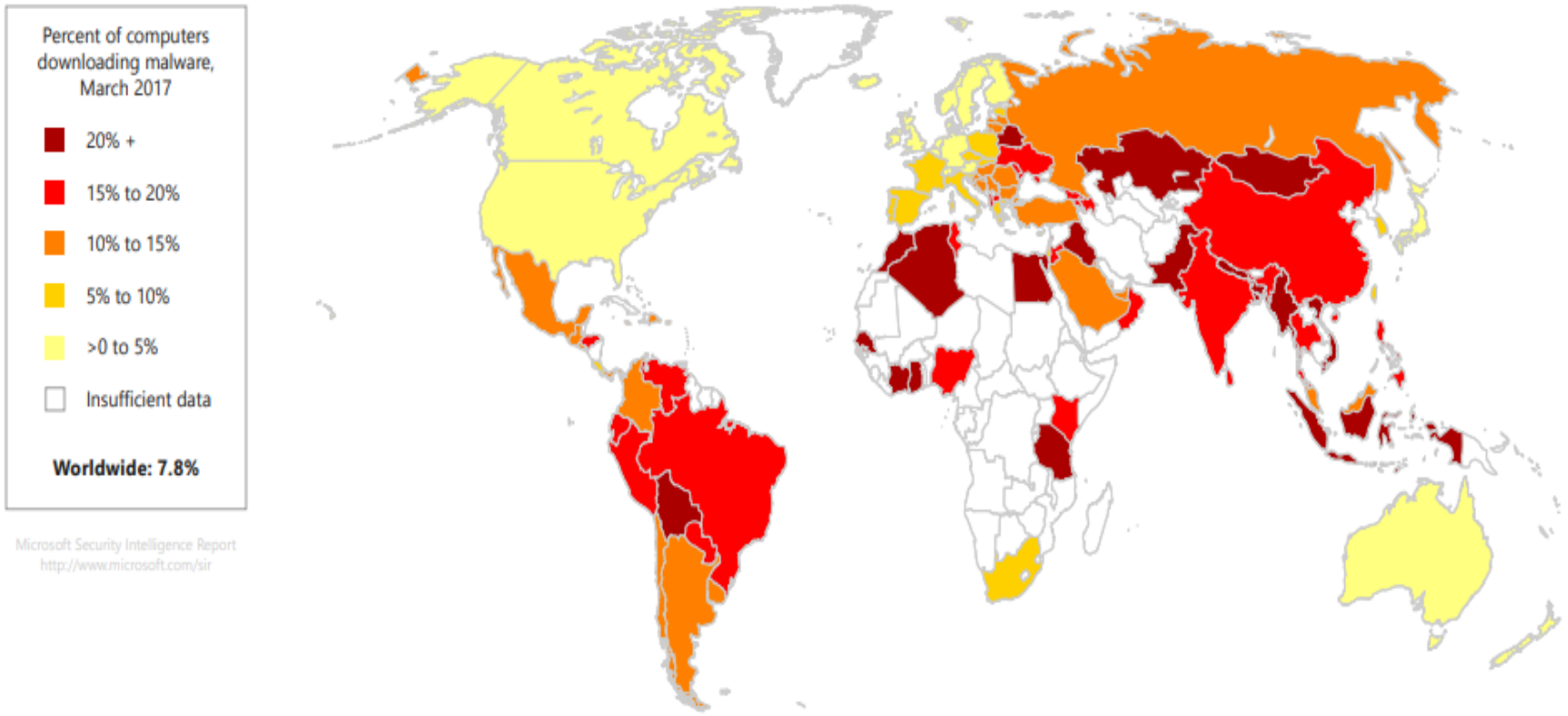
Les menaces informatiques

Dr. Noureddine Chikouche
noureddine.chikouche@univ-msila.dz
https://sites.google.com/view/chikouchenoureddine

Plan du cours

- Logiciels malveillants
- Les menaces de la messagerie électronique
- Protections

Encounter rate by country in March 2017



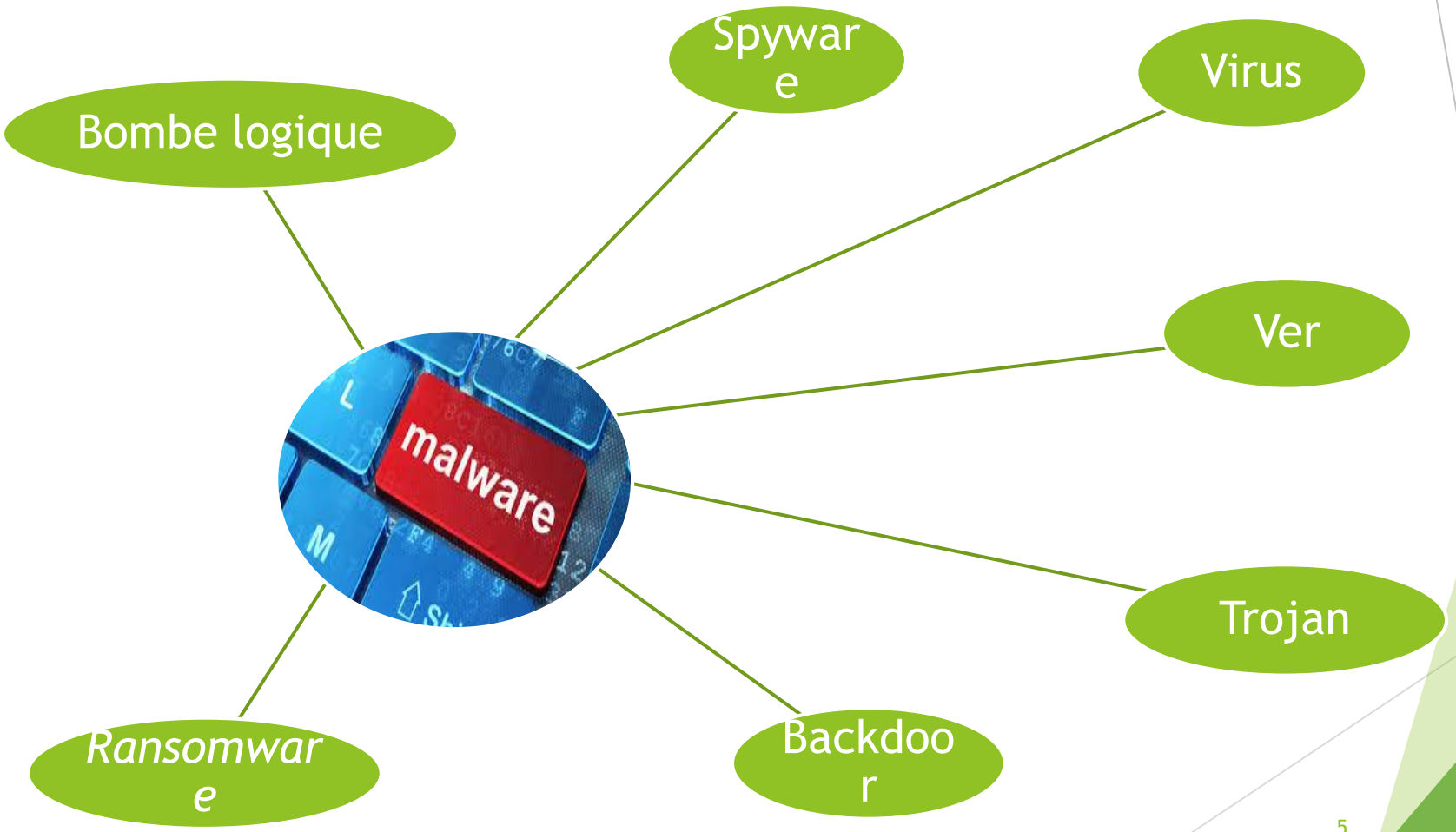
Source: Trends in Global Cybersecurity, Microsift, 2017

Threat category prevalence, worldwide and in 10 locations with the most computers reporting encounters

Category	Worldwide	Algeria	Bangladesh	Egypt	Indonesia	Iraq	Myanmar	Nepal	Pakistan	Palestinian Authority	Vietnam
Trojans	6.2	19.5	22.3	20.2	17.4	17.0	18.9	16.4	21.6	17.4	18.6
Worms	1.1	8.9	6.8	5.6	8.0	6.7	6.7	7.9	14.1	6.7	3.1
Downloaders & Droppers	0.7	2.1	1.7	2.3	1.2	1.1	1.1	2.0	2.2	1.1	0.7
Viruses	0.7	1.5	3.1	2.6	3.7	2.2	3.7	2.1	2.8	2.3	2.4
Other Malware	0.4	1.1	0.9	1.1	1.0	0.8	0.8	0.8	1.3	1.2	0.9
Obfuscators & Injectors	0.2	1.2	0.9	0.9	0.6	0.7	0.5	0.5	0.7	0.8	0.4
Backdoors	0.2	1.0	0.5	0.7	0.3	2.3	0.8	0.3	0.8	1.1	0.4
Password Stealers & Monitoring Tools	0.1	0.2	0.2	0.2	0.2	0.1	0.3	0.2	0.2	0.2	0.2
Ransomware	0.1	0.2	0.2	0.3	0.2	0.1	0.1	0.2	0.2	0.2	0.1
Exploits	0.1	0.2	0.1	0.2	0.2	0.1	0.2	0.1	0.1	0.2	0.1

Source: Trends in Global Cybersecurity, Microsift, 2017

Logiciels malveillants



Logiciels malveillants (*malware*)

Virus:

- Un virus est un programme qui s'exécute sur un ordinateur et peut se répandre à travers d'autres machines d'un système d'un information dans l'objectif de provoquer des perturbations dans les applications informatiques.
- Les virus résidents se chargent dans la mémoire vive de l'ordinateur afin d'infecter les fichiers exécutables lancés par l'utilisateur.
- Les virus non-résidents infectent les programmes présents sur le disque dur dès leur exécution.

Virus

Ils peuvent contaminer de machine de plusieurs manière:

- Téléchargement de logiciels et exécution sans précaution.
- échange de données (Flash disque, Bluetooth, …)
- Ouverture sans précaution de documents avec macro
- Pièces jointes de courrier électronique (.exe, .vbs)
- Ouverture d'un courrier au format HTML contenant JavaScript exploitant une faille de sécurité du logiciel
- Exploitation d'un bug du logiciel de courrier

Prévention: Virus

- se méfier d'un nom de fichier attaché ou d'un sujet d'e-mail trop attractif;
- ne jamais ouvrir un fichier joint avec une extension (.exe, .com, .bat, .vbs, .pif,);
- se méfier des documents Word (.doc), Excel (.xls) ou PowerPoint (.pps) contenant des macros en Visual Basic;
- ne jamais ouvrir un fichier contenant une double extension, comme " TrucMuche.GIF.VBS ", qui sont des astuces utilisées pour cacher la vraie identité d'un fichier infecté;

Prévention: Virus

- ne jamais faire confiance à l'expéditeur, même si c'est une personne connue. En effet, certains vers se servent des carnets d'adresses d'ordinateur infecté pour se propager;
- ne pas insérer de disquettes sans en connaître la provenance;
- sauvegarder régulièrement ses fichiers importants, car même avec la plus extrême vigilance, le pire peut arriver.
- installer un antivirus et mettre à jour régulièrement les définitions de virus.
- vérifier la provenance des fichiers téléchargés sur Internet (vérifier avec l'antivirus qu'ils ne sont pas infectés);
- supprimer tous les e-mails non sollicités. (ex. : SPAM);

Ver (Worm)

- est une variété de virus qui se propage par le réseau.
- exploite les communications réseaux d'un ordinateur afin d'assurer sa reproduction sur d'autres ordinateurs
- En 1988, l’étudiant Robber T. Morris a développé un ver qui infecté plusieurs milliers ordinateur dans 8 heures après leur lancement. C’est ainsi que de nombreux ordinateurs sont tombés en pannes en quelques heures.

Ver (Worm)

- Ils peuvent se propager sur des machines non maintenues à jour grâce au applications messagerie et sous la forme de code directement exécuté par le client de messagerie (JavaScript, VBS…).
- Les vers ont un avenir certain dans les applications web, comme les sites de réseaux sociaux (Facebook, Myspace) ont vu apparaître des scripts utilisant les langages de ces applications ou JavaScript et pouvant se répandre sur les comptes de tous les utilisateurs de ces services.

Exemple ?

Stuxnet

•Spécifique au système Windows, il a été découvert en juin 2010 par VirusBlokAda

• vise les systèmes utilisant les logiciels SCADA WinCC/PCS 7 de Siemens.

•Le premier ver découvert qui espionne et reprogramme des systèmes industriels

•Le ver a affecté 45 000 systèmes informatiques, dont 30 000 situés en Iran, y compris des PC appartenant à des employés de la centrale nucléaire de Bouchehr.

Logiciel espion (*spyware*)

- le programme espion (spyware, espiogiciel) est un programme indésirable qui s'installe en général sur un poste de travail. Sa fonction est récupérer des informations sur une personne ou une société de façon transparente pour l'utilisateur.
- Il fait de la collecte d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation. Ces informations sont ensuite transmises à un ordinateur tiers ;

Logiciel espion (*spyware*)

- Les informations récoltées peuvent être :
  - les sites web visités (URL),
  - les mots-clés utilisés dans les moteurs de recherche,
  - l'analyse des achats réalisés via Internet, voire les informations de paiement bancaire (numéro de carte bleue/VISA),
  - des informations personnelles (numéro de sécurité sociale, etc.).

Logiciel espion (*spyware)*

On trouve trois types de spywares:

- Commerciaux : Profilage des internautes
- Affichage de bannières publicitaires.
- Mouchard : Récupération de données personnelles

Logiciel espion (*spyware*)

Tempting Cedar

International Business Times

UK World Business Fintech **Technology** Science Sport Entertainment Opinion Video Pictures

Smartphones | **Cybersecurity** | Innovation | Social Media | Games | Motoring

Technology | CyberSecurity

What is Tempting Cedar? Hackers using fake Facebook profiles to spread Android spyware

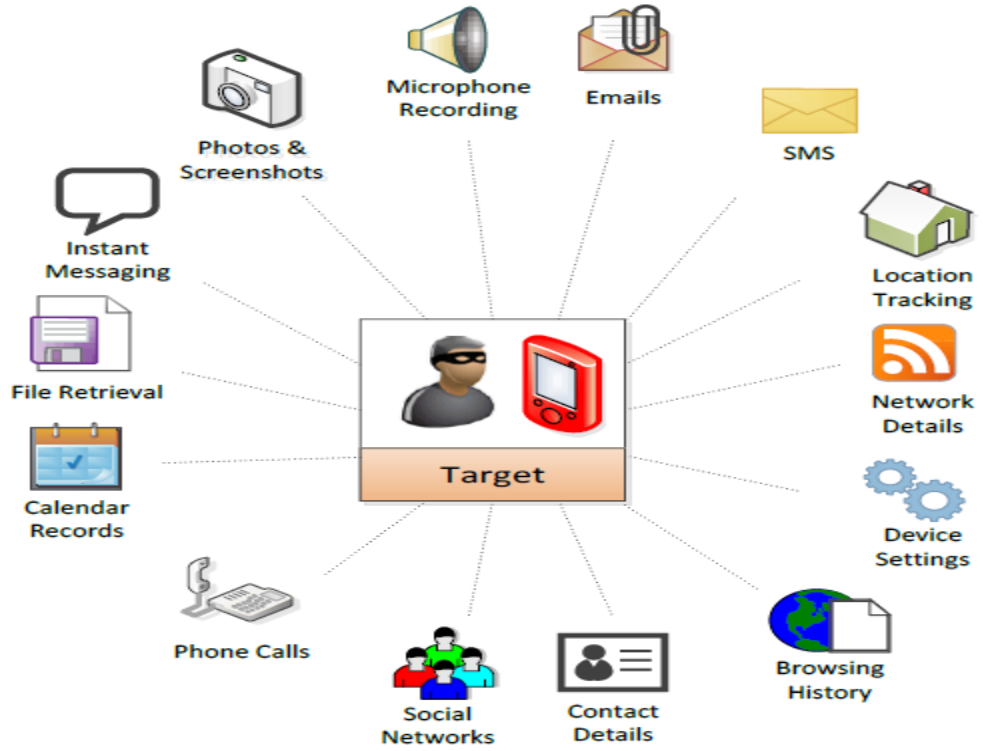
Security experts believe that the hackers behind the Tempting Cedar spyware may be Lebanese.

By India Ashok

February 23, 2018 05:07 GMT

The spyware steals victims' photos, contacts, call logs and can also spy on conversations when the infected device is within range. The Tempting Cedar spyware can also harvest a victim's geolocation via the infected device to track their location, as well as record surrounding sounds.

Exemple



Zero-day Attack

NSO GROUP

Update (Sept 1, 2016): Today Apple released security updates for Desktop Safari and Mac OS X. These updates patch the Trident vulnerabilities that identified in this report for desktop users. The Trident vulnerabilities used by NSO could have been weaponized against users of non iOS devices, including OSX.**We encourage all Apple users to install the update as soon as possible**. Citizen Lab is not releasing samples of the attack at this time to protect the integrity of still-ongoing investigations.

This report describes how a government targeted an internationally recognized human rights defender, Ahmed Mansoor, with the Trident, a chain of zero-day exploits designed to infect his iPhone with sophisticated commercial spyware.

Logiciel espion (*spyware*)

Protection:

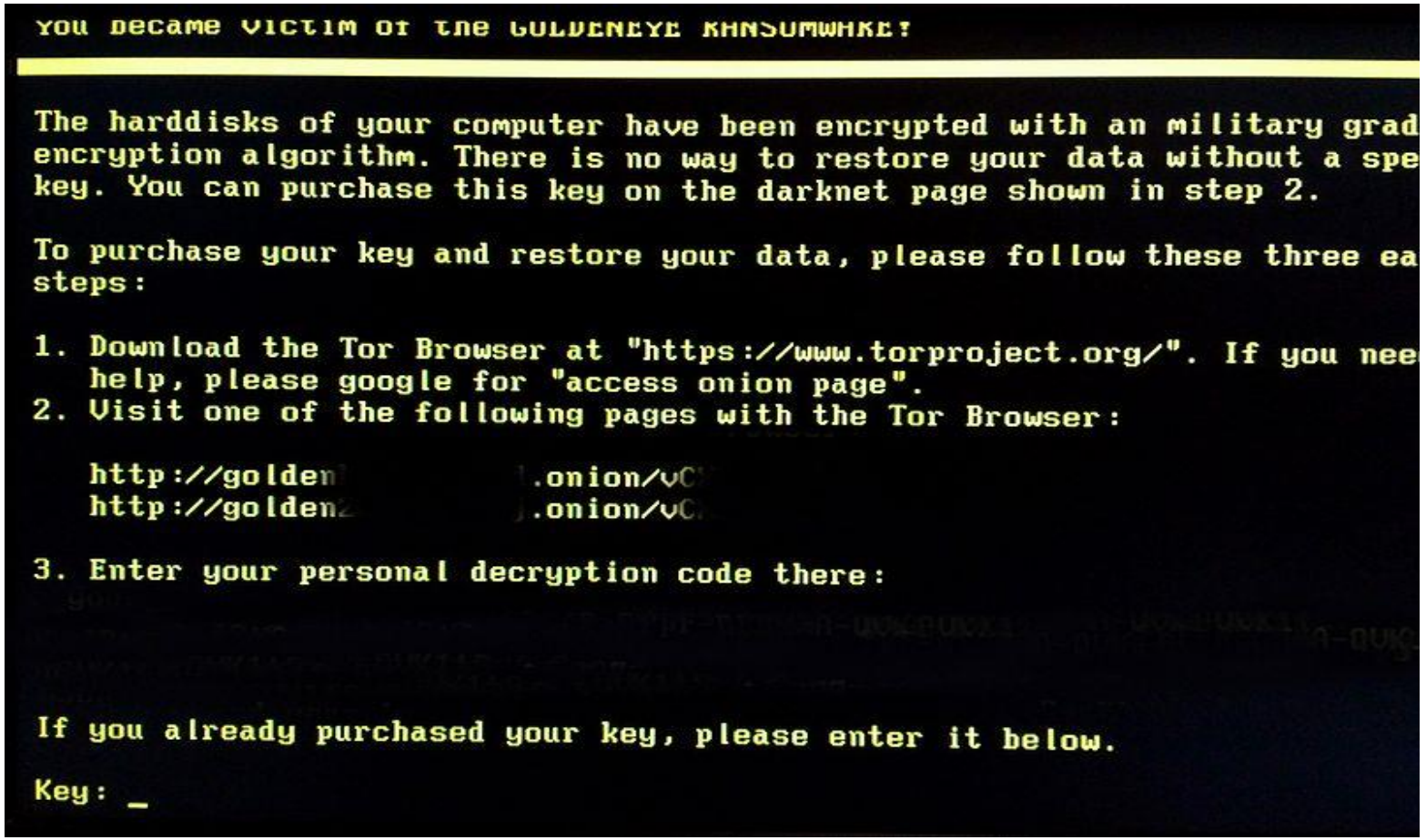
- Installation d'un pare-feu personnel qui permet de détecter la présence d'espiogiciels, d'autre part de les empêcher d'accéder à Internet
- Utilisation un anti-Spyware pour détecter et de supprimer les fichiers, processus et entrées de la base de registres créés par des spywares. Exemple: *Ad-Aware*.

Ransomware

- C’est un logiciel malveillant qui infecte l’ordinateur et affichent des messages demandant de verser une certaine somme afin que le système fonctionne à nouveau.
- Cette catégorie peut être installée en cliquant sur des liens trompeurs dans un e-mail, via la messagerie instantanée ou un site Internet.
- Le ransomware a la capacité de verrouiller l’écran d’un ordinateur ou de chiffrer des fichiers importants prédéfinis avec un mot de passe.

Source: Kaspersky

Ransomware


You became victim of the GOLDENEYE RANSOMWARE!
The harddisks of your computer have been encrypted with an military grad
encryption algorithm. There is no way to restore your data without a spe
key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three ea
steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you nee
help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://golden .onion/vC
http://golden .onion/vC
3. Enter your personal decryption code there:
If you already purchased your key, please enter it below.
Key: _

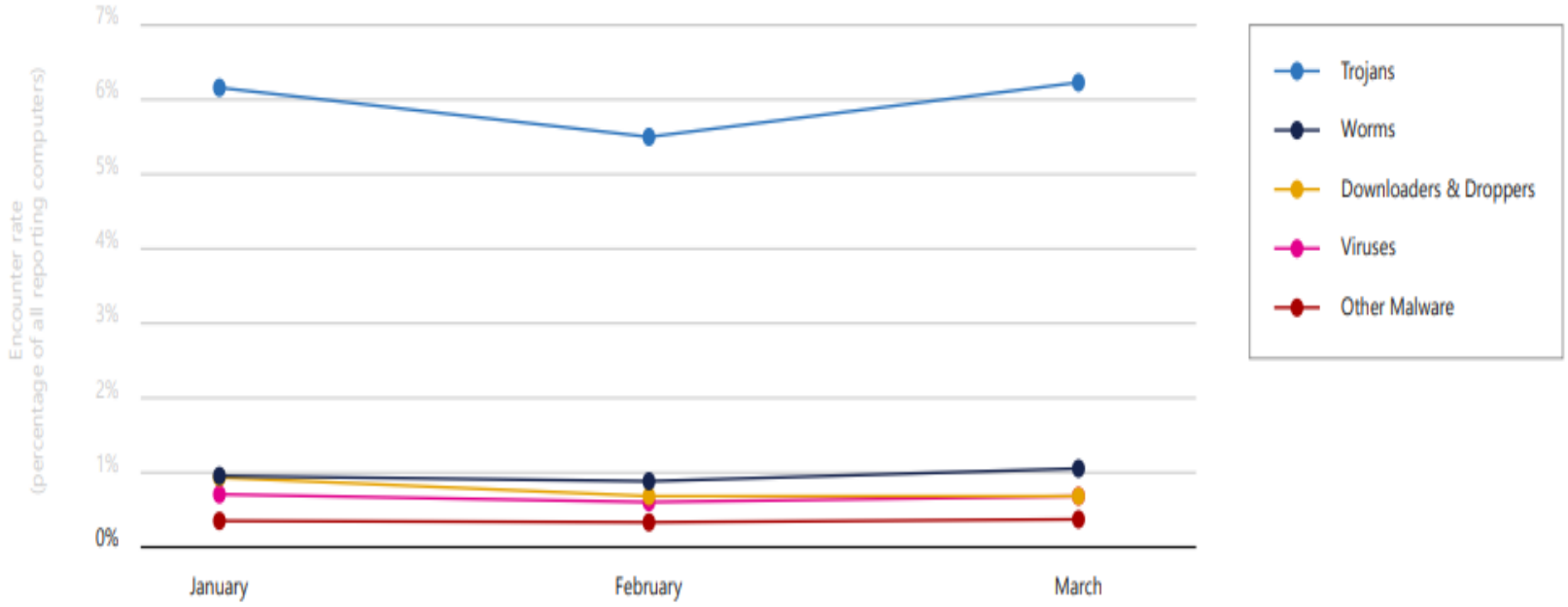
Ransomware

- **Exemples:**
  - Reveton (2012),
  - Ransomware RSA-4096 (avril 2016),
  - WannaCry (mai 2017),
  - Bad Rabbit (octobre 2017)

Cheval de Troie (*trojan)*

- programme informatique à apparence légitime (voulue) qui exécute des routines nuisibles et des actions cachées et pernicieuses sans l'autorisation de l'utilisateur ;
- Il ouvrant une porte dérobée (*backdoor)* dans un système pour y faire entrer un hacker ou d’autres programmes indésirables.

Encounter rates for significant malicious software categories in 1Q17



Source: Trends in Global Cybersecurity, Microsift, 2017

Cheval de Troie (*trojan*)

- Un cheval de Troie peut par exemple :
  - voler des mots de passe
  - exécuter toute autre action nuisible, etc.
  - copier des données sensibles
- Détecter un tel programme est difficile parce qu'il faut arriver à détecter si l'opération du programme (le cheval de Troie) est voulue ou non par l'utilisateur.

Cheval de Troie (*trojan)*

- **Exemples :** Troj/Zulu, Happy 99, Backdoor, BackOrifice
- Trojan.ByteVerify
  - cheval de Troie sous forme d'une applet java.
  - Utilise une faiblesse dans la machine virtuelle java de Microsoft permettant à un pirate d'exécuter du code arbitraire sur la machine infectée.
  - Par exemple, il peut modifier la page d'accueil d'Internet Explorer.

Cheval de Troie (*trojan)*

Symptômes d'une infection

- activité anormale du modem ou de la carte réseau : des données sont chargées en l'absence d'activité de la part de l'utilisateur
- des réactions curieuses de la souris
- des ouvertures impromptues de programmes
- des plantages à répétition.

- **Protection:** un pare-feu applicatif permet de stopper les communications d'applications non autorisées à accéder au Web. exemple: ZoneAlarm.

Porte dérobée (*backdoor*)

- logiciel de communication caché, installé par exemple par un virus ou par un cheval de Troie,
- permet d'ouvrir d'un accès réseau frauduleux sur un système informatique.
- Il est ainsi possible d'exploiter à distance la machine,
- Exemple: elle a été découverte au début des années 2000 dans le SGBD interbase de Borland. Il suffisait d'entrer le nom d'utilisateur " politically " et le mot de passe "correct " pour se connecter à la base de données avec les droits d'administrateur.

Enregistreur de frappe (*keylogger)*

- programme généralement invisible installé sur le poste d'un utilisateur et chargé d'enregistrer à son insu ses frappes clavier; pour intercepter des mots de passe par exemple.
- Certains *keyloggers sont capables d'enregistrer les URL visitées, les* courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur

Bombe logique

- Une bombe logique est une fonction, cachée dans un programme en apparence honnête, utile ou agréable, qui se déclenchera à retardement, lorsque sera atteinte un moment déterminé en exploitant la date du système, ou lorsque surviendra un certain événement.
- Cette fonction produira alors des actions indésirées,

Bombe logique

- Sa objective principal est généralement utilisée dans le but de créer un déni de service en saturant les connexions réseau d'un service en ligne, d'un site, ou d'une entreprise
- **Exemples :** Tchernobyl, Vendredi 13
- Le virus Tchernobyl avait une bombe logique qui s'est activée le 26 avril 1999, jour du treizième anniversaire de la catastrophe nucléaire de Tchernobyl.

Plan du cours

- Principaux défauts de sécurité
- Logiciels malveillants
- Les menaces de la messagerie électronique
- Protections

Courrier électronique non sollicité (*spam*)

- un courrier électronique non sollicité, la plupart du temps de la publicité.
- L'objective principal du spam est de faire de la publicité à moindre prix par « envoi massif de courrier électronique non sollicité » ou par « multipostage abusif ».
- Les spammeurs collectent des adresses électroniques sur Internet via des logiciels (appelés robots) parcourant les différentes pages et stockant au passage dans une base de données toutes les adresses e-mail y figurant. Finalement, il lance une application envoyant successivement à chaque adresse le message publicitaire.

Courrier électronique non sollicité (*spam*)

- **Inconvénients**
- l'espace qu'il occupe dans les boîtes aux lettres des victimes ;
- la difficile consultation des messages personnels ou professionnels au sein de nombreux messages publicitaires et l'augmentation du risque de suppression erronée ou de non lecture de messages importants ;
- la perte de temps occasionnée par le tri et la suppression des messages non sollicités,
- la bande passante qu'il gaspille sur le réseau des réseaux.
- **Protection:** anti-spam

Hameçonnage (*phishing*)

- Est un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles ;

Principaux défauts de sécurité

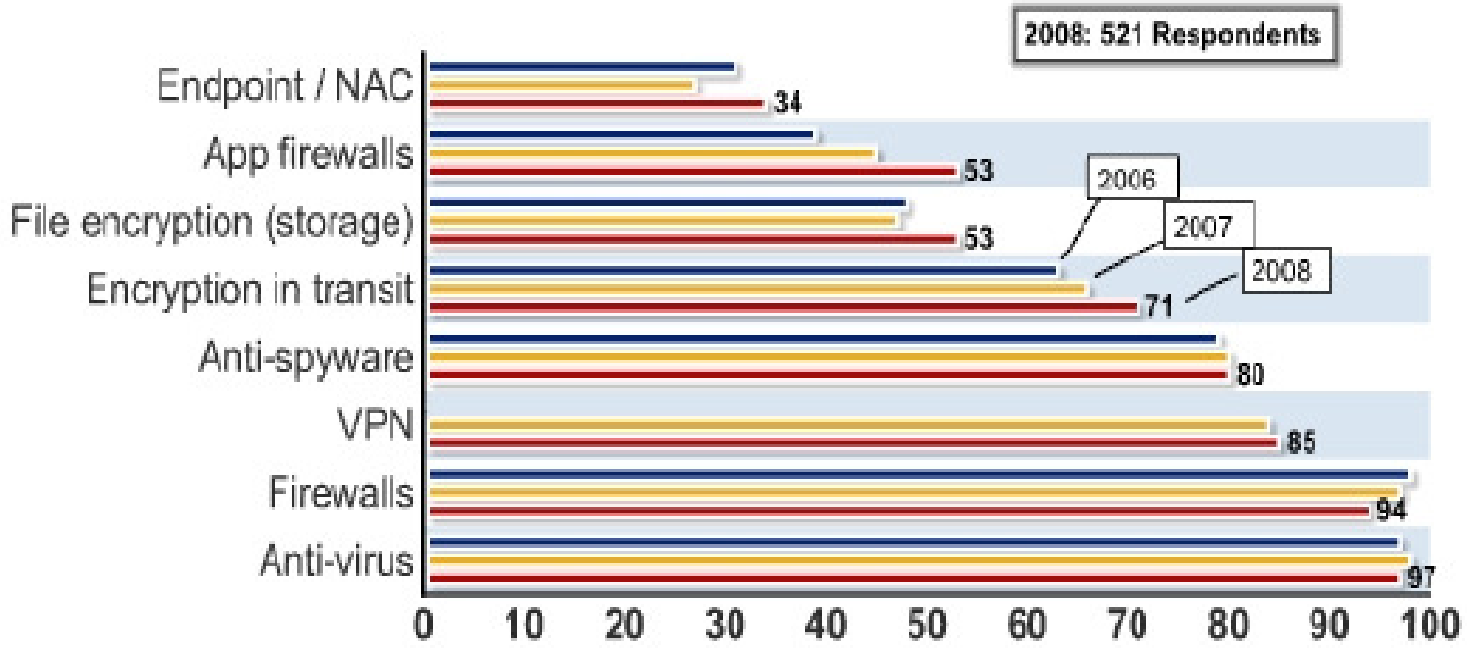
- Installation des logiciels et matériels par défaut
- Pas de mises à jour des systèmes d'exploitation et des correctifs
- Mots de passe non existant ou par défaut
- Réseaux complexe, non protégés
- Pas de séparation des flux opérationnels/ administration système
- Procédure de sécurité obsolètes
- Authentification faible
- Services inutile conservés
- Absence ou mauvaise stratégie de sauvegarde des données.
- Accès aux salle informatique non sécurisé

Plan du cours

- Principaux défauts de sécurité
- Logiciels malveillants
- Les menaces de la messagerie électronique
- Protections

Quelques solutions

Figure 16: Security Technologies Used



❶ Antivirus

- Les antivirus sont des programmes capables de détecter la présence de virus sur un ordinateur, ainsi que de nettoyer celui-ci dans la mesure du possible si jamais un ou des virus sont trouvés.

❶ Antivirus

Les antivirus peuvent s'installer principalement en deux sortes d'endroits :

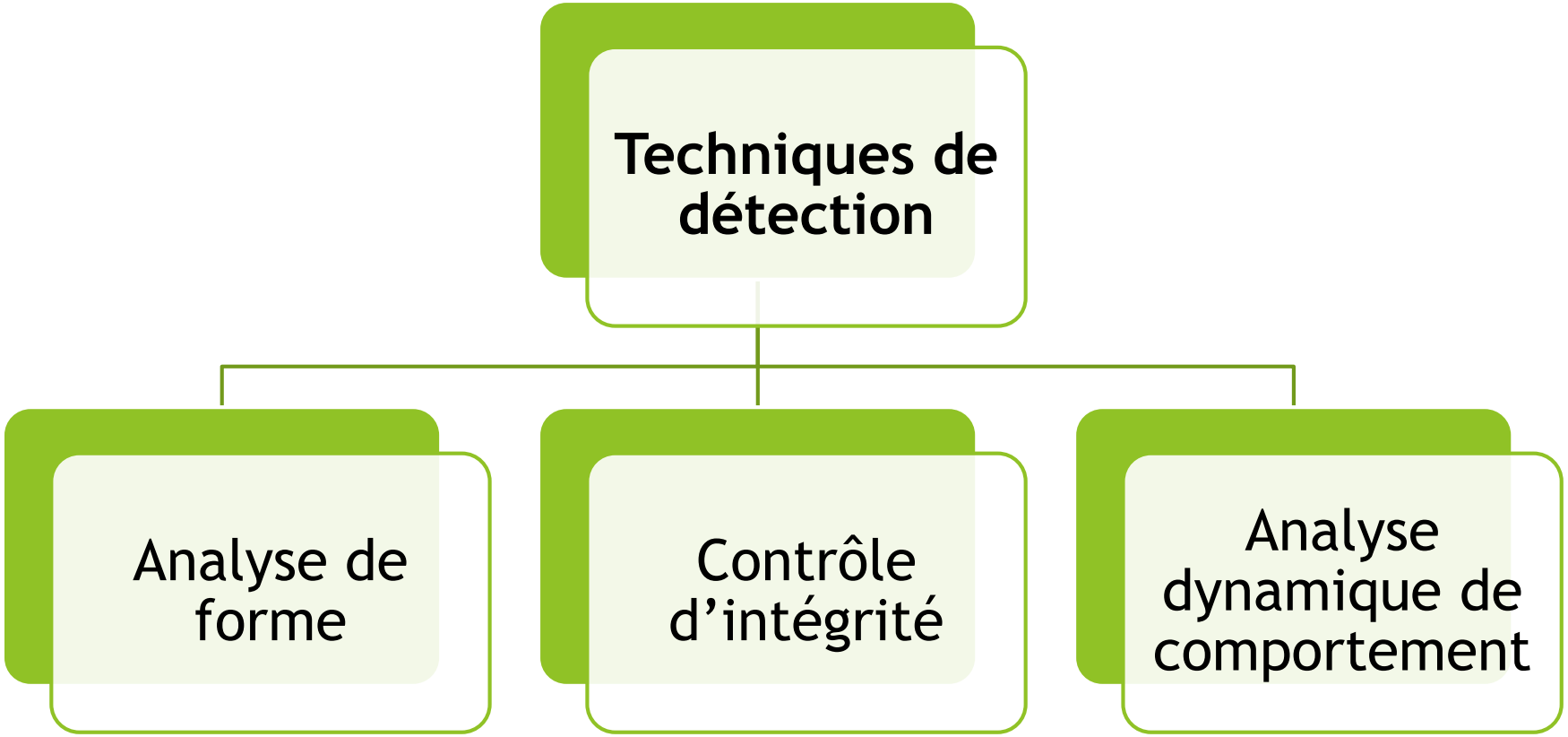
- Entrée d'un réseau local, où arrivent les flux en provenance de l'Internet ; certains de ces flux seront filtrés pour y détecter des virus, essentiellement les flux relatifs aux protocoles HTTP (Web) et SMTP (courrier électronique)
- Poste de travail de l'utilisateur, et là l'antivirus servira généralement à inspecter et désinfecter le disque dur (problème d'exécution certains virus en mémoire vive, sans s'enregistrer sur le disque).

❶Antivirus

Il y a deux modes de fonctionnement des logiciels antivirus :

- mode statique: le logiciel est activé uniquement sur ordre de l'utilisateur, par exemple pour déclencher une inspection du flash disque
- mode dynamique: le logiciel est actif en permanence, et il scrute certains événements qui surviennent dans le système,
  - Il induit une consommation non négligeable de ressources telles que temps de processeur et mémoire,
  - Il permet une meilleure détection des attaques, notamment par analyse comportementale des logiciels suspects d'être contaminés.

❶ Antivirus



❶Antivirus

Analyse de forme

consiste à détecter la présence d'un virus dans un fichier par des caractères statiques qui permettent de le reconnaître.

1) **La recherche de signatures:** on cherche un motif textuel, i.e une suite de bits, caractéristique d'un virus connu. Avec cette méthode, ne peut pas détecter un nouveau virus, ou un virus déjà connu mais modifié. Elle impose l'installation et la mise à jour en permanence d'une base de données des signatures,

2) **Analyse spectrale:** il y a des instructions sont rares dans les programmes ordinaires mais fréquentes dans les virus, alors une analyse statistique de la apparition de ces instructions peut permettre la détection de virus. Mais il y a possibilité de détecter d'un virus dans un fichier exécutable légitime.

❶Antivirus

3) **Analyse heuristique:** établir et de mettre à jour un corpus de règles qui permettent de caractériser les propriétés d'un fichier suspect. Cette approche est sujette aux faux positifs, comme la dernière.

❶Antivirus

Contrôle d'intégrité:

consiste à détecter la modification anormale d'un fichier, qui peut signaler sa contamination par un virus.

- il faut calculer pour chaque fichier sensible une empreinte numérique infalsifiable par une fonction de hachage.
- La réalisation de cette méthode est difficile pratiquement.

❶Antivirus

Analyse dynamique de comportement:

- Consiste à examiner les actions d'un programme dès qu'il s'exécute et à détecter les activités louches:
  - *Essais* d'accès en écriture à des fichiers de programmes exécutables,
  - ou à des bibliothèques,
  - ou à des zones du disque réservées au système.

Virus Blindés

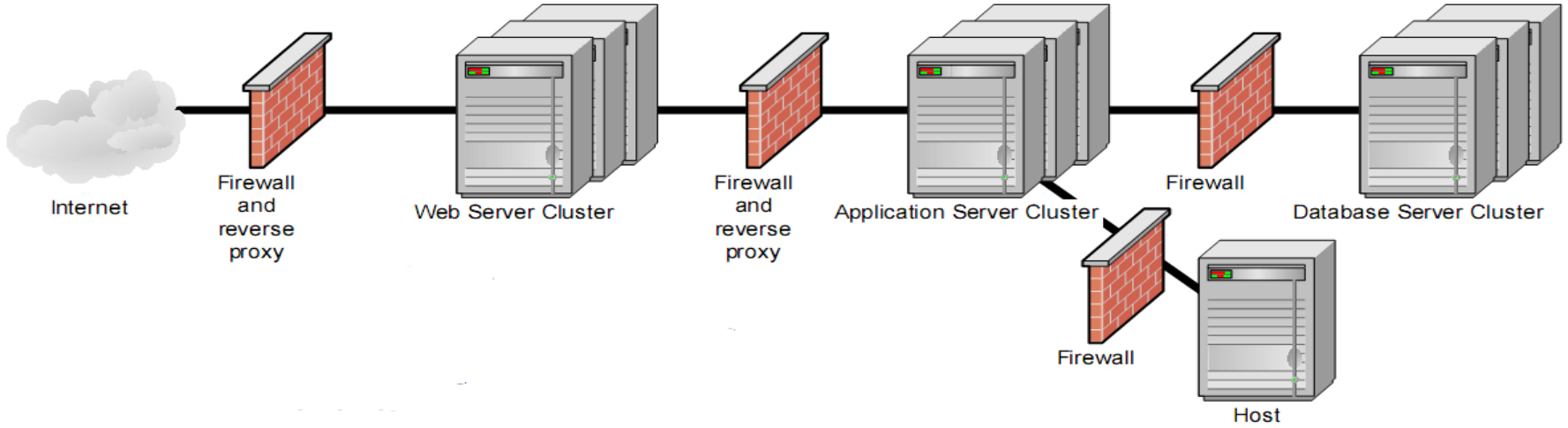
❷Firewall (pare-feu)

- Un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent.
- Système qui filtre les paquets réseau pour protéger l'accès aux données accessibles a travers le réseau ainsi qu'aux services ouverts par les serveurs.
- Deux types:
  - **Firewall réseau:** Equipement réseau qui sépare le réseau Intranet du réseau Internet.
  - **Firewall personnel:** Protège le poste de travail

❷Firewall (pare-feu)

Exemple:

Banking Application Architecture



Exemples: IPCop, Zone Alarm

❸ Détection des intrusions

- Les systèmes de détection (IDS) sont conçu pour informer, et dans certain cas pour empêcher, des accès non autorisés ou des intrusions dans le réseau.
- Ces systèmes sont aussi capable de détecter les pirates internes (70% à 80% des actes malveillance).

❹Formation des utilisateurs

- Discrétion: sensibilité des utilisateurs à la faible sécurité des outils de communication, et à l'importance de la non divulgation des informations.
- Virus: plusieurs utilisateurs ouvert des pièces jointes suspectes == > information régulière du personnel.
- Charte: obliger les employés à lire et signer un document précisent leurs droits et devoirs, et de leur faire prendre conscience de leur responsabilité individuelles.

❺Authentification et cryptage

- L’authentification est basée sur les 3 principes:
  - Savoir: login, PSW, …
  - Etre : biométrie (empreinte,…)
  - Avoir: clés USB, carte à puce…

❻Authentification et cryptage

- Pour évite l'espionnage on pourra utiliser la signature numérique ou le **cryptage** de toute l'information.
- Applications:
  - Les fichiers stockés
  - Les données transmis.

Références

- Pierre-François Bonnefoi, « Cours de Sécurité Informatique », https://doc.lagout.org/Others/Cours_securite%20informatique.pdf
- Jean-François Pillou, Jean-Philippe Bay, « Tout sur la sécurité informatique », Dunod, 2016.
- Laurent Poinsot, « Introduction à la sécurité informatique », UMR 7030 - Université Paris 13 - Institut Galilée.