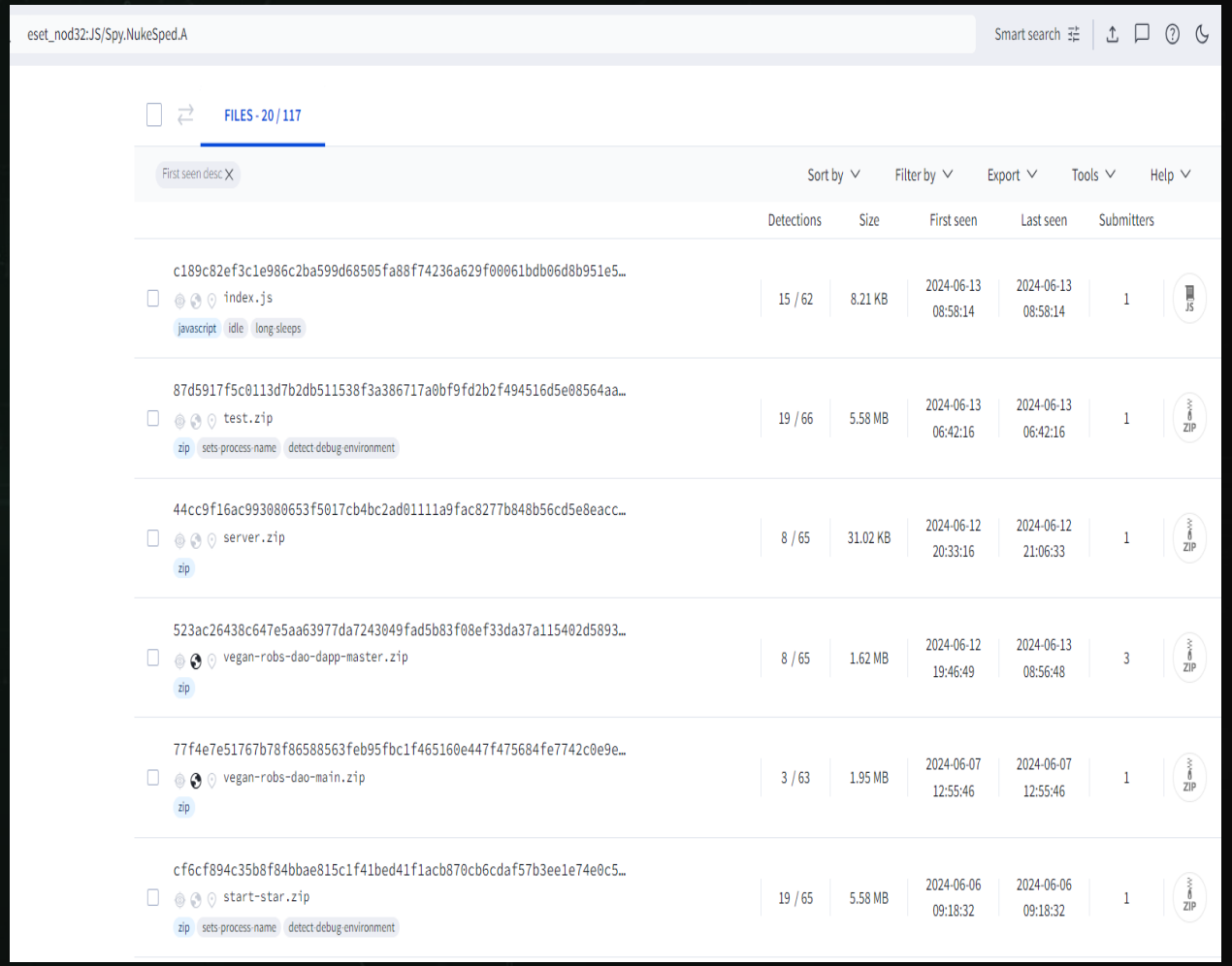
```
rule SFX_TUR_AND_KOPILUWAK
{
  meta:
    author = "H2J"
    description = "Strings contained in SFX"


  strings:
        $str1 = "Setup=c:\\windows\\system32\\wscript.exe /b"
        $str2 = "Silent=1"
  condition:
     all of them

}
```

File-based Tracking

AV Signatures

LAZARUS APT

- Specialized Signatures developed by companies can be used to track APT-linked malware.
- Lazarus APT Campaign
- **Malware:** BeaverTail
- **Detection:** AV signatures used to identify new samples associated with the attack campaign.
- .

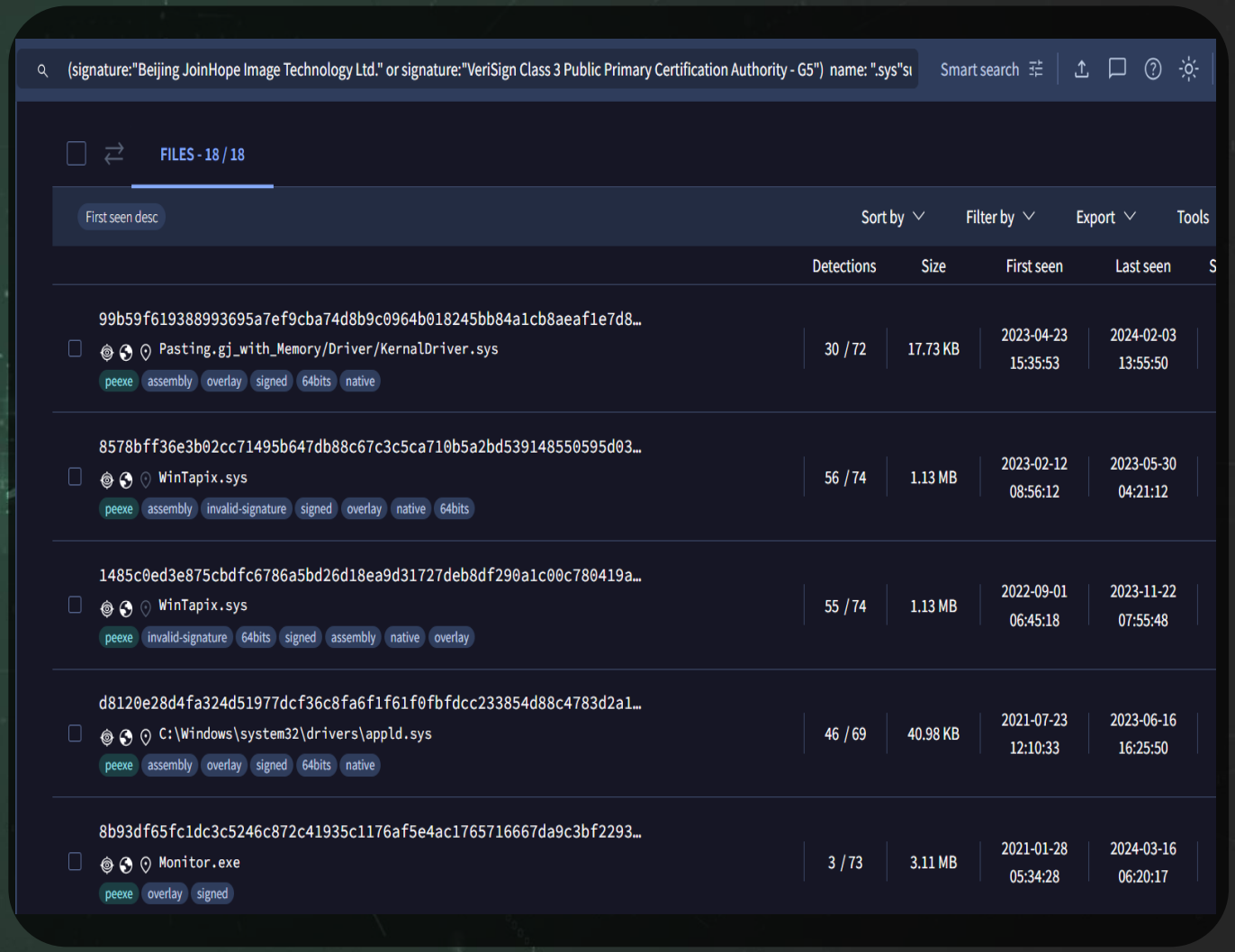


File-based Tracking

Code signing certificate

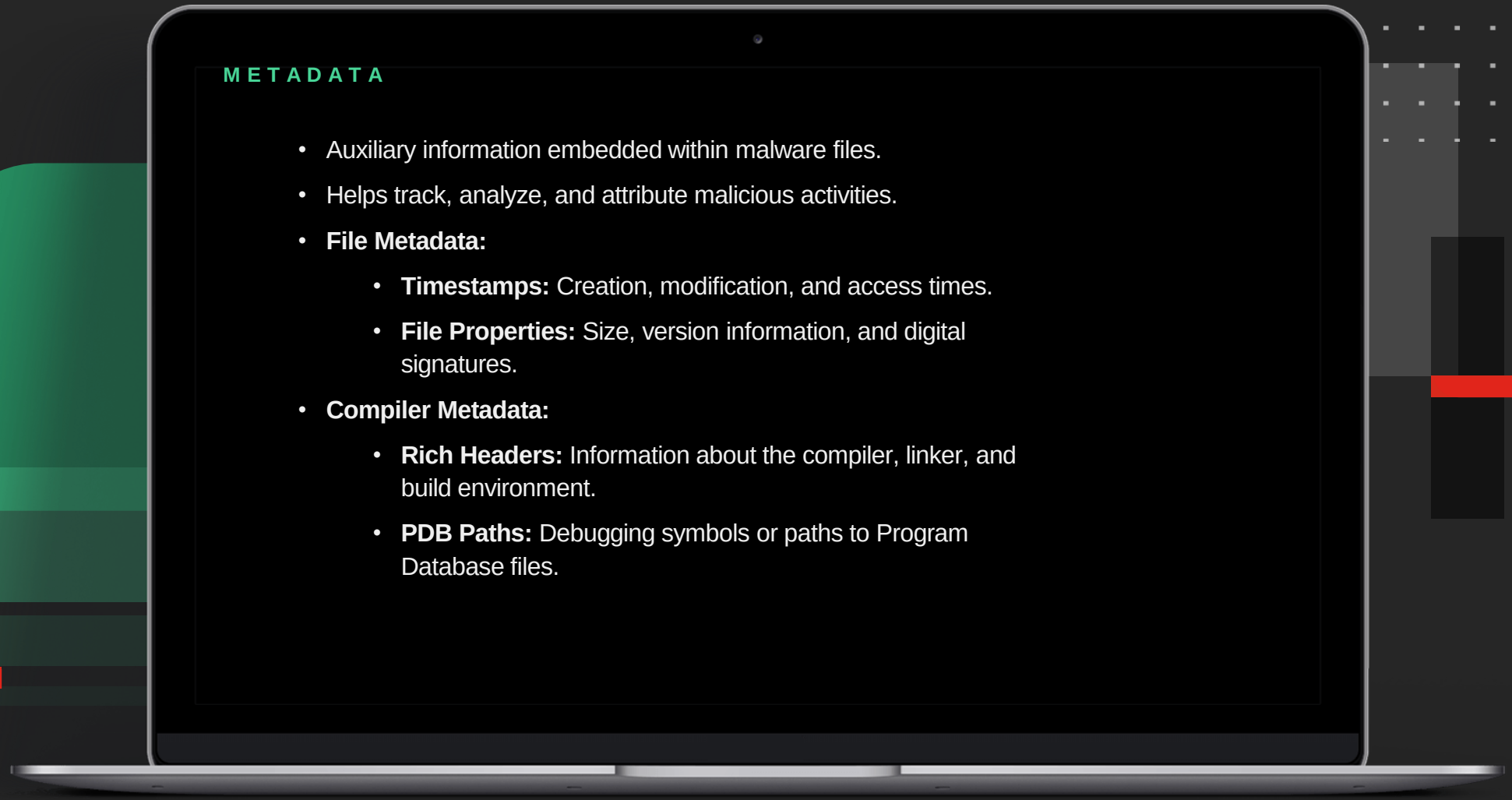
LEAF MINER –WINTAPIX DRIVER

- Digital certificates used to sign software, ensuring authenticity and integrity.
- Attackers use stolen certificates to sign malware, making it appear legitimate and bypassing security measures.
- Analyzing certificate details (e.g., issuers, serial numbers) can help link malware to specific actors.
- WinTAPIX code signing certificates from:
  - "Beijing JoinHope Image Technology Ltd."
  - "VeriSign Class 3 Public Primary Certification Authority - G5."



File-based Tracking

METADATA



File-based Tracking

Rich headers

TURLA APT

- Encoded metadata in Portable Executable (PE) files that contains information about compiler version, linked libraries, and build environment details.
- **Rich Header Hashing**
  - Generate a cryptographic hash from the decoded Rich header data.
  - Acts as a fingerprint for the build environment.
- **Applications for Tracking APTs**
- **Clustering:** Identifies malware samples with similar build environments.
- **Attribution:** Links new samples to known threat actors based on shared development practices.

```
rule APT_RU_Turla_Gazer_Embedded_Resource_RichHeader
{
  meta:
    description = "lets get weird - track embedded Gazer payloads based on their shared rich headers"
    hash = "d0b169d2e753191a5c366a863d216bc5a9eb5e173f0bd5a61f126c4fd16484ac"
    hash = "473aa2c3ace12abe8a54a088a08e00b7bd71bd66cda16673c308b903c796bec0"
    hash = "a65bc4adbd61c098acf40ef81dc8b6b10269af0d9ebbdc18b48439df76c18cb3"
    DaysofYARA_day = "94/100"
    author = "Greg Lesnewich"
  condition:
     for any var_rsrc in pe.resources: (
      uint16be(var_rsrc.offset) == 0x4d5a and
      hash.md5(var_rsrc.offset+0x80, 0x80) == "dd006bd9a43c05c9457a9e6b9e1636ca")
}
```

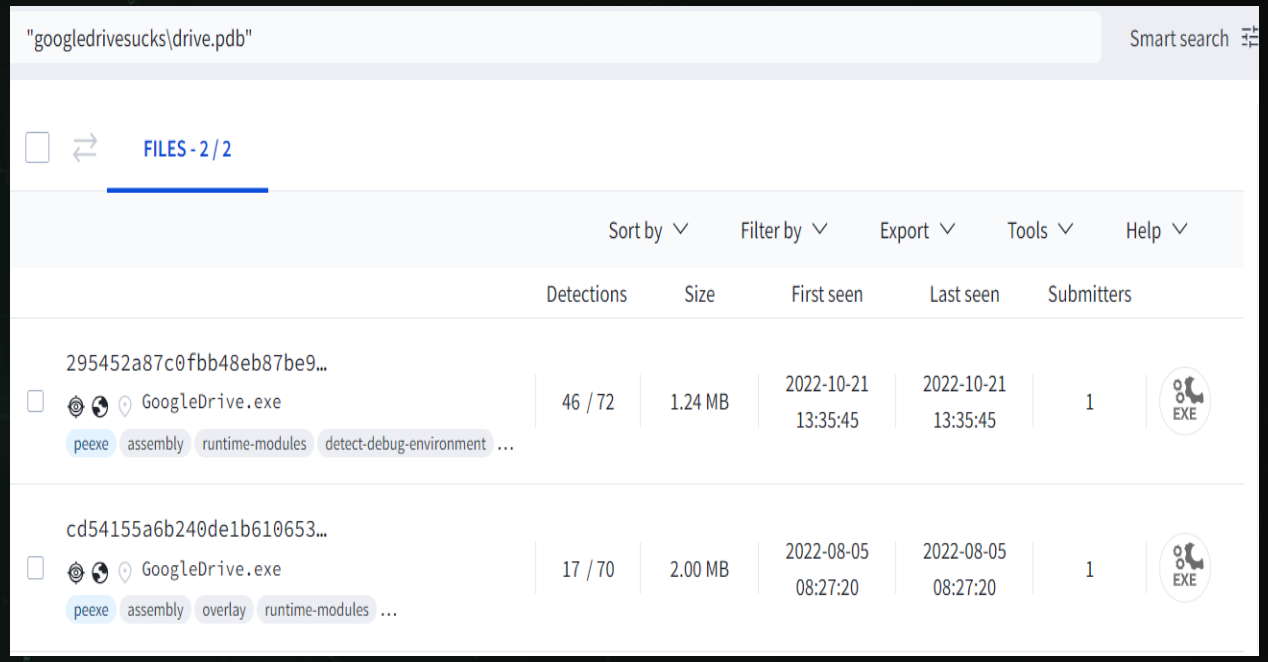
File-based Tracking

PDB

APT29

- Program Database files that store debugging information.
- Symbols, source line information, and stack traces.
- **Function & Variable Names**: Reveals malware structure and behavior.
- **Unstripped PDB Files:** Provides deeper insights if included by accident.

- **PDB Strings and Paths**
- Specific information within PDB files.
- Paths to source code files, directory structures, usernames, project names.



TTP-based Tracking

TTP-based Tracking

Mitre Attack

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/10)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (0/5)	BITS Jobs	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/6)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Autostart Execution (0/14)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Host Software Binary	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replication Through Removable		Create Account (0/3)		Deploy Container	Input Capture	Cloud Storage Object Discovery	Software
						Direct Volume Access		Container and Resource Discovery	
						Domain or Tenant Policy Modification (0/2)			

TTP-based Tracking

Monitor unique behaviors

LAZARUS

behaviour_processes:"pcalua.exe -a %APPDATA%" not tag: peexe

Smart search

FILES - 21 / 26

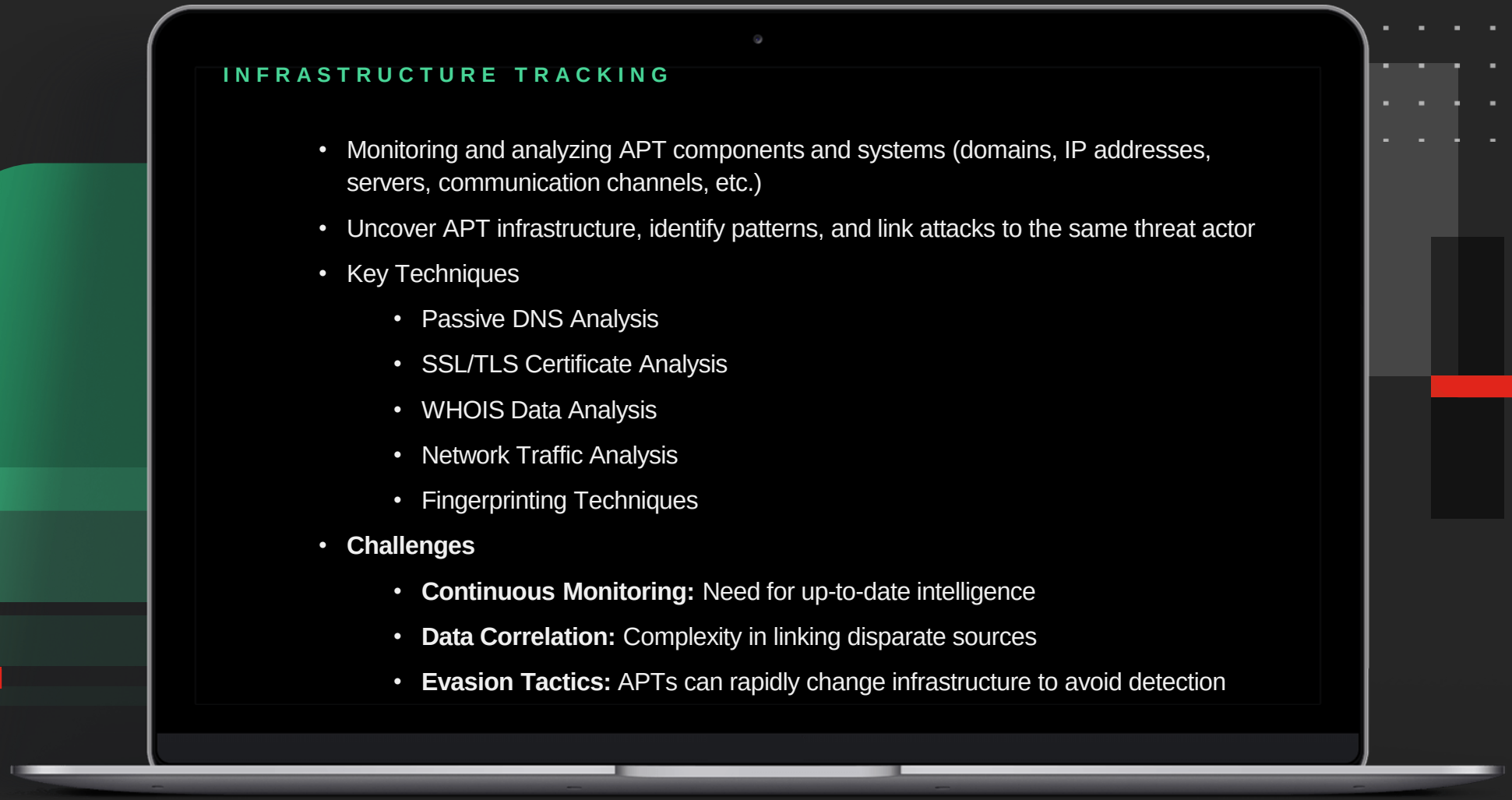
Sort by | Filter by | Export | Tools | Help

	Detections	Size	First seen	Last seen	Submitters
ff44d3dabb82467cd21187039789314bfd70c15777fcdc93ada11059ed4c28… veafdsag.msi msi runtime-modules direct-cpu-clock-access	21 / 62	543.00 KB	2022-07-29 09:18:16	2022-09-28 06:28:54	4
8eec3ac9f7d1ac64fc7397ba57cdac4f56959d1512f71dded60e831a26e076… unknown lnk long-command-line-arguments hiding-window url-pattern runtime-modules high-entropy direct-cpu-clock-access …	32 / 61	388.28 KB	2022-07-27 23:43:20	2022-08-03 22:01:01	3
eaef808e1ac99d13481b23b9dbdb6d246b14feaf35db0b592412dc213e619c… unknown lnk long-command-line-arguments hiding-window url-pattern runtime-modules detect-debug-environment …	25 / 60	2.09 KB	2022-07-27 23:48:15	2022-08-03 19:03:31	2
73f684b87139927012db12ec8d92824bd2404102e17ec427b302c79a4314d4… C:\Users\user\AppData\Local\Temp\hob.lnk lnk long-command-line-arguments hiding-window url-pattern runtime-modules direct-cpu-clock-access	26 / 61	2.09 KB	2022-08-03 13:50:47	2022-08-03 13:50:47	1
bcafd808237f1f29bdae4e45d75d925fb4fa3d7fe7f85abb953ba3f33aa29e… C:\Users\user\AppData\Local\Temp\hob.lnk lnk long-command-line-arguments hiding-window url-pattern runtime-modules detect-debug-environment …	9 / 51	2.09 KB	2022-08-01 09:37:24	2022-08-01 09:37:24	1
2e0abe6352af0924f9d9cc098230fa25e1f05cf4ae43a2d0b71405dedfe029… unknown lnk url-pattern hiding-window long-command-line-arguments executes-dropped-file	31 / 60	2.08 KB	2022-07-29 13:25:14	2022-08-01 01:10:39	2
e40347e7cd335b43a0d27b33521684754f66d1e3be714f22a68e27d396a63f… unknown lnk long-command-line-arguments hiding-window url-pattern runtime-modules detect-debug-environment high-entropy …	24 / 61	276.65 KB	2022-07-29 09:13:10	2022-07-30 23:52:17	4
9dc813afe2ff8963696691d5092b9ea779048c63ba1a8232e8ae81f0f1a476… C:\Users\user\AppData\Local\Temp\hob.lnk lnk long-command-line-arguments hiding-window url-pattern runtime-modules detect-debug-environment …	15 / 61	2.09 KB	2022-07-29 23:51:29	2022-07-29 23:51:29	1
bcfa523b1d55fcadc89bfee8f7c9abac3497f7760485843e6f58fe666984aa… C:\Users\user\AppData\Local\Temp\abo.lnk lnk long-command-line-arguments hiding-window url-pattern runtime-modules direct-cpu-clock-access executes-dropped-file	16 / 61	2.07 KB	2022-07-29 09:18:13	2022-07-29 09:18:13	1

Network-based Tracking

Infrastructure tracking

Network-based Tracking



Network-based Tracking

Infrastructure Reuse

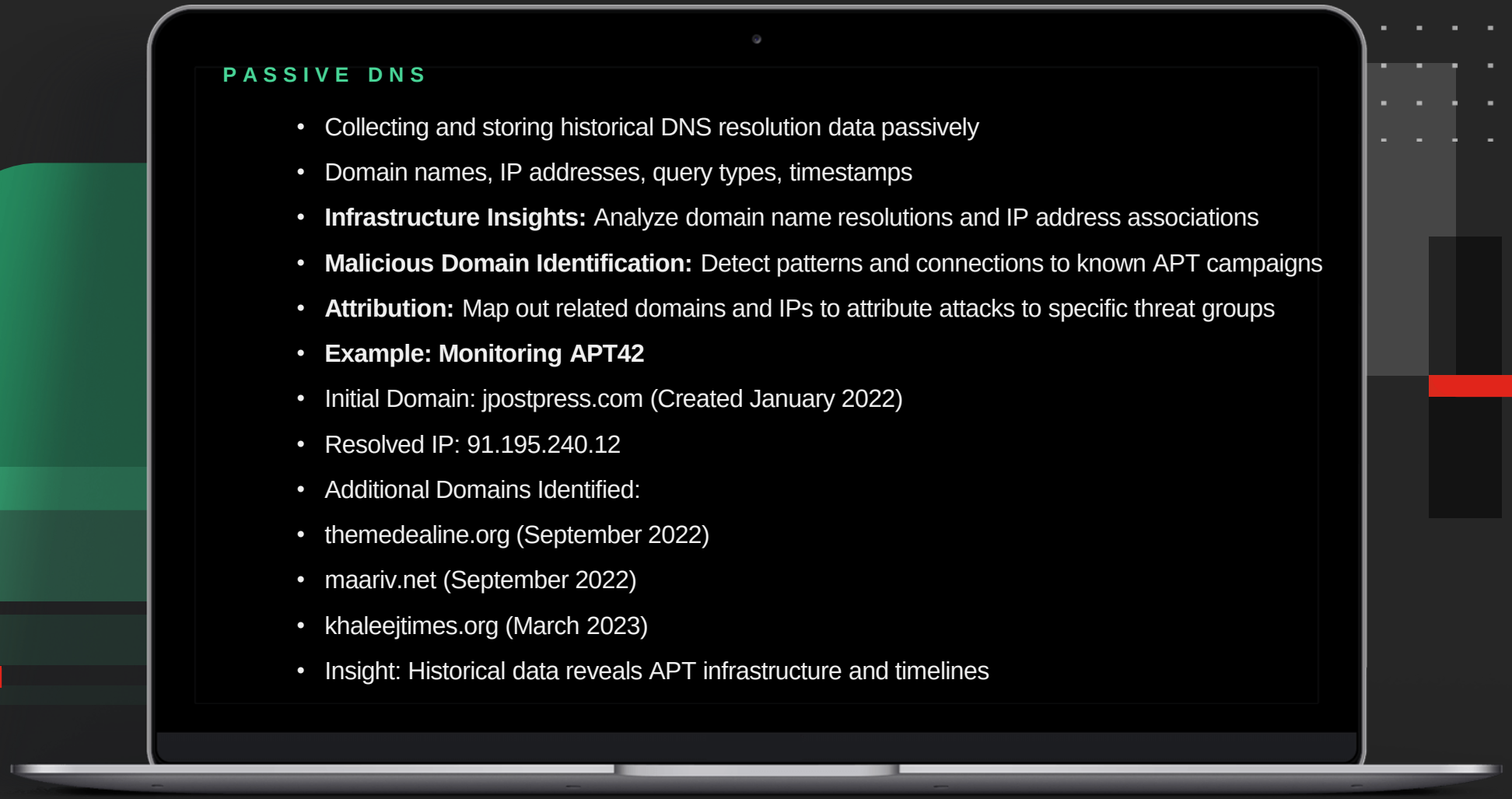
LAZARUS -BEAVERTAIL

- Some APT groups reuse IP addresses and domains due to resource constraints
- Reused infrastructure is common across different campaigns
- VirusTotal nethunt: A new feature that enhances infrastructure tracking
    - Purpose: Allows users to create Yara rules
    - Function: Identifies samples using the same infrastructure
- **Campaign Detection:** Detect new campaigns that reuse existing infrastructure
- **Campaign Analysis:** Identify if samples are part of ongoing or previously analyzed campaigns

```
rule C2_IPs_Lazarus
{
 meta:
  author = "Fortinet TI"
  description = "Rule to find files that contact malicious IPs used by North Korea's Lazarus group"
  target_entity = "ip_address"
 condition:
  // CTI-194
  vt.net.ip.raw matches /^67.203.7.171/ or
  vt.net.ip.raw matches /^147.124.212.89/ or
  vt.net.ip.raw matches /^147.124.214.129/ or
  vt.net.ip.raw matches /^147.124.214.131/ or
  vt.net.ip.raw matches /^147.124.214.237/

}
```

Network-based Tracking

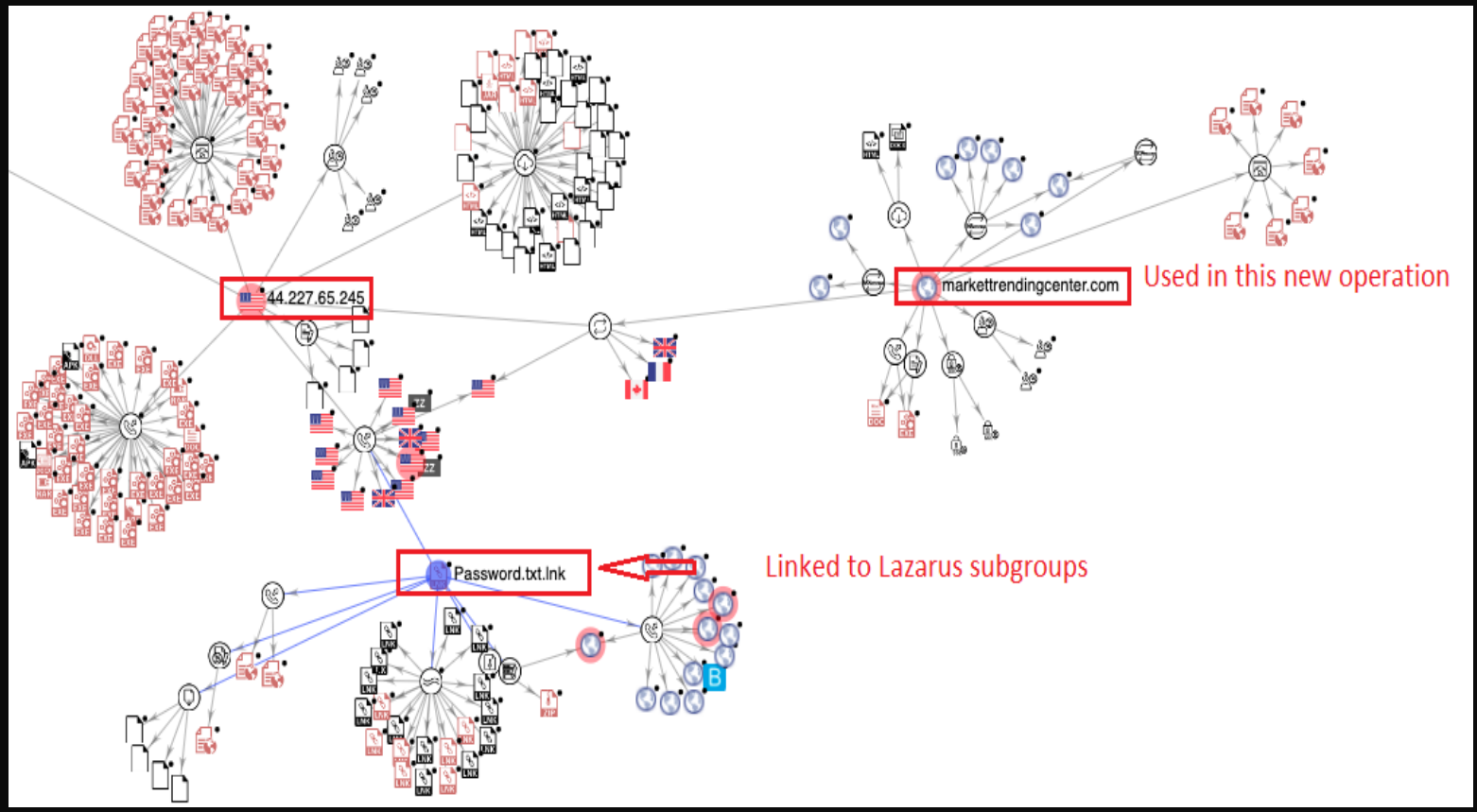
Passive DNS



Network-based Tracking

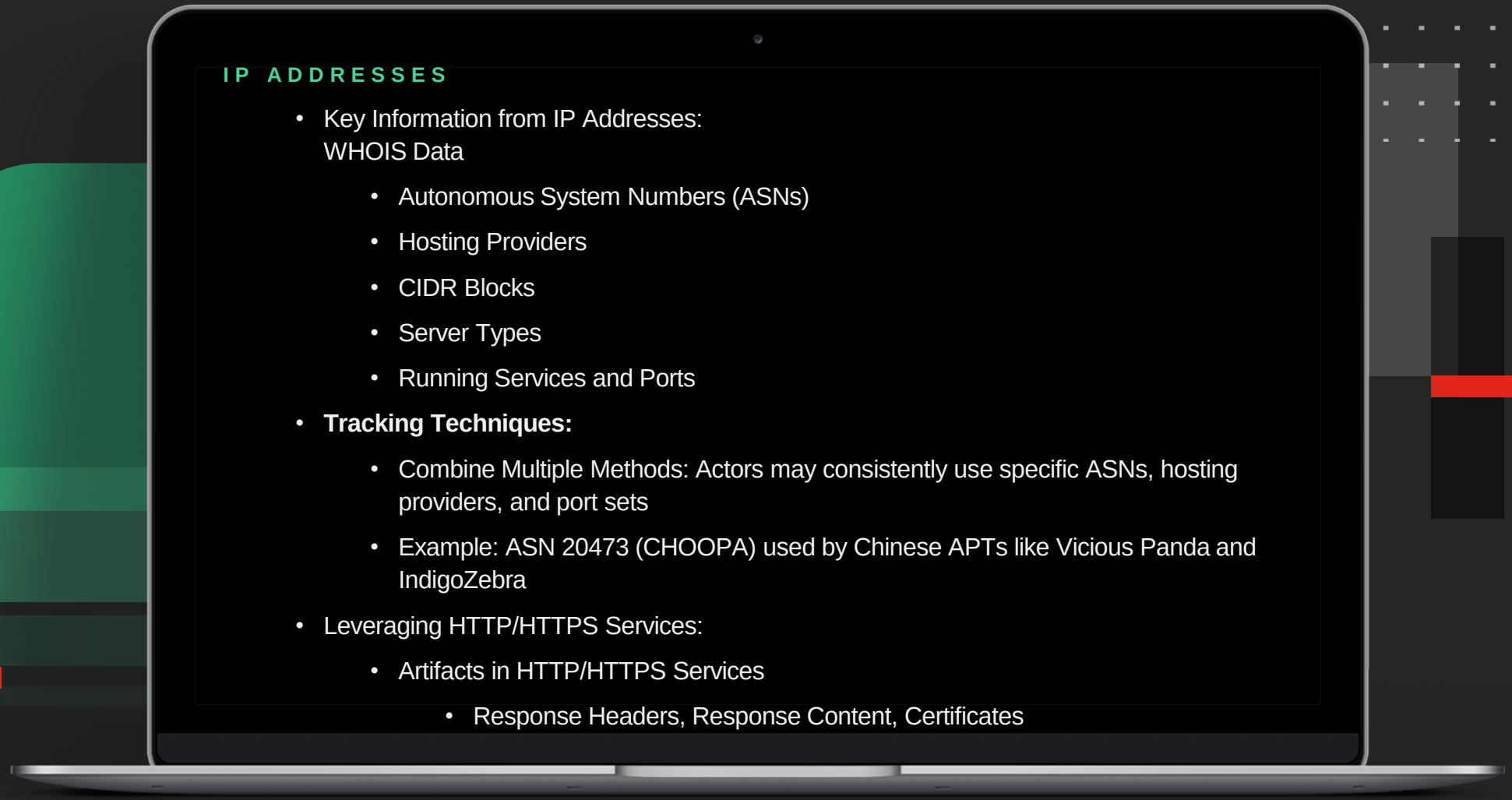
Passive DNS

LAZARUS



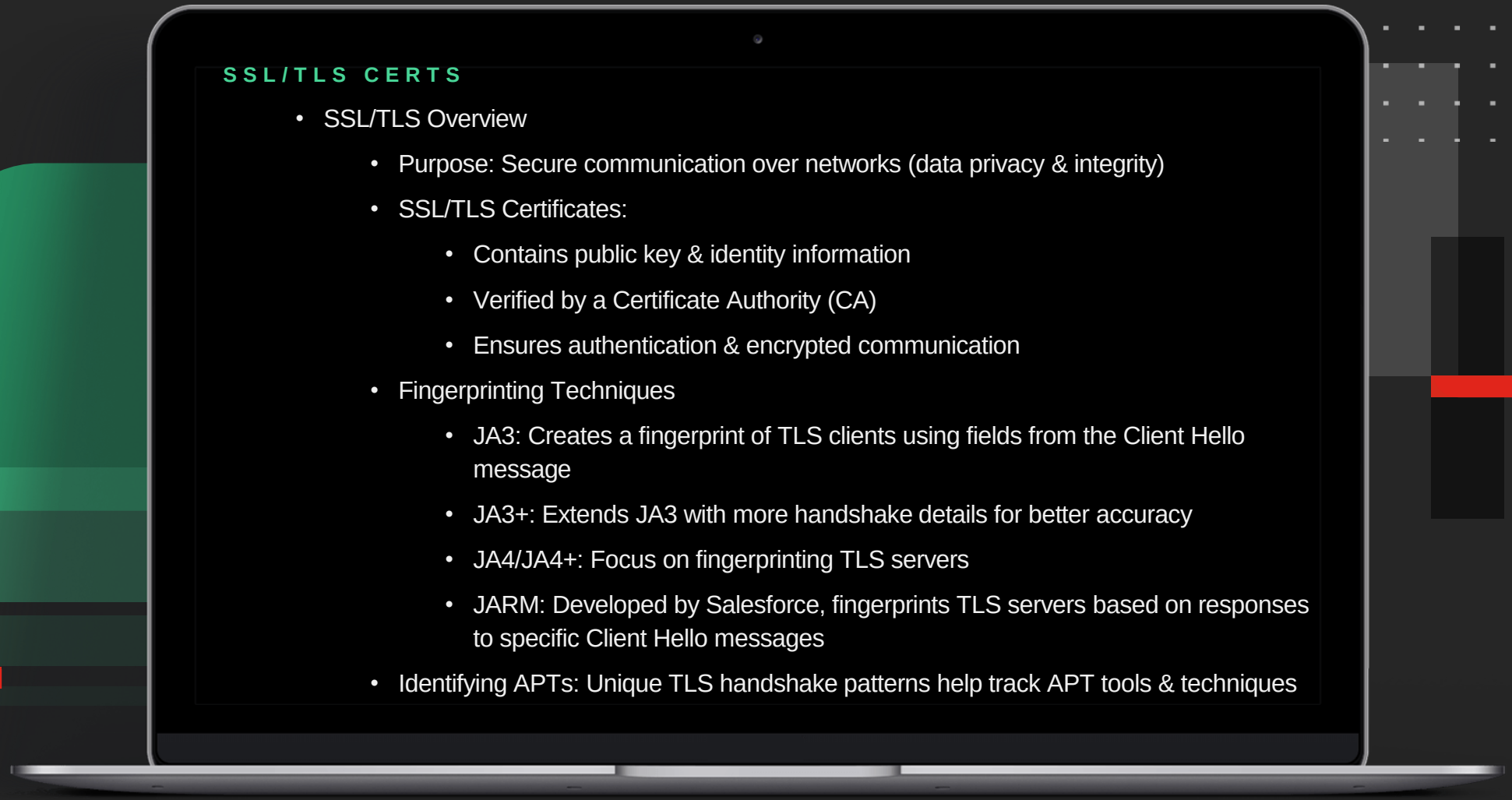
Network-based Tracking

IP Addresses



Network-based Tracking

Certificates and Fingerprints

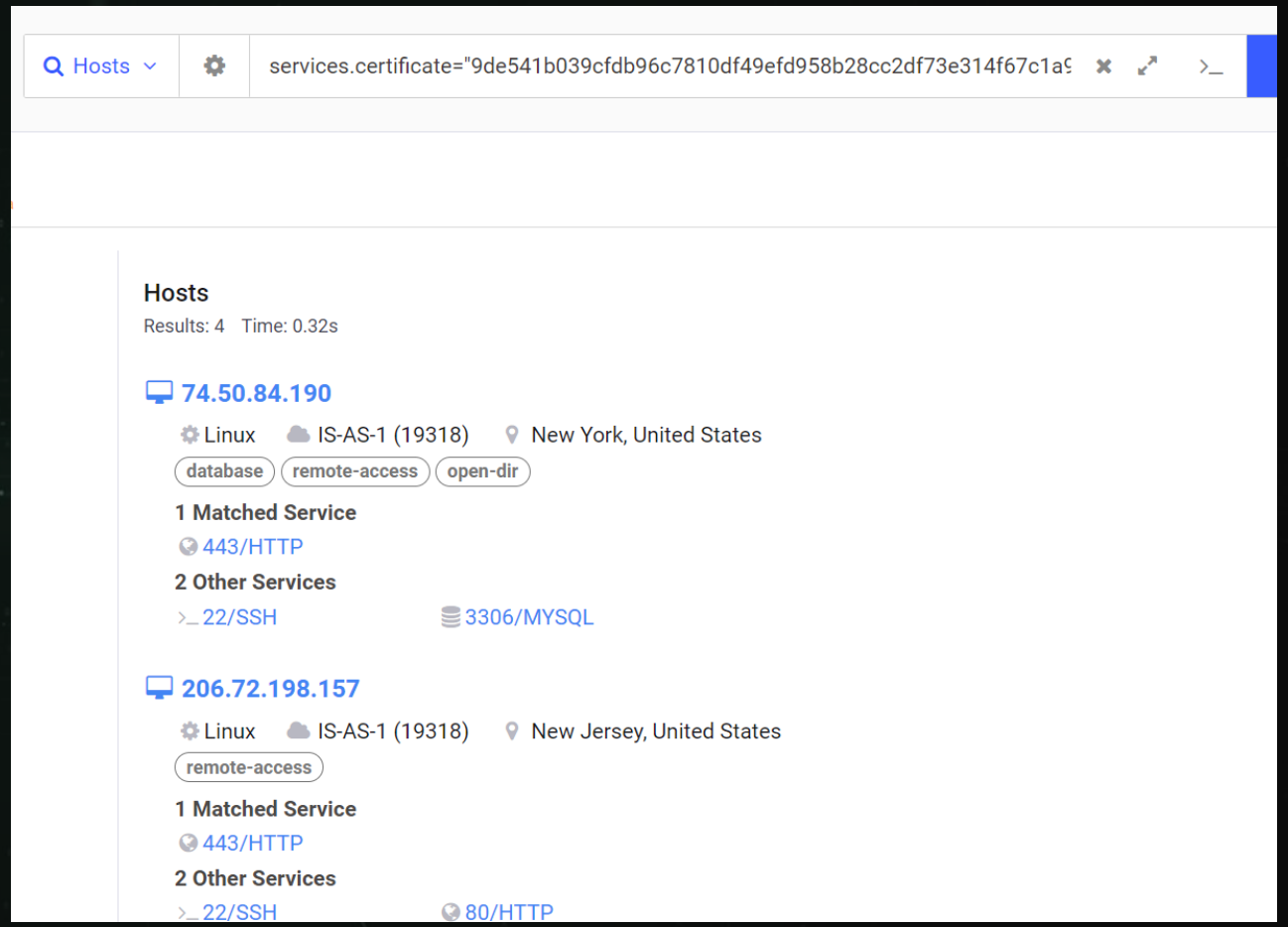


Network-based Tracking

Certificate values/hash

KIMSUKY

- **Common Name (CN):** The primary identifier, often representing the domain name or server name.
- **Subject Alternative Names (SANs):** Additional domain names or IP addresses for which the certificate is valid.
- **Issuer:** The entity (CA) that issued the certificate, providing trustworthiness information.
- **Serial Number:** A unique identifier assigned by the issuer for distinguishing the certificate.
- **Validity Period:** The time frame in which the certificate is valid.
- **Public Key:** Used for encryption and authentication, associated with the private key
- **Signature Algorithm:** Specifies the security algorithm used to sign the certificate.
- **Key Usage:** Defines the cryptographic operations allowed for the public key.
- **Extended Key Usage (EKU):** Specifies additional purposes beyond the basic key usage.

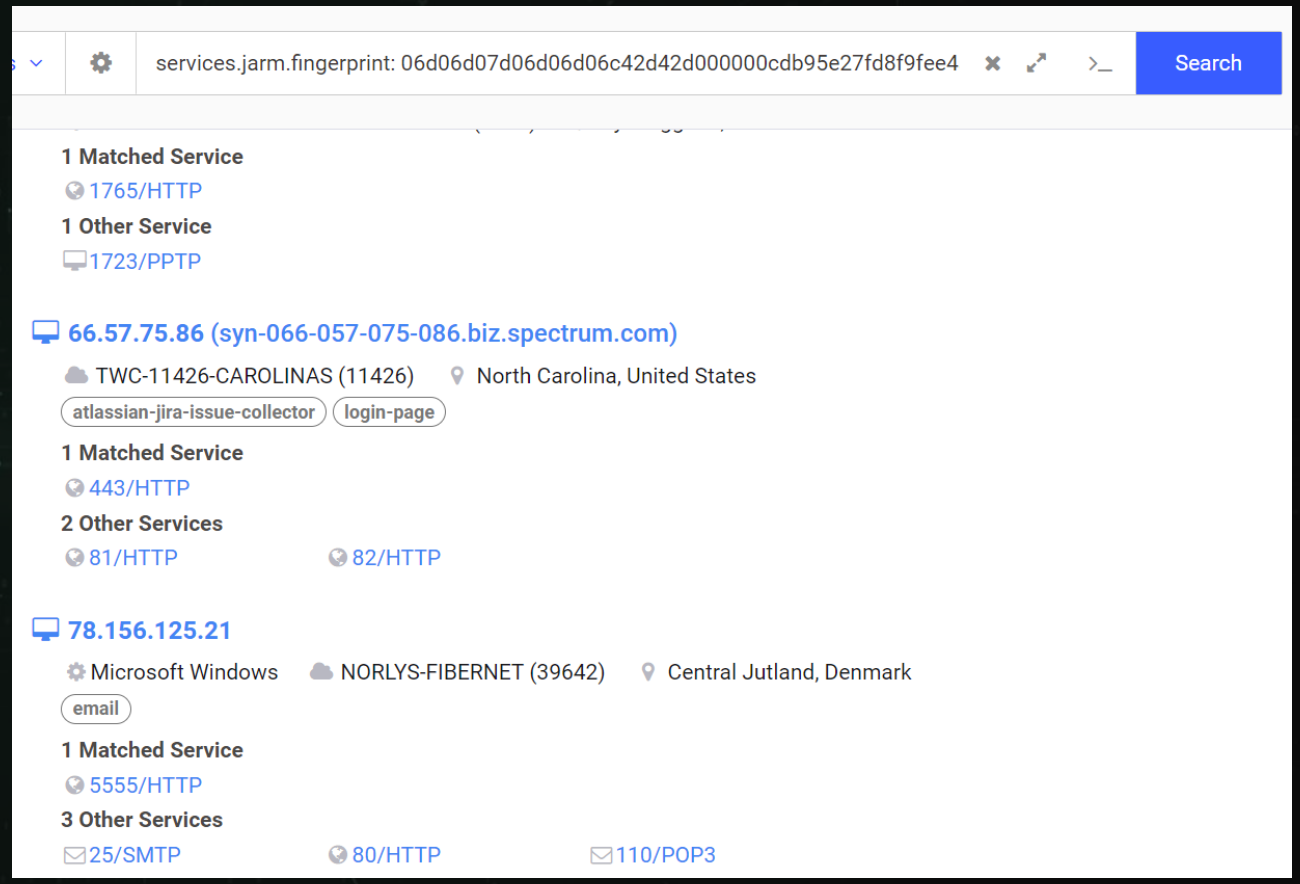


Network-based Tracking

JARM Fingerprint

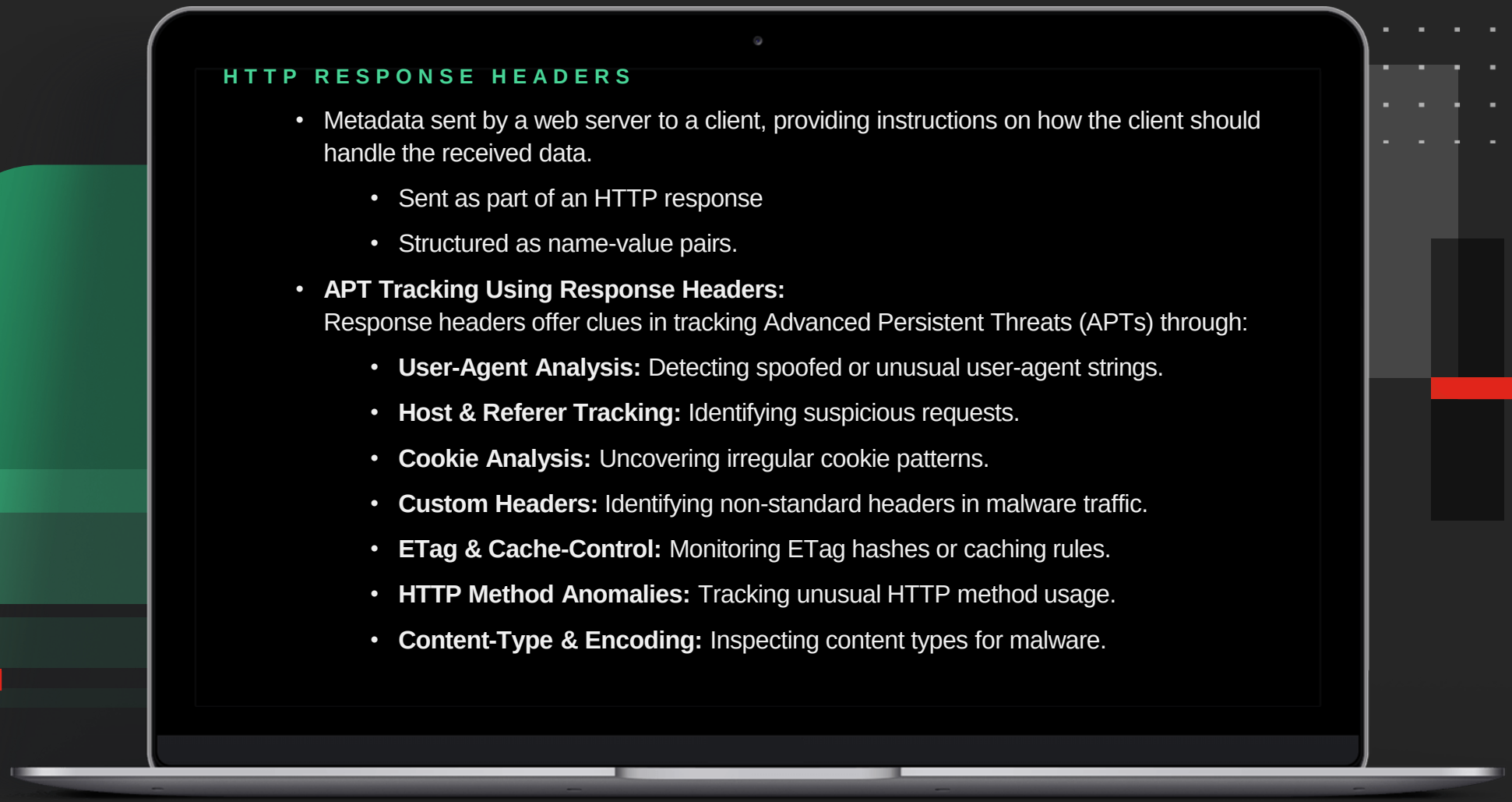
STORM0558

- Use JARM fingerprint consistent with SoftEther VPN
- x509 certificate has expiration date of December 31, 2037
- Subject information within the x509 certificate does not contain “softether”



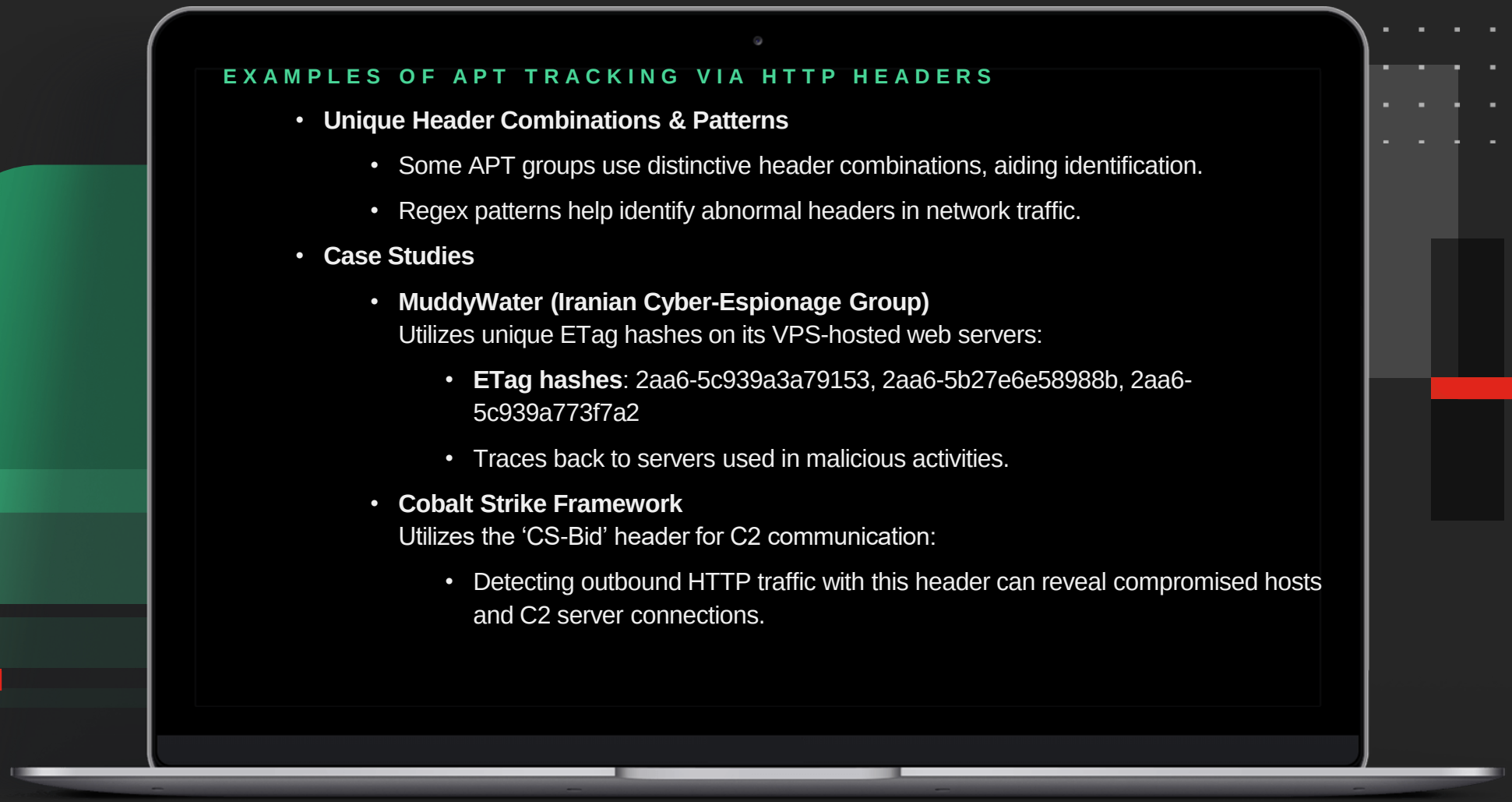
Network-based Tracking

HTTP Response Headers



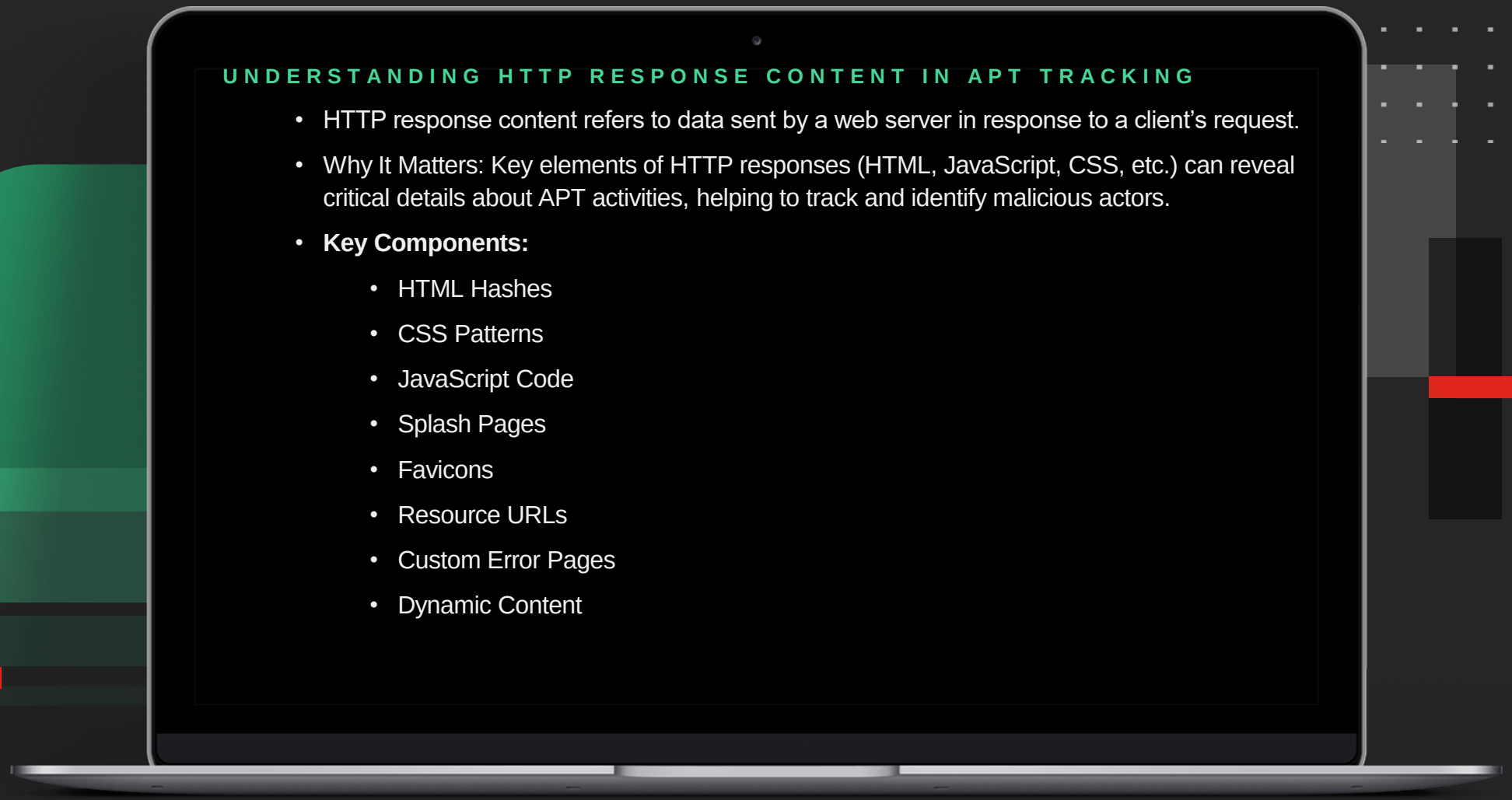
Network-based Tracking

HTTP Response Headers



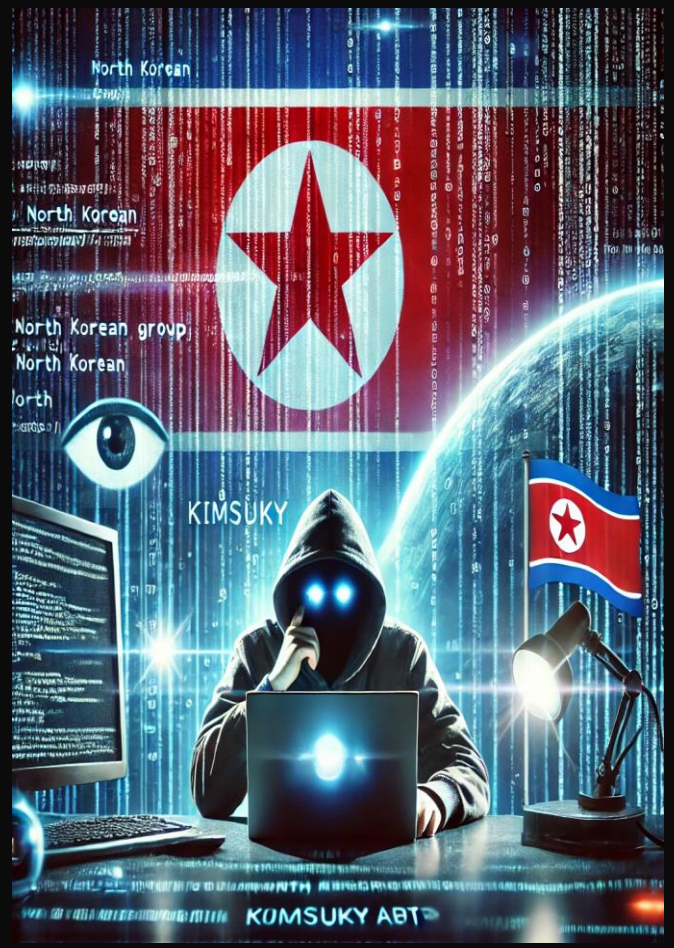
Network-based Tracking

HTTP Response Content

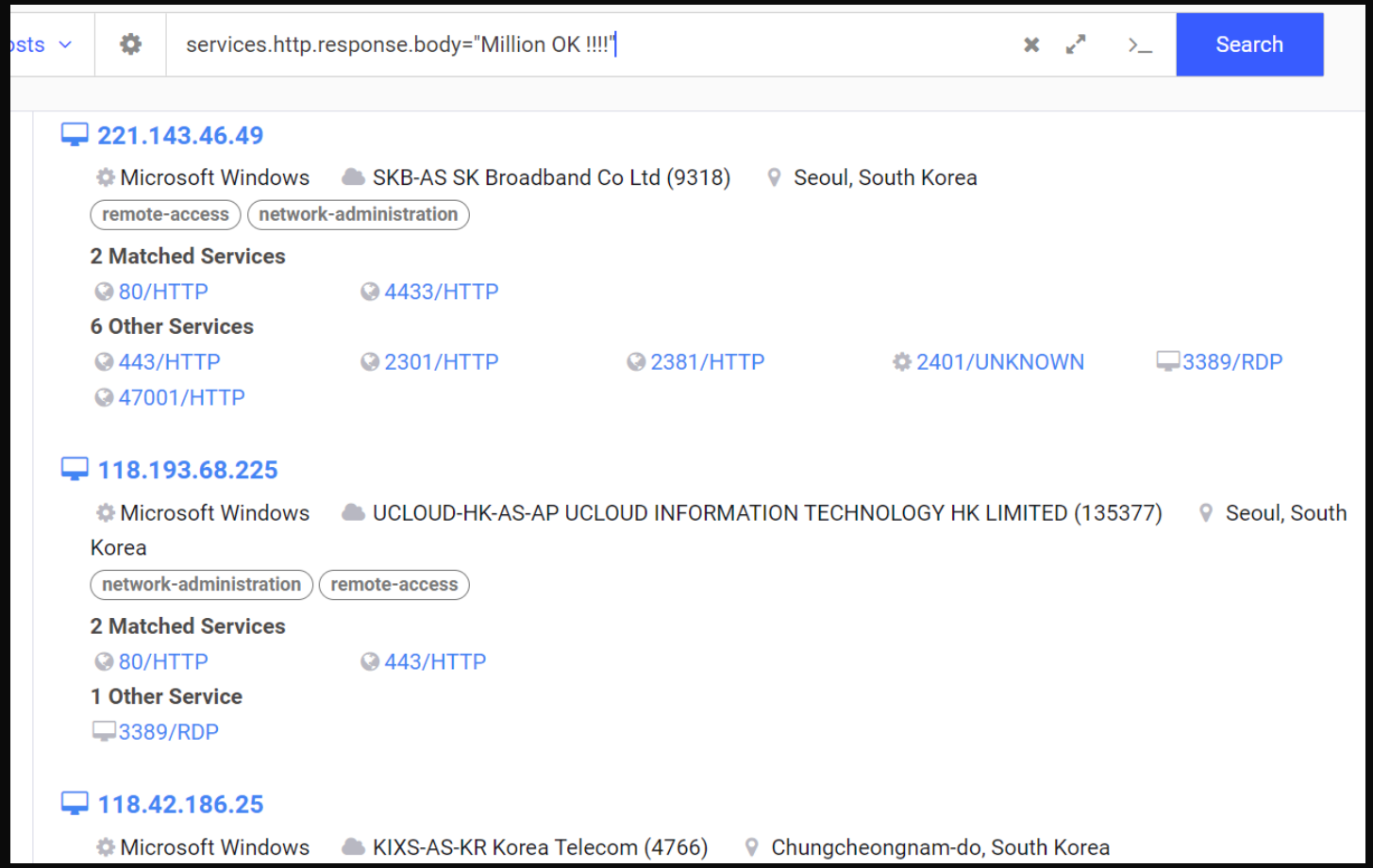


Network-based Tracking

HTTP Response Content



KIMSUKY

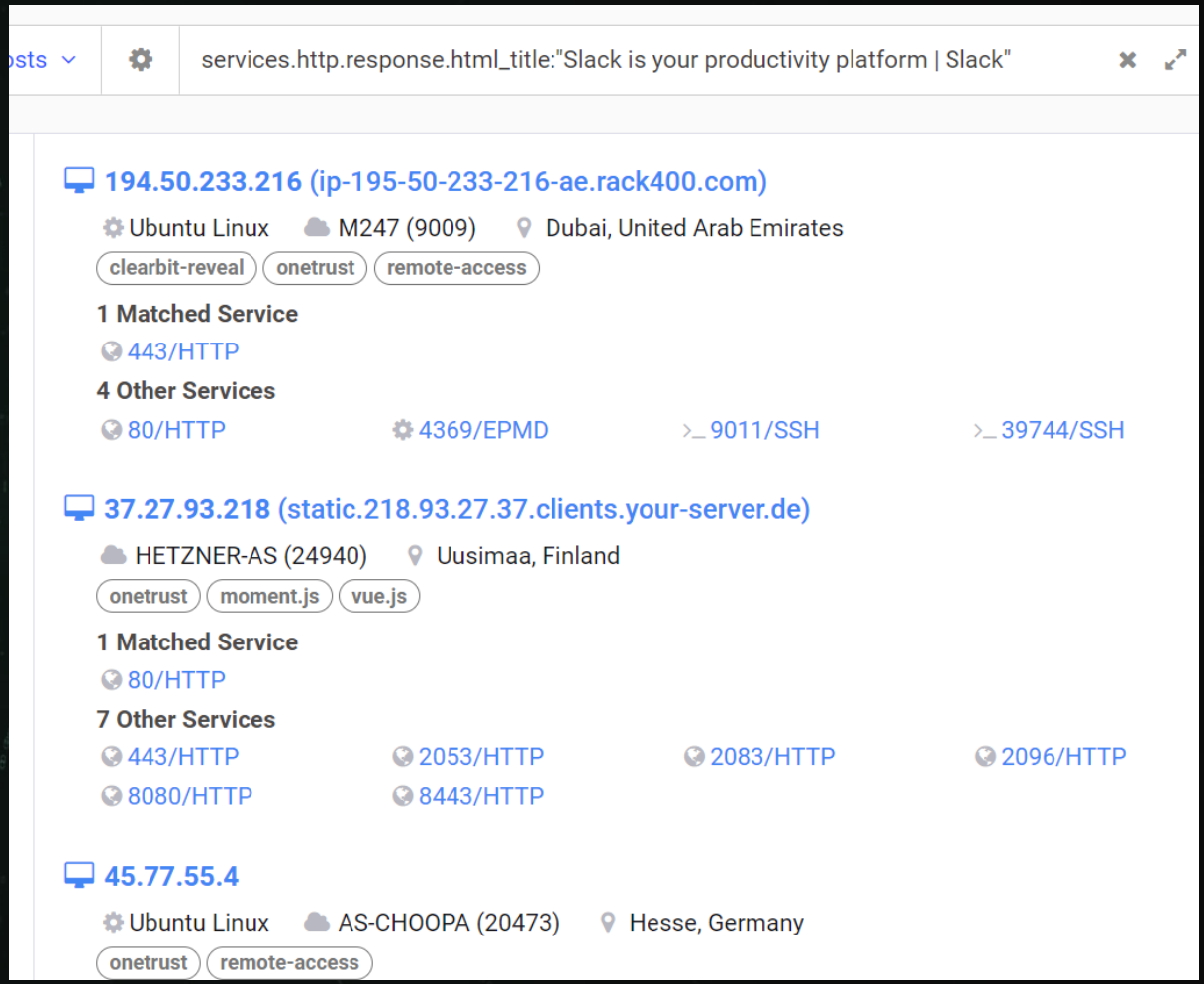


Network-based Tracking

HTTP Response Content

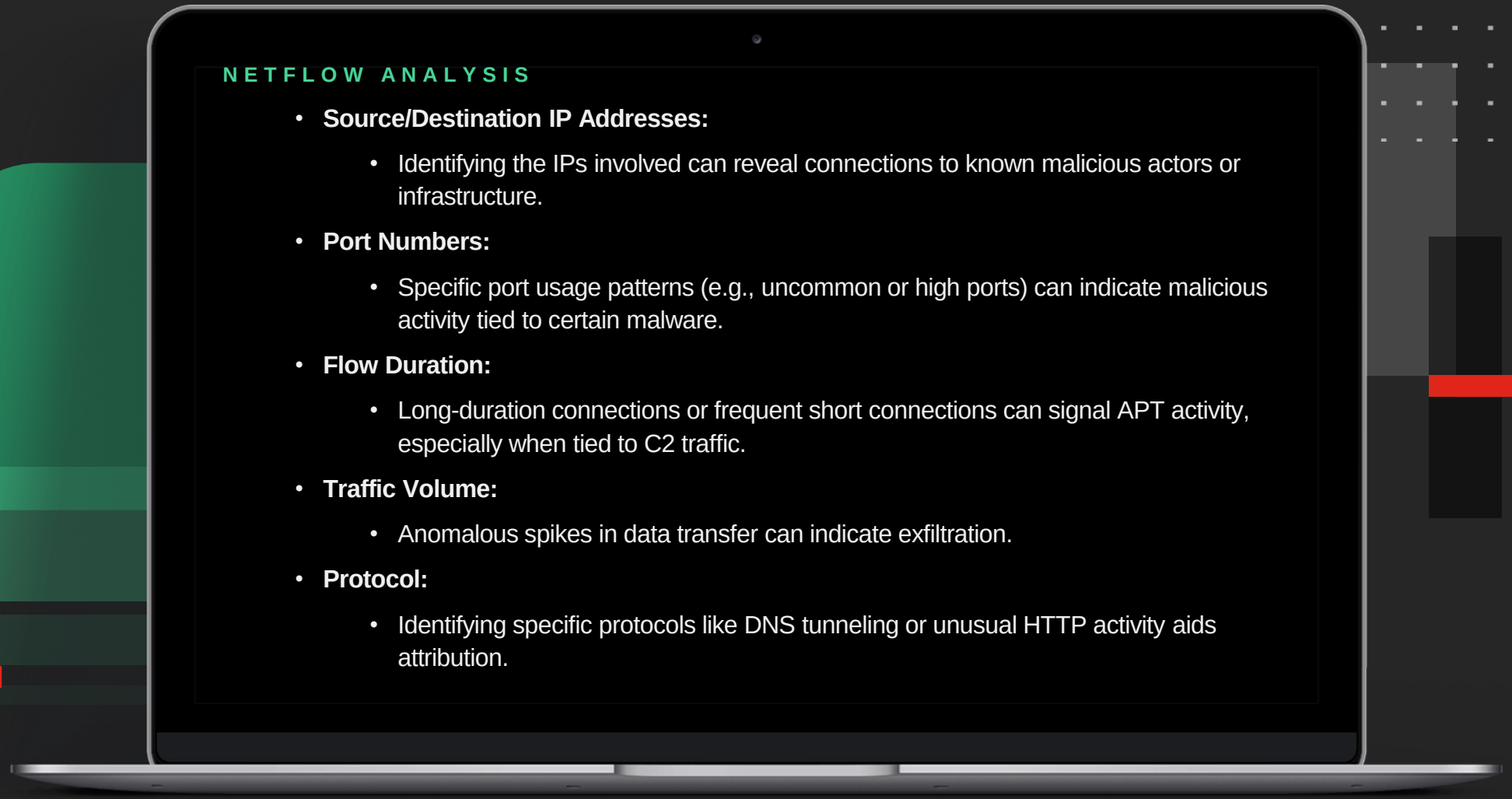
QBOT

- Qbot Malware: Researchers used unique HTML titles in HTTP response content to track servers related to Qbot malware operations.



Network-based Tracking

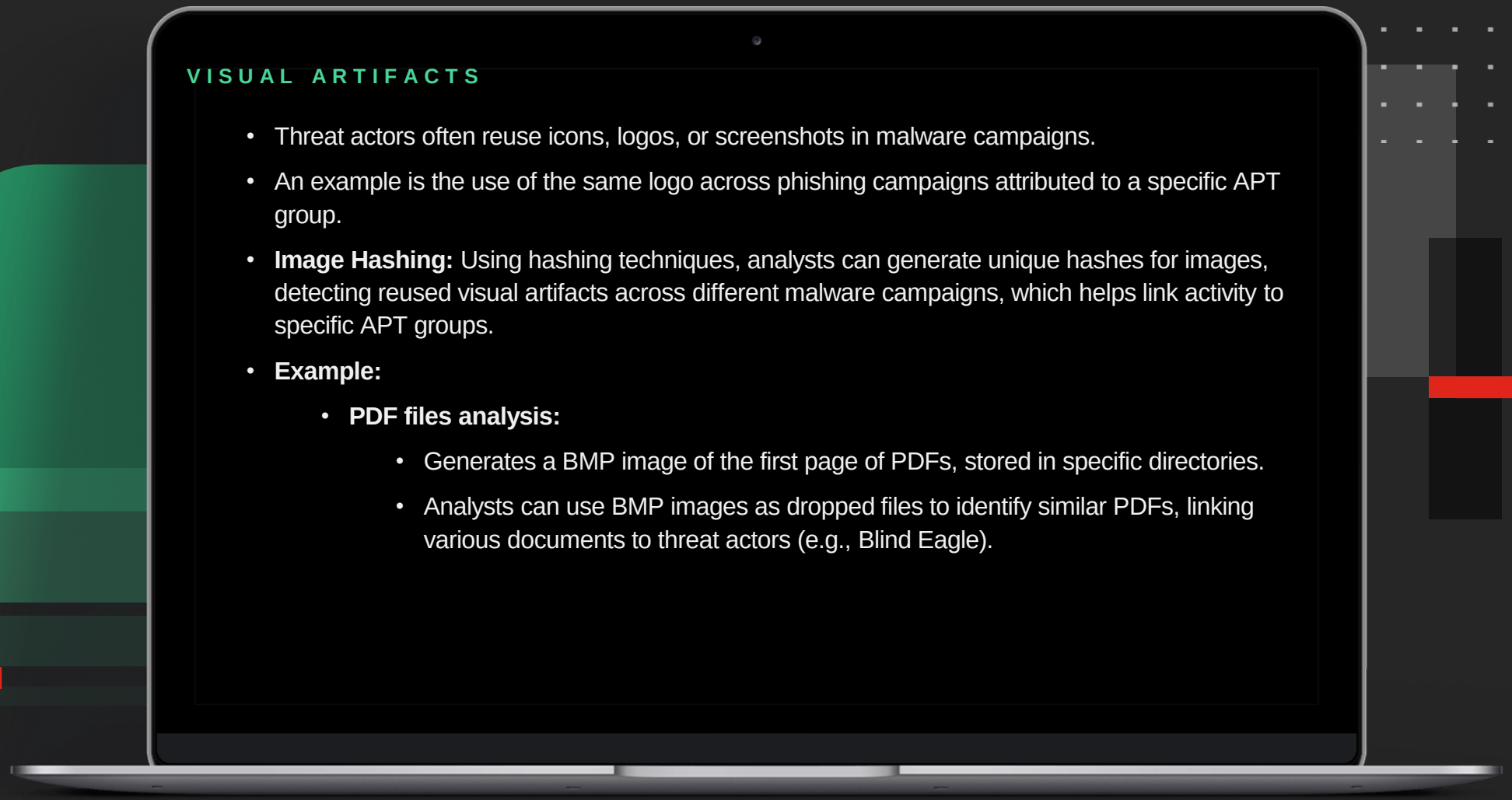
Tracking and Attribution using Netflow



Tracking Threat Actors with Visual Artifacts

APT Tracking

Visual Artifacts



APT Tracking

Visual Artifacts

LAZARUS

main_icon_dhash:1100353b1b800000

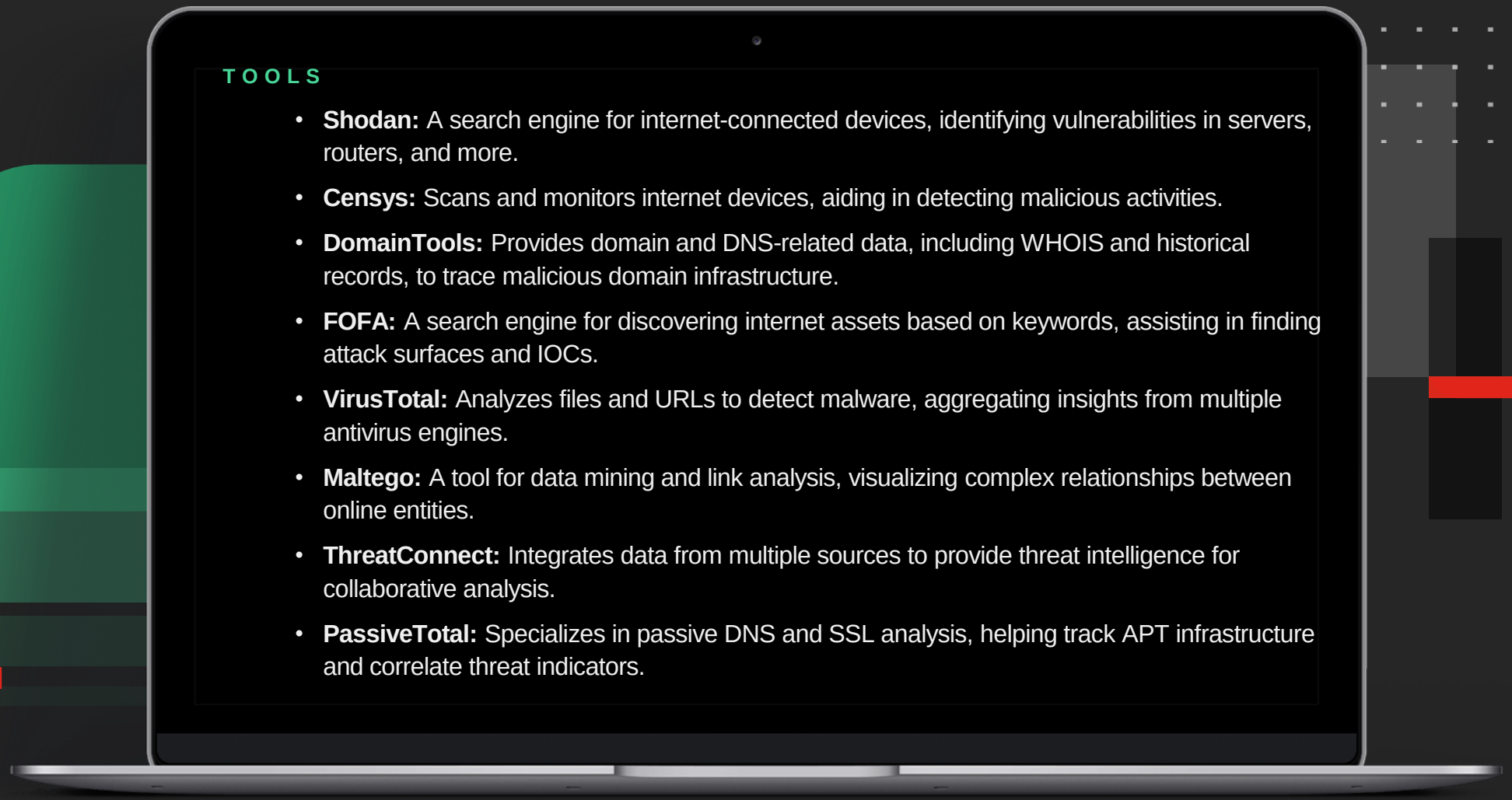
FILES - 6 / 6

Sort by | Filter by | Export | Tools | Help

	Detections	Size	First seen	Last seen	Submitters
0d01b24f7666f9bccf0f16ea97e41e0bc26f4c49cdfb7a4dabcc0a494b44ec… 0d01b24f7666f9bccf0f16ea97e41e0bc26f4c49cdfb7a4dabcc0a494b44ec9b.docx doc macros run-dll persistence long-sleeps detect-debug-environment url-pattern auto-open open-file exe-pattern …	40 / 64	2.27 MB	2022-01-18 16:13:22	2024-09-10 04:29:14	61
87f9f137687187e8eecf98393a7885fdd55cf573d80d94443e9324daa5fc49… 932.docx doc calls-wmi	0 / 63	353.50 KB	2024-01-03 13:19:04	2024-09-09 05:52:21	7
b3218dbbc4417667bee19f637235e25afe0c5ff521151e5ee5bca5ec1d0455… C:\Users\user\Desktop\readme.doc (copy) doc open-file url-pattern exe-pattern malware macros run-dll calls-wmi auto-open	39 / 66	4.24 MB	2024-08-08 19:23:36	2024-08-08 19:23:36	1
3c5d6b1e22ccd420ecbfcc21354929604c8fbd1f3c66d25b89cb9bf13062f3… C:\Users\user\AppData\Local\Temp\~DF269D13A291D288E9.TMP doc open-file exe-pattern macros run-dll url-pattern	32 / 63	4.29 MB	2022-11-20 14:15:06	2022-11-20 14:15:06	1
ef8f4d31e16cfb399b4c69e3d2c43ab33863d3149cb701209061aa5d575747… C:\Users\user\Desktop\attachment.doc (copy) doc open-file exe-pattern macros run-dll url-pattern	35 / 62	4.24 MB	2022-06-22 03:02:51	2022-06-22 03:02:51	1
d1b5961f259b9af90d8c191f679b996c7321d00a17363a7639eb74fa9428b9… clean.doc doc open-file exe-pattern url-pattern malware macros run-dll	31 / 61	2.26 MB	2022-04-26 07:16:00	2022-04-26 07:16:00	1

TOOLS

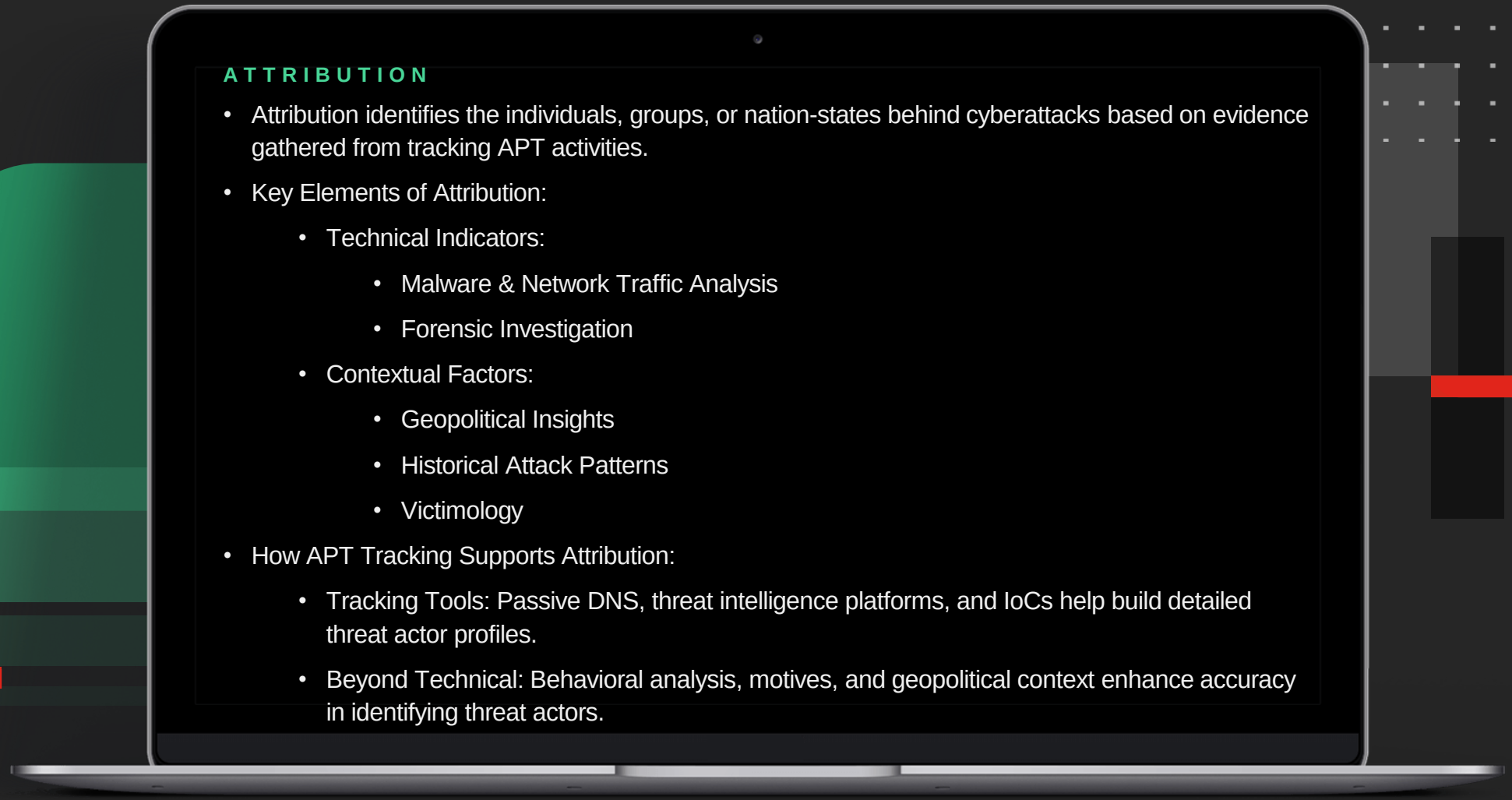
TOOLS



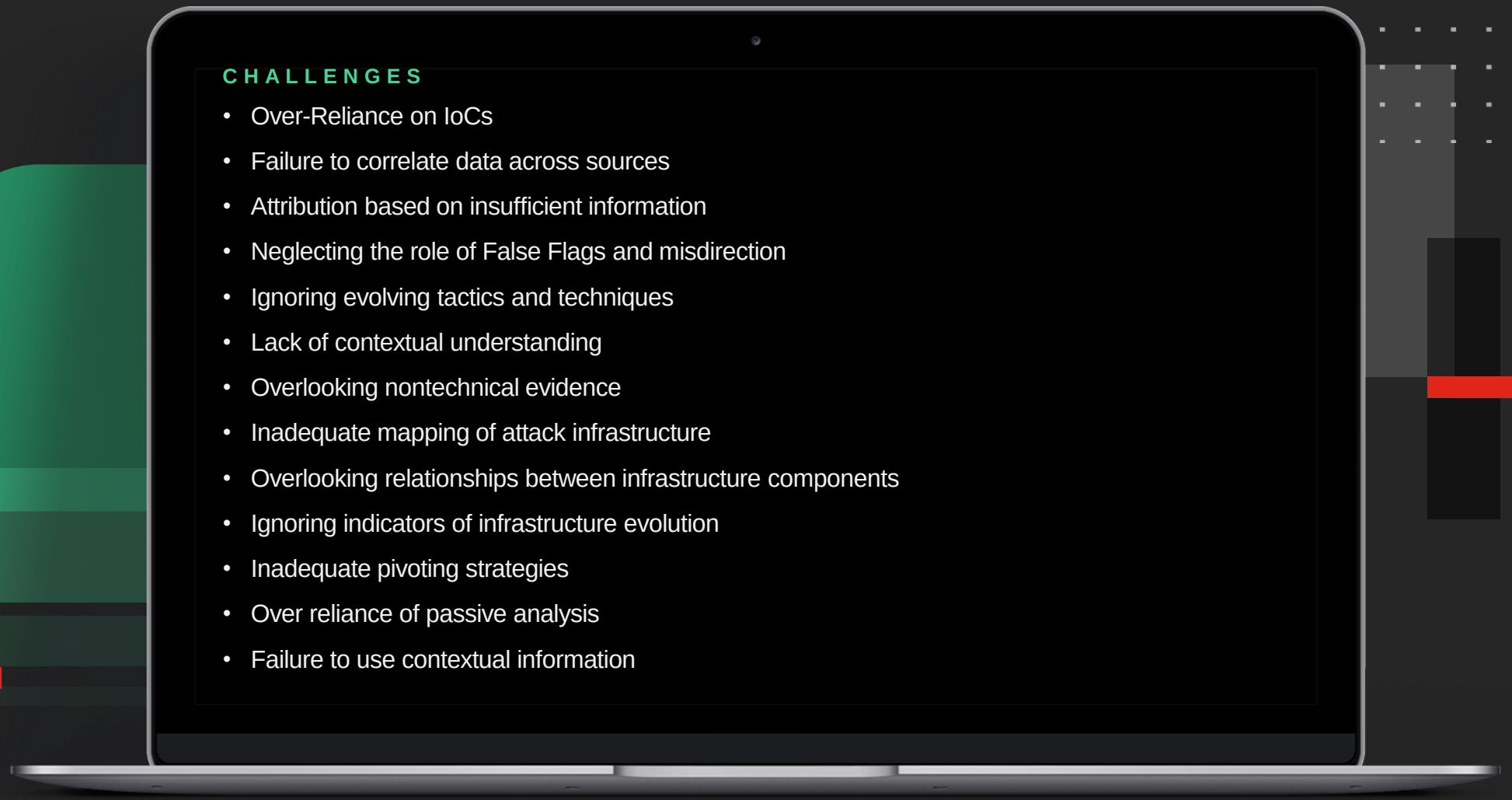
ATTRIBUTION

Attribution of APTs

Connecting the Dots



Attribution Challenges




FORTINET