

A composite image featuring a variety of animals in an urban environment. In the foreground, a lion, a leopard, an elephant with a monkey on its back, a giraffe with a meerkat on its back, a zebra, a rhinoceros, and a crocodile are positioned on a blue surface. The background shows a city skyline with various skyscrapers and birds flying in the sky. The word 'squad' is written in white lowercase letters in the top left corner.

squad

MIX YOUR
TALENT

Forensics réseau – Forensics terminaux mobiles



Réseau



Terminaux mobiles



Réseau

Les périphériques réseaux

Lequel de ces périphériques n'est pas un périphérique réseau ?

- A. Antivirus
- B. Hub
- C. IDS
- D. Pare-feu
- E. Routeur
- F. Serveur DHCP
- G. Serveur DNS
- H. Serveur Proxy
- I. Serveur SMTP
- J. Serveur Web
- K. Switch



Réseau

Les périphériques réseaux (1/2)

Lequel de ces périphériques n'est pas un périphérique réseau ?

A. Antivirus

B. Hub

Un hub Ethernet est un appareil informatique permettant de concentrer les transmissions Ethernet de plusieurs équipements sur un même support dans un réseau informatique local.

C. IDS

Un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée.

D. Pare-feu

Un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau.

E. Routeur

Un équipement réseau informatique assurant le routage des paquets.

F. Serveur DHCP

Un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine.



Réseau

Les périphériques réseaux (2/2)

Lequel de ces périphériques n'est pas un périphérique réseau ?

G. Serveur DNS

Le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP ou autres enregistrements.

H. Serveur Proxy

Un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.

I. Serveur SMTP

Un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique.

J. Serveur Web

Un serveur multi-service, utilisé le plus souvent pour publier des sites web sur Internet ou un intranet.

K. Switch

Un commutateur réseau, équipement ou appareil qui permet l'interconnexion d'appareils communicants, terminaux, ordinateurs, serveurs, périphériques reliés à un même réseau physique.



Réseau

Format d'une capture de paquets

Wireshark interface showing a packet capture. The packet list displays various protocols including SNMP, DNS, and TCP. The packet details pane shows the structure of a DNS response (Standard query response A) for the domain www.cnn.com, including the request ID, flags, and the answer section.

Filter: Expression... Clear Apply

No. .	Time	Source	Destination	Protocol	Info
366	11.767290	192.168.0.31	192.168.0.28	SNMP	get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.7.1
367	11.768865	192.168.0.28	192.168.0.31	SNMP	get-request SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
369	11.775952	192.168.0.31	192.168.0.28	SNMP	get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
381	12.286091	192.168.0.28	192.168.0.1	DNS	Standard query A www.cnn.com
384	12.311862	192.168.0.1	192.168.0.28	DNS	Standard query response A 64.236.91.21 A 64.236.91.23 A 64.236.91.25
385	12.312727	192.168.0.28	64.236.91.21	TCP	56606 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2
386	12.361495	64.236.91.21	192.168.0.28	TCP	http > 56606 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460
387	12.361583	192.168.0.28	64.236.91.21	TCP	56606 > http [ACK] Seq=1 Ack=1 win=17520 Len=0
388	12.361805	192.168.0.28	64.236.91.21	HTTP	GET / HTTP/1.1
389	12.413166	64.236.91.21	192.168.0.28	TCP	http > 56606 [ACK] Seq=1 Ack=845 win=6960 Len=0
390	12.413611	64.236.91.21	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
391	12.414386	64.236.91.21	192.168.0.28	TCP	[TCP segment of a reassembled PDU]

Frame 384 (167 bytes on wire, 167 bytes captured)

Ethernet II, Src: Sparklan_04:d0:9e (00:0e:8e:04:d0:9e), Dst: HonHaiPr_26:66:a2 (00:1c:26:26:66:a2)

Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.28 (192.168.0.28)

User Datagram Protocol, Src Port: domain (53), Dst Port: 62872 (62872)

Domain Name System (response)

[Request ID: 381]

[Time: 0.025771000 seconds]

Transaction ID: 0xcff1f

Flags: 0x8180 (standard query response, No error)

Questions: 1

Answer RRs: 6

Authority RRs: 0

Additional RRs: 0

Queries

www.cnn.com: type A, class IN

Name: www.cnn.com

Type: A (Host address)

Class: IN (0x0001)

Answers

www.cnn.com: type A, class IN, addr 64.236.91.21

0000 00 1c 26 26 66 a2 00 0e 8e 04 d0 9e 08 00 45 00 ..&&f... ..E.

0010 00 99 00 00 40 00 40 11 b8 e6 c0 a8 00 01 c0 a8@.

0020 00 1c 00 35 f5 98 00 85 98 5a cf 1f 81 80 00 01 ...5... .Z....

0030 00 06 00 00 00 00 03 77 77 77 03 63 6e 6e 03 63w ww.cnn.c

0040 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00 om.....

0050 b7 00 04 40 ec 5b 15 c0 0c 00 01 00 01 00 00 00 ...@. [...]

0060 b7 00 04 40 ec 5b 17 c0 0c 00 01 00 01 00 00 00 ...@. [...]

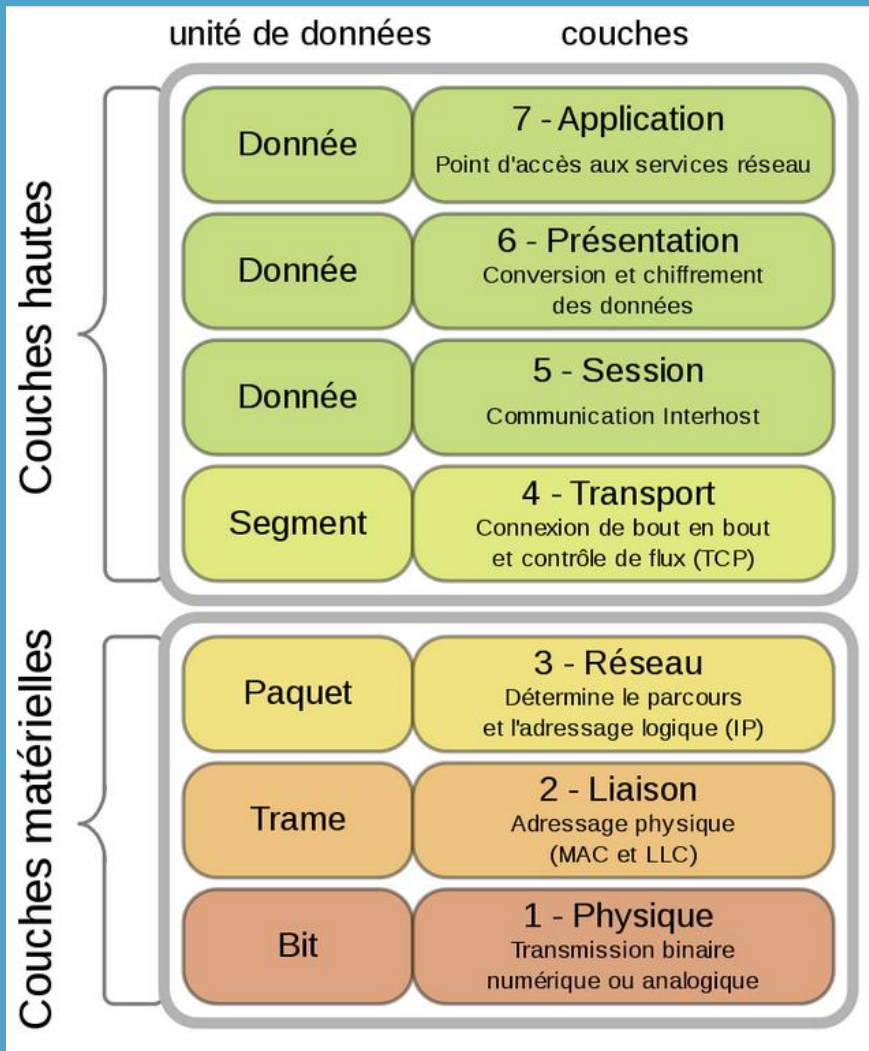
0070 b7 00 04 40 ec 10 14 c0 0c 00 01 00 01 00 00 00 ...@.....

This is a response to the DNS query in this fr... Packets: 1273 Displayed: 909 Marked: 0 Dropped: 0 Profile: Default

pcap (« packet capture ») est une interface de programmation permettant de capturer un trafic réseau. Elle est implémentée sous les systèmes GNU/Linux, FreeBSD, NetBSD, OpenBSD et Mac OS X par la bibliothèque *libpcap*. WinPcap est le portage sous Windows de *libpcap*.



Réseau Modèle OSI



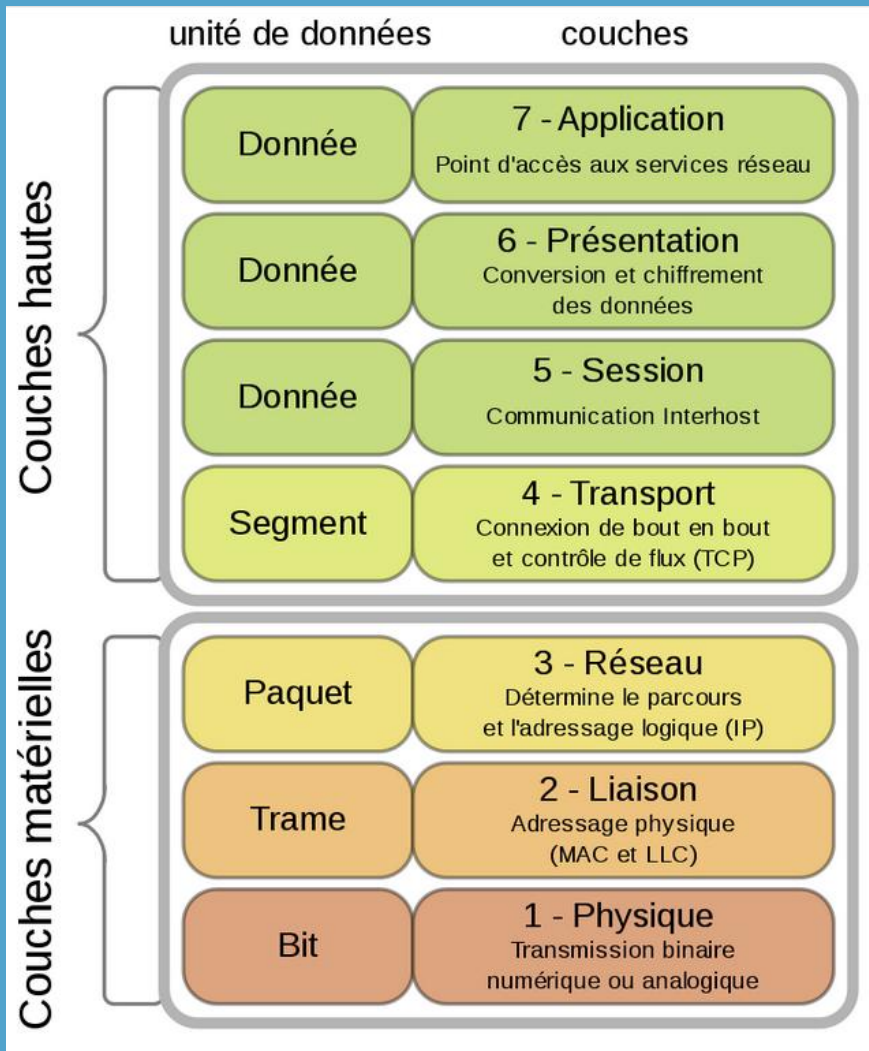
Le protocole UDP est un protocole de quel niveau du modèle OSI ?

Quel est le protocole pour convertir une adresse IP (niveau 3) en adresse MAC (niveau 2) ?

Comment un pare-feu peut-il bloquer un tunnel SSH s'il ne connaît pas sur quel port TCP il transite ?



Réseau Modèle OSI



Le protocole UDP est un protocole de quel niveau du modèle OSI ?

Niveau 4 - Transport

Quel est le protocole pour convertir une adresse IP (niveau 3) en adresse MAC (niveau 2) ?

ARP

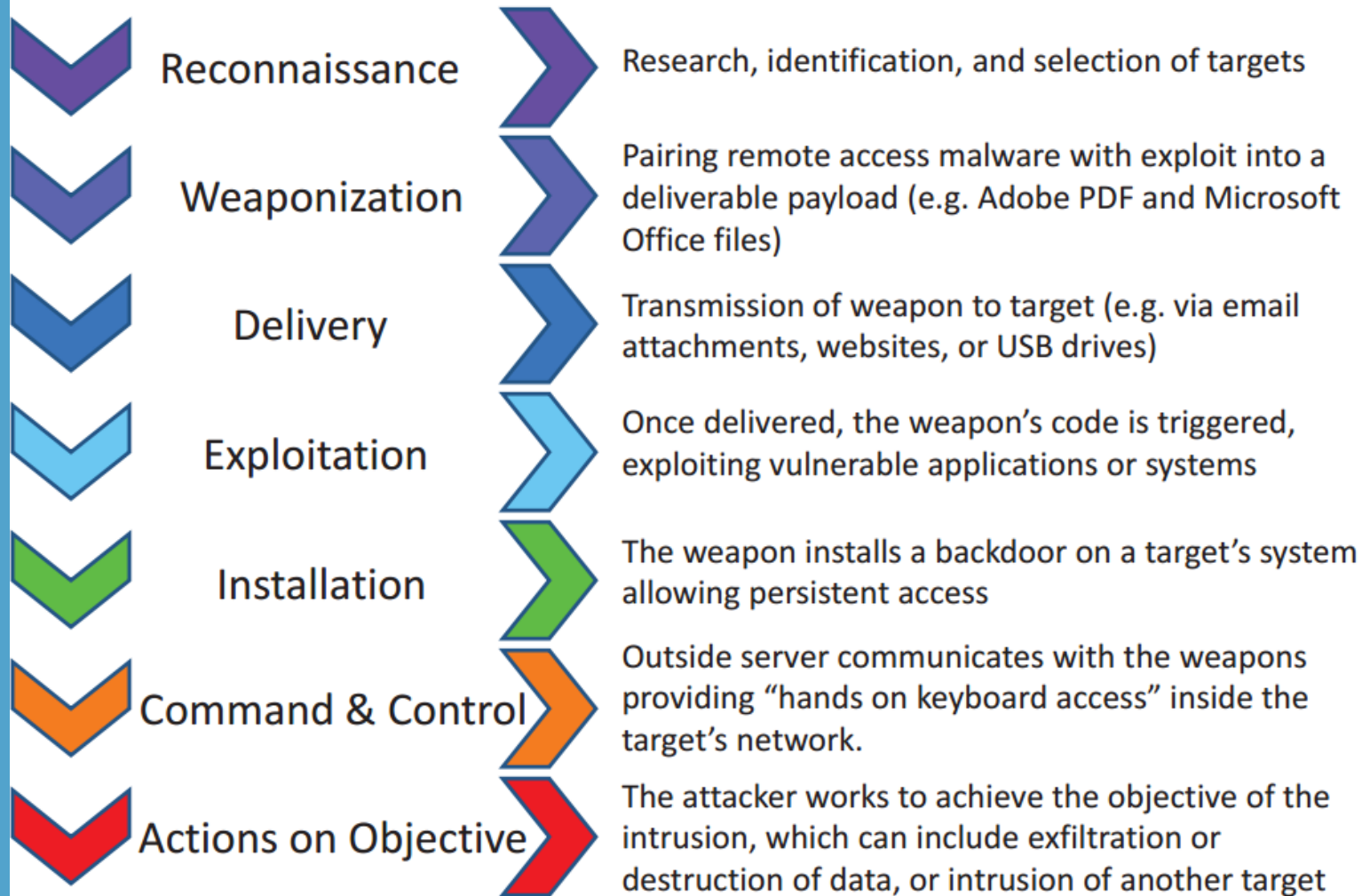
Comment un pare-feu peut-il bloquer un tunnel SSH s'il ne connaît pas sur quel port TCP il transite ?

Le pare-feu doit être un pare-feu applicatif qui analyse la couche 7 du modèle OSI.



Réseau Cyber Kill Chain

Phases of the Intrusion Kill Chain





Réseau

Indicateur de compromission

IOC - (anglais pour "Indicator of Compromise") - en informatique forensics est un artefact observé sur un réseau ou dans un système d'exploitation qui indique une intrusion informatique.

Lesquels de ces éléments sont des indicateurs de compromission ?

- A. Adresse IP
- B. Hash MD5
- C. Mutex
- D. Nom de domaine
- E. Nom de fichier
- F. Nom de virus
- G. Numéro de série de smartphone
- H. Protocole réseau
- I. URL



Réseau

Indicateur de compromission

IOC - (anglais pour "Indicator of Compromise") - en informatique forensics est un artefact observé sur un réseau ou dans un système d'exploitation qui indique une intrusion informatique.

Lesquels de ces éléments sont des indicateurs de compromission ?

- A. Adresse IP
- B. Hash MD5
- C. Mutex
- D. Nom de domaine
- E. Nom de fichier
- F. Nom de virus
- G. Numéro de série de smartphone
- H. Protocole réseau
- I. URL



Une connexion sur un site malveillant a été détectée par une sonde chez une filiale du client. Après analyse du JavaScript offusqué, il s'avérait que le site d'un important vendeur d'électroménager était compromis et redirigeait sur des sites malveillants. Le propriétaire du site a été informé.

PUBLIC



Réseau

Cas concret d'incident

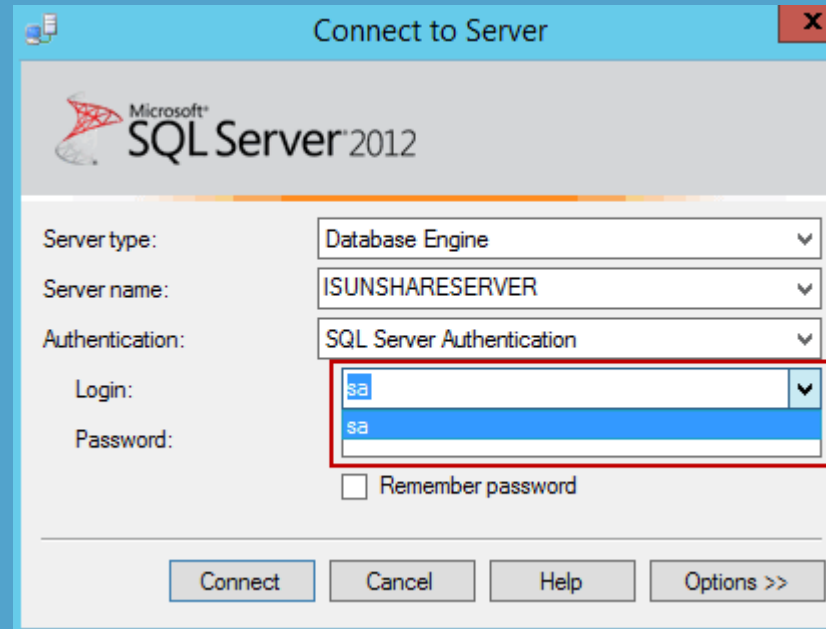
```
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-09-13 13:00 CEST
Nmap scan report for 192.168.1.14
Host is up (0.010s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          Unreal ircd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:0C:29:BC:7D:F4 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, localhost, irc.metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Un scan interne est détecté, c'est-à-dire qu'une machine du client semble scanner un serveur du client. L'investigation a permis de confirmer que ce n'était pas un scan malveillant mais que c'était un produit utilisé par le client qui effectue un balayage réseau lors de son exécution.



Réseau

Cas concret d'incident



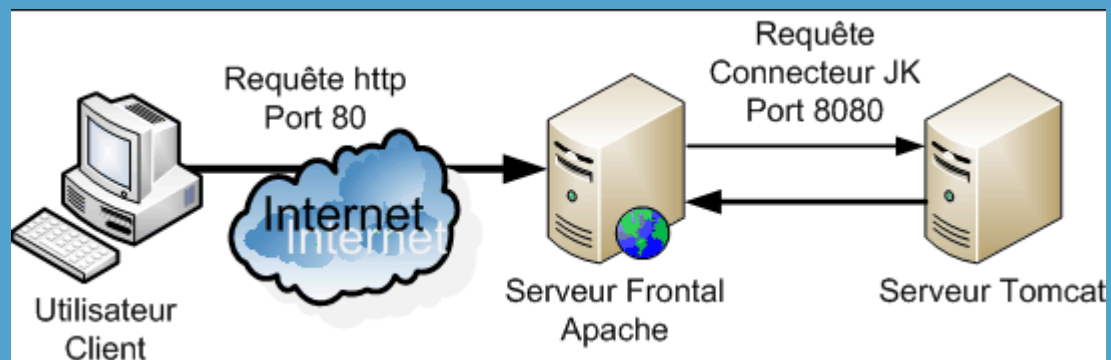
Une alerte du SIEM a sonné concernant un scan du compte sa sur SQL.
L'investigation a permis de comprendre que c'était un faux-positif lié à une sauvegarde d'un fichier de journalisation des connexions SQL qui est passé sur le même port TCP que les connexions SQL. Ainsi, les nombreuses connexions vues en peu de temps étaient en fait le contenu du fichier de journalisation lors de son transit.



Réseau

Cas concret d'incident

Une alerte a été remontée par l'IDS local sur un serveur. Après analyse, c'était un faux-positif car elle concernait une application non-présente sur le serveur. Cependant cela nous a fait découvrir que ce serveur présentait des services en frontal sur Internet alors que le client l'ignorait. Un scan de vulnérabilité a été demandé et a révélé des vulnérabilités potentielles. Une investigation dans les logs du serveur a permis de valider qu'aucun attaquant n'a exploité ces vulnérabilités.





Réseau

Cas concret d'incident

```
File Edit Search View Tools Options Language Buffers Help
[Icons] [Search]

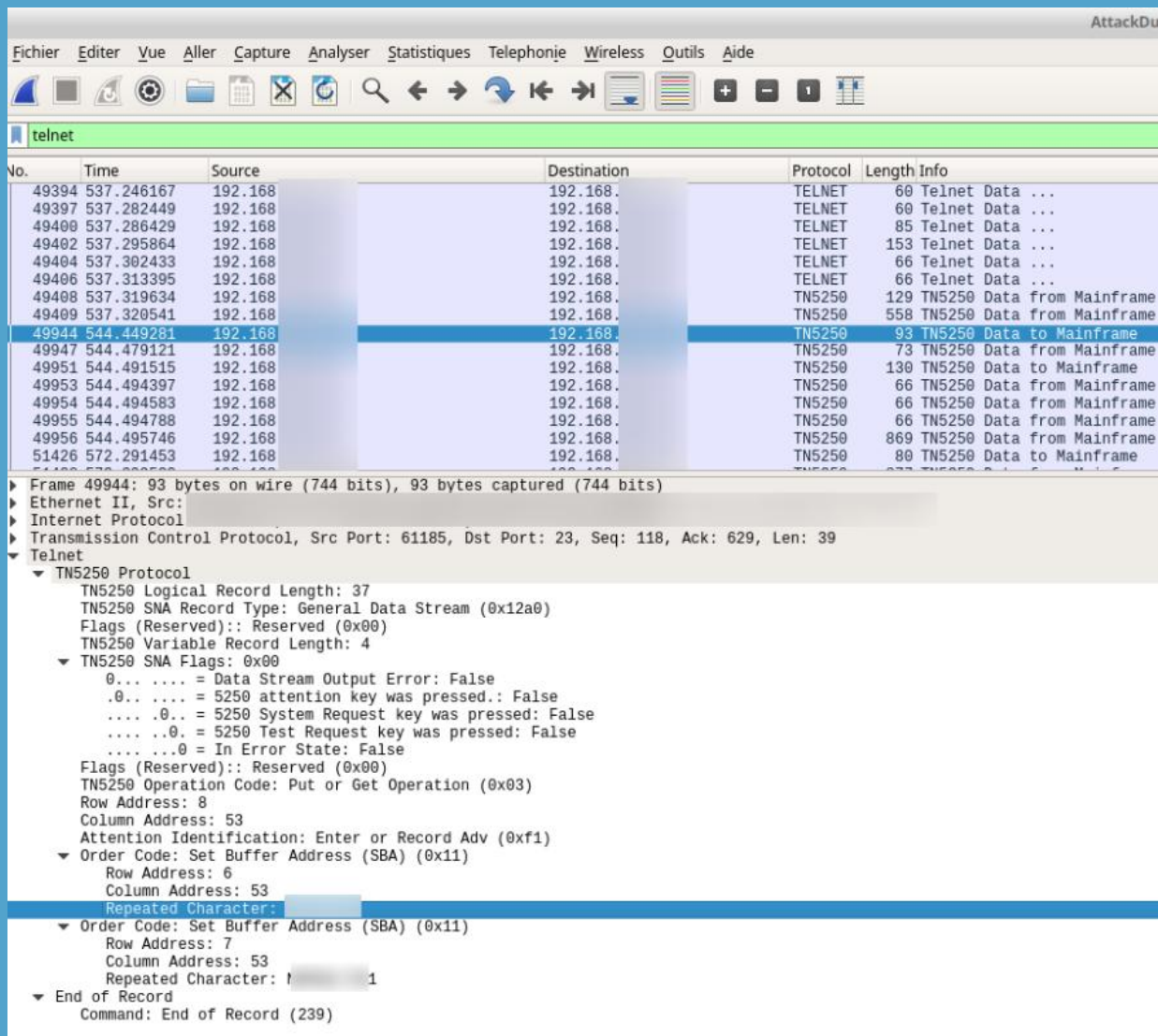
79 GUICtrlSetState(-1, $GUI_DISABLE)
80 GUICtrlCreateGroup("", -99, -99, 1, 1) ;close group
81
82 GUICtrlCreateGroup("Timeout", 230, 450, 200, 50)
83 $idTimeout = GUICtrlCreateInput("", 240, 470, 100, 20, $ES_NUMBER)
84 GUICtrlSetTip(-1, "Optional Timeout in seconds. After the timeout has elapsed the message box will be automatically closed.")
85 GUICtrlCreateGroup("", -99, -99, 1, 1) ;close group
86
87 $idBTNPVIEW = GUICtrlCreateButton("&Preview", 10, 510, 100)
88 GUICtrlSetTip(-1, "Show the MessageBox")
89 $idBTNCOPY = GUICtrlCreateButton("&Copy", 120, 510, 100)
90 GUICtrlSetTip(-1, "Copy the generated AutoIt code to the Clipboard")
91 $idBTNEXIT = GUICtrlCreateButton("&Exit", 230, 510, 100)
92 GUICtrlSetTip(-1, "Quit the program")
93
94 $idButton = $idOptOK
95
96 GUISetState() ; will display an empty dialog box
97
98 ; Run the GUI until the dialog is closed
99 While 1
100     $iMSG = GUIGetMsg()
101     Select
102     Case $iMSG = $GUI_EVENT_CLOSE Or $iMSG = $idBTNEXIT
103         Exit
104
105     Case $iMSG = $idOptOK
106         $idButton = $idOptOK
107         GUICtrlSetState($idOptFirst, $GUI_CHECKED)
108         GUICtrlSetState($idOptFirst, $GUI_ENABLE)
109         GUICtrlSetState($g_idOptSecond, $GUI_DISABLE)
110         GUICtrlSetState($g_idOptThird, $GUI_DISABLE)
111
112     Case $iMSG = $g_idOptOkCancel
113         $idButton = $g_idOptOkCancel
114         GUICtrlSetState($idOptFirst, $GUI_CHECKED)
115         GUICtrlSetState($idOptFirst, $GUI_ENABLE)
116         GUICtrlSetState($g_idOptSecond, $GUI_ENABLE)
```

Un callback vers un site malveillant a été détecté par une sonde. L'analyse des traces forensique remontées par un outil en interne a permis de trouver le processus initiant cette connexion. Le programme malveillant était lancé au démarrage et consistait à lancer un script autoIT offusqué qu'il a fallu analyser à la main car il avait des mécanismes de détection de machine virtuelle. Le malware a été envoyé à une compagnie d'antivirus.

1

Réseau

Cas concret d'incident



No.	Time	Source	Destination	Protocol	Length	Info
49394	537.246167	192.168.	192.168.	TELNET	60	Telnet Data ...
49397	537.282449	192.168.	192.168.	TELNET	60	Telnet Data ...
49400	537.286429	192.168.	192.168.	TELNET	85	Telnet Data ...
49402	537.295864	192.168.	192.168.	TELNET	153	Telnet Data ...
49404	537.302433	192.168.	192.168.	TELNET	66	Telnet Data ...
49406	537.313395	192.168.	192.168.	TELNET	66	Telnet Data ...
49408	537.319634	192.168.	192.168.	TN5250	129	TN5250 Data from Mainframe
49409	537.320541	192.168.	192.168.	TN5250	558	TN5250 Data from Mainframe
49944	544.449281	192.168.	192.168.	TN5250	93	TN5250 Data to Mainframe
49947	544.479121	192.168.	192.168.	TN5250	73	TN5250 Data from Mainframe
49951	544.491515	192.168.	192.168.	TN5250	130	TN5250 Data to Mainframe
49953	544.494397	192.168.	192.168.	TN5250	66	TN5250 Data from Mainframe
49954	544.494583	192.168.	192.168.	TN5250	66	TN5250 Data from Mainframe
49955	544.494788	192.168.	192.168.	TN5250	66	TN5250 Data from Mainframe
49956	544.495746	192.168.	192.168.	TN5250	869	TN5250 Data from Mainframe
51426	572.291453	192.168.	192.168.	TN5250	80	TN5250 Data to Mainframe

Frame 49944: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0

Ethernet II, Src: [redacted], Dst: [redacted]

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2

Transmission Control Protocol, Src Port: 61185, Dst Port: 23, Seq: 118, Ack: 629, Len: 39

Telnet

▼ TN5250 Protocol

TN5250 Logical Record Length: 37

TN5250 SNA Record Type: General Data Stream (0x12a0)

Flags (Reserved):: Reserved (0x00)

TN5250 Variable Record Length: 4

▼ TN5250 SNA Flags: 0x00

0... .. = Data Stream Output Error: False

.0... .. = 5250 attention key was pressed.: False

... .0... = 5250 System Request key was pressed: False

... .0... = 5250 Test Request key was pressed: False

... ..0 = In Error State: False

Flags (Reserved):: Reserved (0x00)

TN5250 Operation Code: Put or Get Operation (0x03)

Row Address: 8

Column Address: 53

Attention Identification: Enter or Record Adv (0xf1)

▼ Order Code: Set Buffer Address (SBA) (0x11)

Row Address: 6

Column Address: 53

Repeated Character: [redacted]

▼ Order Code: Set Buffer Address (SBA) (0x11)

Row Address: 7

Column Address: 53

Repeated Character: [redacted]

▼ End of Record

Command: End of Record (239)

Un port maritime en Afrique a demandé un audit suite à une répétition de compromission d'un compte d'accès à l'application gérant le port. L'administrateur a changé son mot de passe 3 fois mais à chaque fois il constate des connexions avec son compte à des heures où il n'était pas présent. Rien d'intéressant n'a été trouvé sur le système cible ni sur le poste de travail de l'administrateur. Une sonde d'enregistrement des flux entre son poste et le système a été placée. Après analyse, il s'avérait qu'une machine effectuait du man-in-the-middle. Tous les flux étaient chiffrés sauf... l'administration du mainframe qui s'effectuait en « telnet ». Il est très probable que la récupération du mot de passe a été effectué à chaque fois avec cette méthode.



1

Réseau



2

Terminaux mobiles



Terminaux mobiles

Introduction

L'inforensique sur mobile est devenue extrêmement importante pour les investigations judiciaires à cause de la richesse des preuves qu'elle peut fournir. Ce type d'information peut même être plus important que les preuves obtenus sur un ordinateur traditionnel car le téléphone portable est toujours allumé et on peut l'emporter partout. Les outils d'inforensique à ce sujet sont en cours d'évolution mais il y a encore des smartphones qui ne sont pas supportés.

Les terminaux mobiles sont problématiques à analyser car il y a un grand nombre de système d'exploitation et de modèles disponible. De plus, les données sur le téléphone sont modifiées en permanence. Le contenu d'un smartphone ne peut être analysé en une fois car il y a plusieurs éléments à prendre en compte (la mémoire amovible et la carte SIM).

Les autres terminaux mobiles, comme les tablettes et les GPS, sont également une source d'information importante lors d'une investigation. Comme tous ces équipements n'ont pas forcément d'outils inforensique associés, l'investigateur-riche doit toujours tester l'outil inforensique qu'il utilise avant son utilisation dans le cadre de l'investigation.

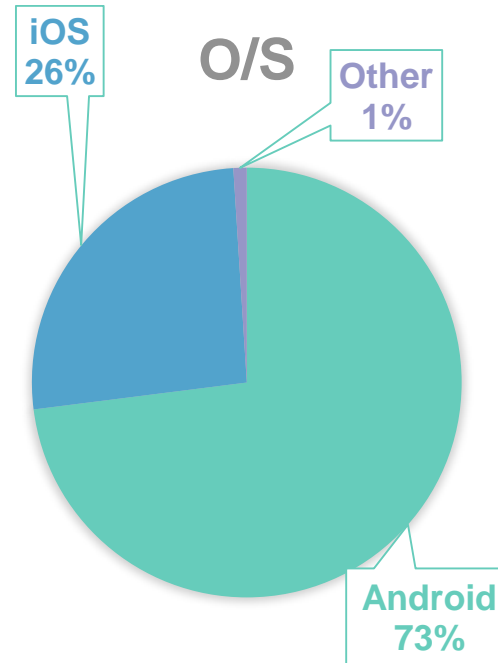
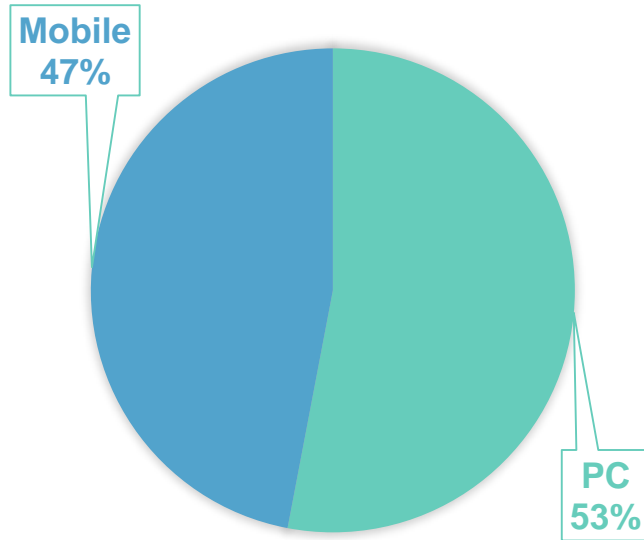


2

Terminaux mobiles

Aperçu de l'usage des smartphones

PÉRIPHÉRIQUES SE CONNECTANT À INTERNET



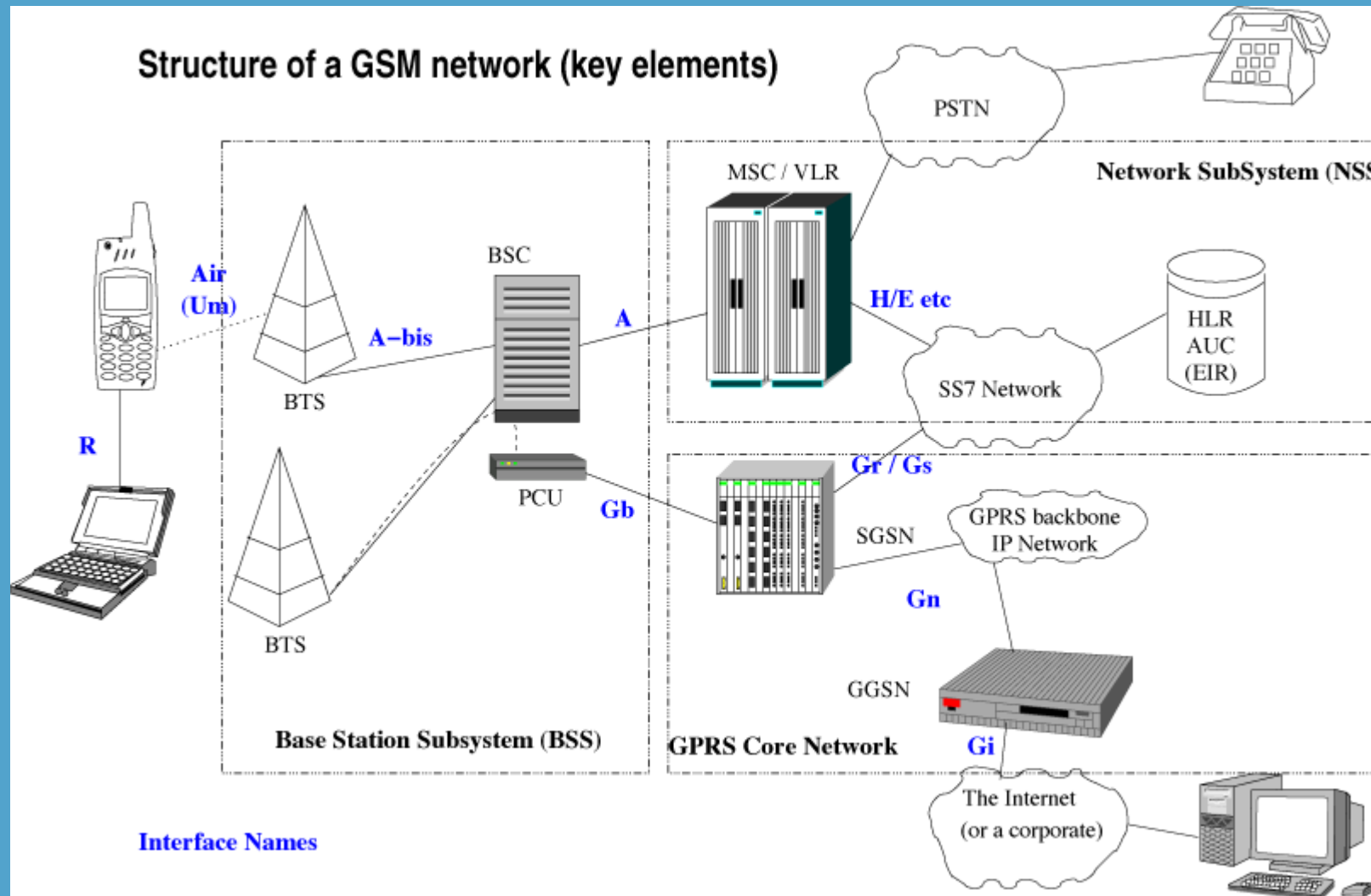
statcounter.com 2020



2

Terminaux mobiles

Le réseau cellulaire



Le réseau spécifique pour le GSM s'appelle PLMN (Public Land Mobile Network), chaque opérateur ayant le sien propre. Il est relié au Réseau Téléphonique Commuté Public (RTCP), mais aussi directement aux autres réseaux de téléphonie mobile (UMTS, LTE) et à ceux des autres opérateurs.

2

Terminaux mobiles La problématique des smartphones

Comme les smartphones communiquent en permanence, afin d'éviter que le réseau puisse altérer les preuves, il est recommandé de mettre le smartphone dans une cage de Faraday à la perquisition.

Cependant, comme les smartphones ont souvent la batterie qui ne tient pas longtemps, il y a un risque à ce qu'il se décharge et que des mécanismes supplémentaires soient en place (PIN, mot de passe...). Mettre le smartphone dans la cage de Faraday avec le fil d'alimentation qui sort du sac pour être sûr qu'il ne se décharge pas n'est pas la solution optimal car le fil d'alimentation empêche la cage de Faraday de fonctionner correctement.





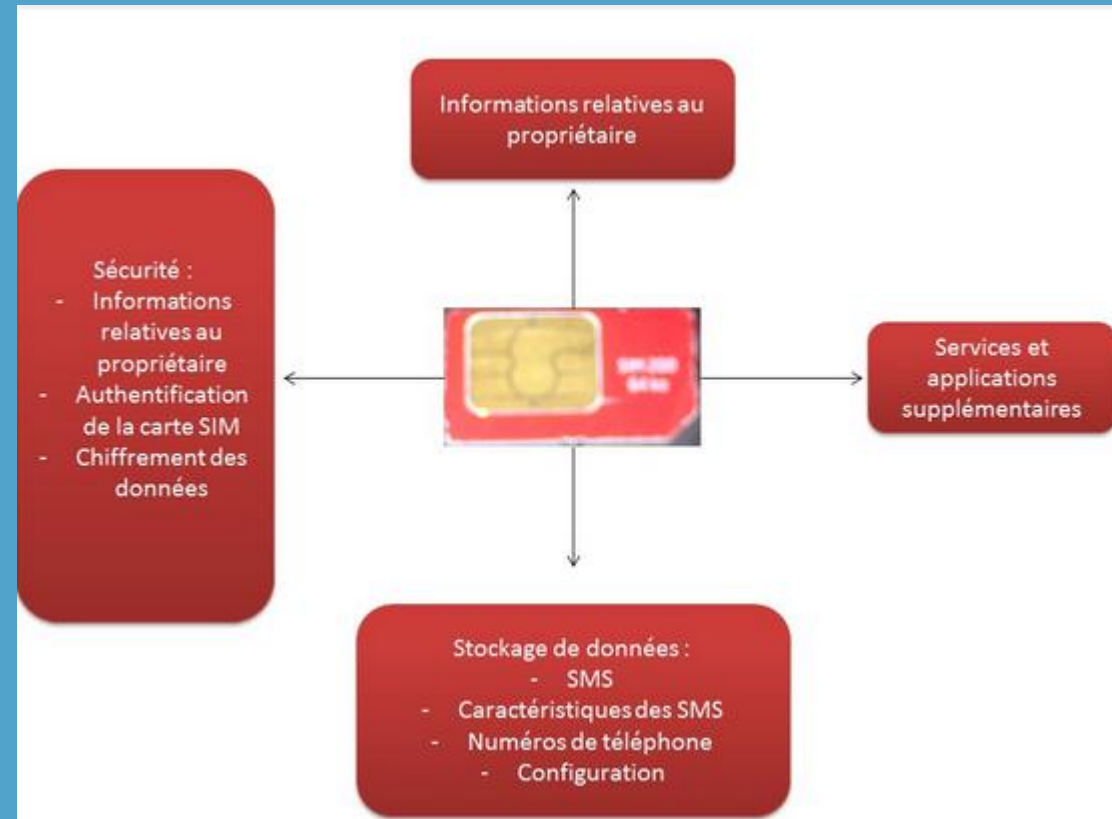
Terminaux mobiles

La carte SIM

Pour mieux comprendre la carte SIM, voir <https://www.hackersrepublic.org/hacking-mobile/la-sim-dans-tous-ses-etats>

Voici une liste d'outil permettant l'analyse inforensique d'un téléphone portable et de sa carte SIM :

- BitPim
- Mobile Phone Examiner
- MOBILedit! Forensic
- Device Seizure
- SIMcon
- XAMN





Terminaux mobiles

Android

Android est un système d'exploitation mobile fondé sur le noyau Linux et développé actuellement par Google.

Quelles sont les moyens disponibles pour extraire des preuves inforensiques d'Android ?

- A. A travers la prise jack du smartphone
- B. En demandant le support de la NSA
- C. En retirant la puce du smartphone
- D. JTAG
- E. Logique en copiant les fichiers accessibles
- F. Physique en acquérant l'image du backup
- G. Via l'alimentation du smartphone



Terminaux mobiles

Android

Android est un système d'exploitation mobile fondé sur le noyau Linux et développé actuellement par Google.

Quelles sont les moyens disponibles pour extraire des preuves inforensiques d'Android ?

- A. A travers la prise jack du smartphone
- B. En demandant le support de la NSA
- C. En retirant la puce du smartphone
En dernier recours, si aucune des autres méthodes ne fonctionne.
- D. JTAG
- E. Logique en copiant les fichiers accessibles
De préférence une copie intégrale depuis l'utilisateur *root* (à l'aide d'un exploit si nécessaire)
- F. Physique en acquérant l'image du backup
- G. Via l'alimentation du smartphone



Terminaux mobiles

Sandboxing applicatif sur Android et iOS

Ring 3 - Apps

Apps non-privilégiées

- Navigateur web
- Client mail
- Chat
- Jeux
- Apps bancaires

Mode développeur

Divers SDK

Ring 0 - Système

Apps privilégiées
Root/Jailbreak

Librairies système
Librairies de
sécurité/crypto

Drivers

Hardware

TEE/Enclave de sécurité/Embedded
Secure Element
Fonctions biométriques
Caractéristiques OEM

Réseau cellulaire
Bluetooth
Wifi
NFC

- Les Apps sont *sandboxées* en *userland* et doivent utiliser un IPC spécifique ou un système de fichier pour partager des données ainsi qu'enregistrer les permissions d'utilisation des caractéristiques de l'OS
- Les accès *root* baissent le niveau de sécurité du smartphone mais sont utiles pour l'inforensique
- Les sécurités du MDM peuvent être désactivé avec le client
- Les données et opérations sensibles sont stockées et effectuées dans un 'secure world' isolé du 'normal world' (Secure OS/Rich OS)

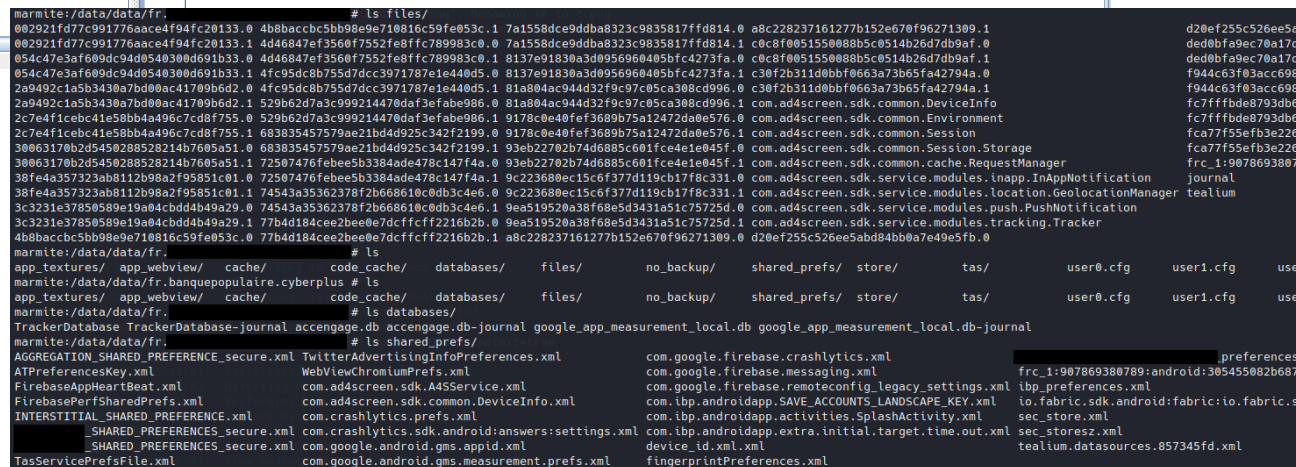


Terminaux mobiles iOS

iOS, anciennement iPhone OS, le « i » de iOS étant pour iPhone d'où la minuscule, est le système d'exploitation mobile développé par Apple pour plusieurs de ses appareils.

Pour un-e investigateur-ric(e), avec les versions d'iOS évoluant, il est de plus en plus difficile d'acquérir des preuves inforensiques car le niveau de chiffrement et de sécurité a augmenté. De moins en moins de gens synchronisent leur iOS avec leur Mac ou PC car ce n'est plus requis dans le processus d'activation. Les smartphones sont à présent synchronisés à travers l'iCloud.



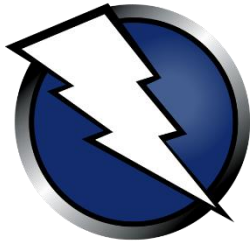


- Secrets codés en dur
- Cryptographie utilisé
- Les hôtes distants avec qui ça communique
- Les certificats
- La détection d'une action en *root* ou qui essaie de modifier le système du smartphone
- Les accès au système de fichier ou aux bases de données
- Les interceptions de schémas d'URL
- ...

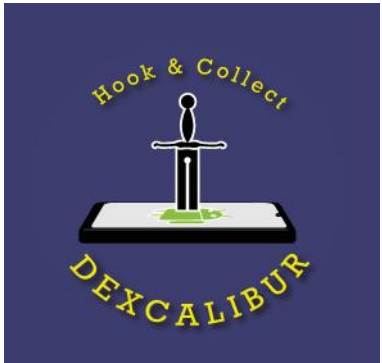


Terminaux mobiles

Analyse dynamique



drozer



FRIIDA

Un émulateur peut être utilisé mais l'utilisation d'un smartphone *rooté* est moins détectable par le programme malveillant.

Genymotion est pratique pour émuler de nombreuses version d'Android rapidement .



Terminaux mobiles

Analyse statique et dynamique automatisé



The screenshot displays the MobSF Static Analyzer web interface. The browser address bar shows the URL: `localhost:8000/StaticAnalyzer/?name=com.ZeroMotorcycles-1.apk&type=apk&checksum=38dd9d9354e73c1e7c4bd82e01cf1dbb`. The interface is divided into several sections:

- APP SCORES:** Shows an average CVSS score of 5.2, a security score of 60/100, and 1/302 trackers detected.
- FILE INFORMATION:** Lists file details such as File Name (`com.ZeroMotorcycles-1.apk`), Size (19.57MB), MD5, SHA1, and SHA256 hashes.
- APP INFORMATION:** Provides metadata including App Name (Zero Motorcycles), Package Name (`com.ZeroMotorcycles`), Main Activity (`com.zeromotorcycles.ui.setup.SetupActivity`), Target SDK (27), Min SDK (23), and Android Version Name (2.0.0).
- PLAYSTORE INFORMATION:** Displays app details from the Google Play Store, including Title (Zero Motorcycles), Score (3.02), Installs (10,000+), Price (0), Android Version Support, Category (Lifestyle), Play Store URL, Developer (Zero Motorcycles), Developer ID (Zero+Motorcycles), Developer Address (380 El Pueblo Rd Scotts Valley CA, 95066), Developer Website (<http://www.zeromotorcycles.com/>), Developer Email (inquiries@zeromotorcycles.com), Release Date (Feb 18, 2013), Privacy Policy ([Privacy link](#)), and a Description.

The Description section states: "The Zero Motorcycles App is the perfect companion to your 100% electric Zero. The app utilizes your Android device's Bluetooth connection to communicate with any 2013 model year or later Zero Motorcycles model. The Zero App includes a 'Demo Mode' that allows you to browse the App and envision what it might be like to use this app with your own Zero. We encourage you to check it out. With the Zero App, you can:"

- Customize your motorcycle's performance by adjusting 'ECO mode' (2013 model year) or 'CUSTOM mode' (2014 model year and later) to set top speed, maximum torque, and deceleration and braking regenerative levels.
- View live data from your motorcycle in a configurable dashboard-like riding screen (options include torque, battery current, motor temperature, estimated range, and more).
- View detailed battery and performance data from the motorcycle when not in use.
- Get real-time estimates for recharge times as well as view battery voltage and total kilowatt-hours used.
- Gather trip statistics, including average watt-hours per mile, cost per mile, money saved v. gasoline and CO2 reduced vs gas.
- See the latest Zero Motorcycles news and updates through a discrete ticker.

At the bottom, there are four colored boxes with counts: 20 ACTIVITIES, 2 SERVICES, 0 RECEIVERS, and 4 PROVIDERS.



Terminaux mobiles

Cas concret d'incident

Une connexion sur un nœud Tor utilisé par WannaCry a été détectée par le SIEM. La connexion a été effectuée depuis un smartphone Android et l'utilisateur n'était pas au courant. Après recoupement avec les informations du proxy, il a été mis en évidence que c'était l'application Google Hangouts qui passait par des nœuds Tor !

L'investigation n'a pas été poussée plus loin mais il est probable que le nœud Tor est sur un serveur hébergeant également des services pour Hangouts.





Terminaux mobiles

Cas concret d'incident



Un outil de hacking a été détecté sur un poste d'un utilisateur qui n'a pas de numéro de téléphone dans l'annuaire. L'utilisateur ne répondant pas aux mails, j'ai appelé un par un les gens du même service que lui pour finir par trouver quelqu'un connaissant cet utilisateur et pouvant nous fournir son numéro de téléphone.

Il s'avérait en fait que l'utilisateur n'était pas du tout *IT-friendly* et que le poste était partagé par plusieurs personnes. A l'aide d'un rapport issu du SIEM, les autres utilisateurs de ce poste ont été retrouvés et avertis.



Terminaux mobiles

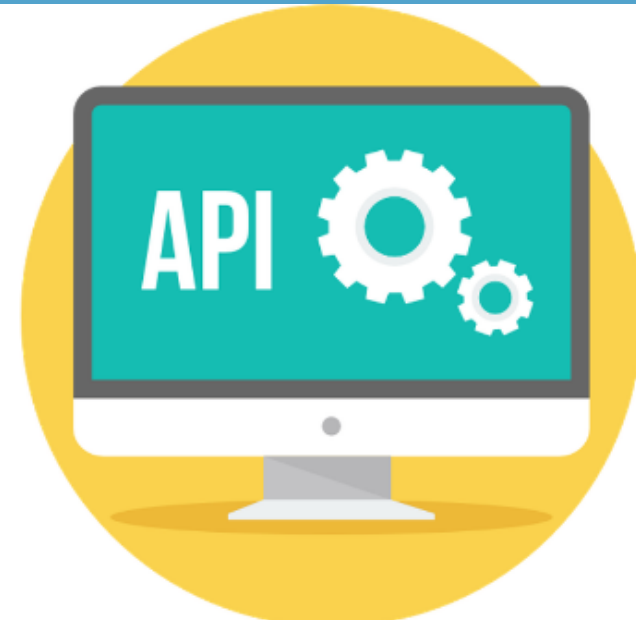
Cas concret d'incident

Une application smartphone basée sur le volontariat permet aux employé-es du client de déclarer s'ils ont le Covid-19 afin d'identifier et prévenir les personnes qui étaient dans le bâtiment en même temps.

De nombreux événements se sont retrouvés injectés et après analyse il s'avérait que la décompilation de l'application permettait de comprendre rapidement que l'authentifiant était basé sur le numéro de badge qu'il était facile de brute-forcer.



Event injection





Réseau

Si on résume ensemble :

- Les périphériques réseaux
- Format d'une capture de paquets
- Modèle OSI
- Cyber Kill Chain
- Indicateur de compromission
- Cas concret d'incident

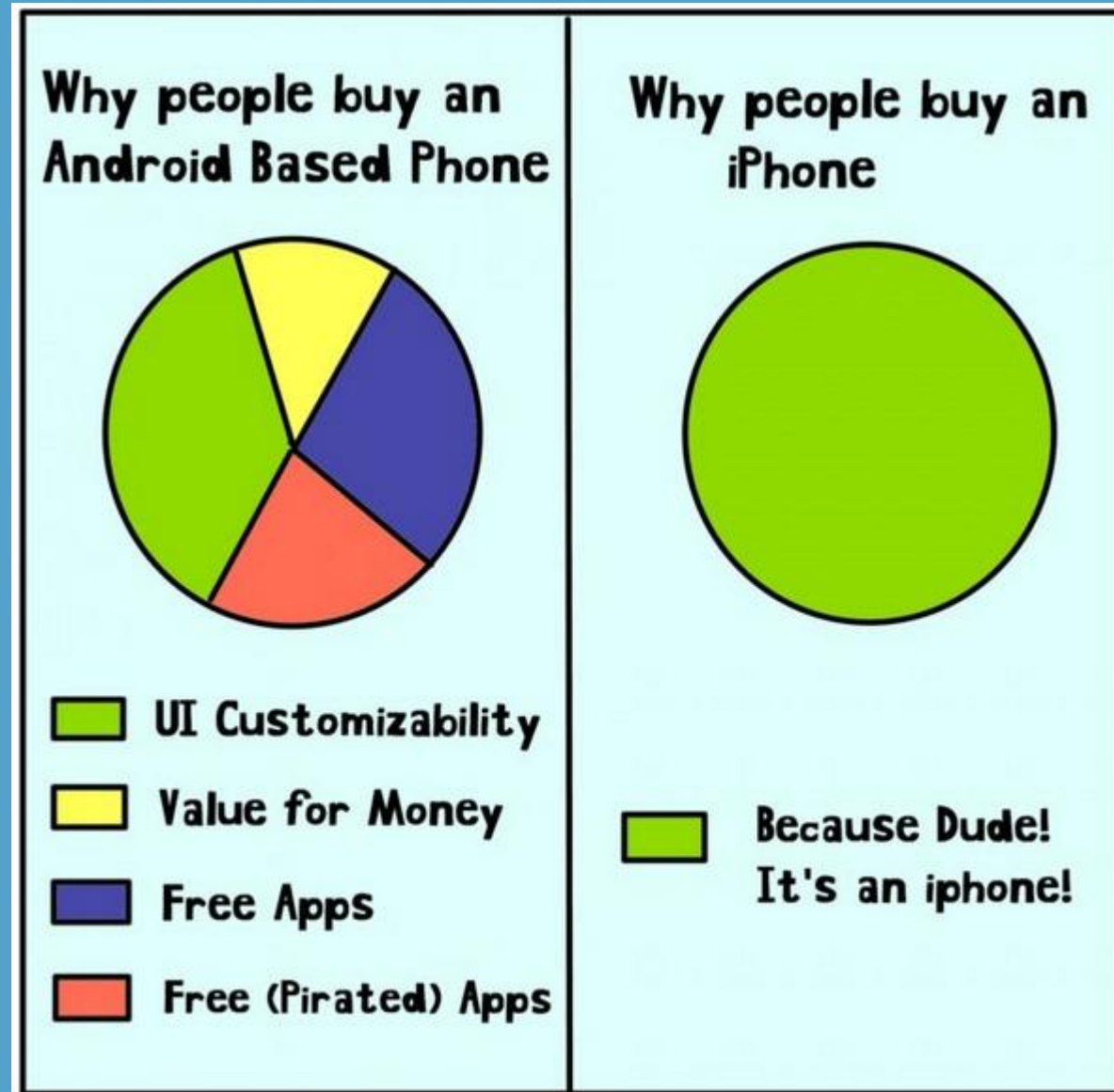
Si on résume ensemble :



Terminaux mobiles

- Introduction
- Aperçu de l'usage des smartphones
- Le réseau cellulaire
- La problématique des smartphones
- La carte SIM
- Android
- *Sandboxing* applicatif sur Android et iOS
- iOS
- Analyse statique
- Analyse dynamique
- Analyse statique et dynamique automatisé
- Cas concret d'incident

Conclusion



MERCI

www.squad.fr

PUBLIC

