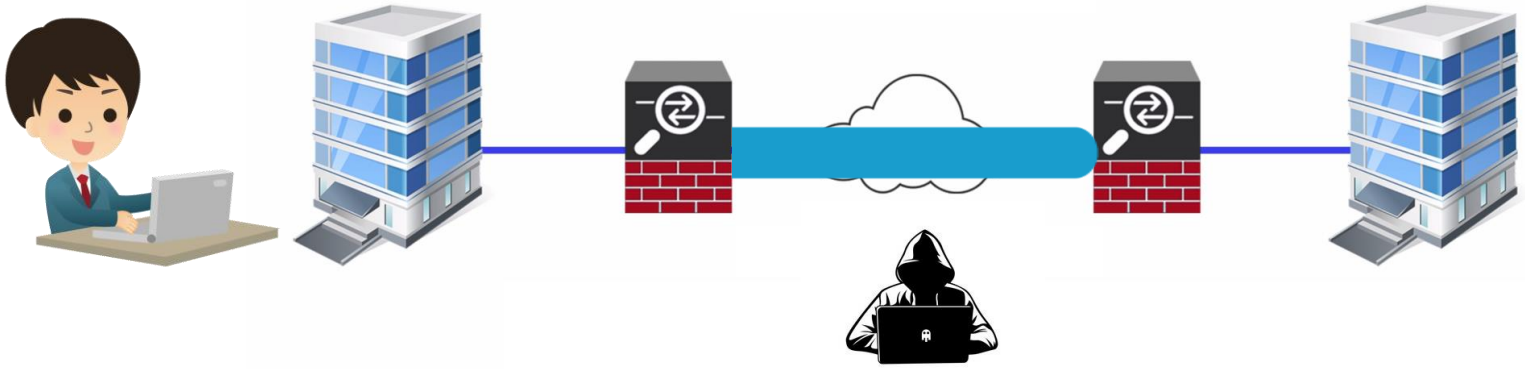


Computer Security

Software Security

Threats, Attacks, and Vulnerabilities

There’s no silver bullet solution with cyber security, a layered defense is the only viable defense.
-James Scott

Tamer ABUHMED
Department of Computer Science & Engineering
Sungkyunkwan University

SUNG KYUN KWAN UNIVERSITY

Outline

- Threats
- Threat Models
- Attacks, Attack Surface
- Exploits
- Indicators of Compromise
- Malware
- Vulnerabilities
- Mitigations and Patches

Definitions

Threats are people who are able to take advantage of security vulnerabilities to attack systems. Also known as adversaries.

- Vandals, hacktivists, criminals, spies, disgruntled employees, etc.

Vulnerabilities are weaknesses in a system that allow a threat to obtain access to information assets in violation of a system's security policy.

Ex. (2719662)	Vulnerabilities in Gadgets Could Allow Remote Code Execution

Attacks are actions taken by threats to obtain assets from systems in violation of the security policy.

Who are the Threats?

Hacktivists

Vandals

Criminals

Spies

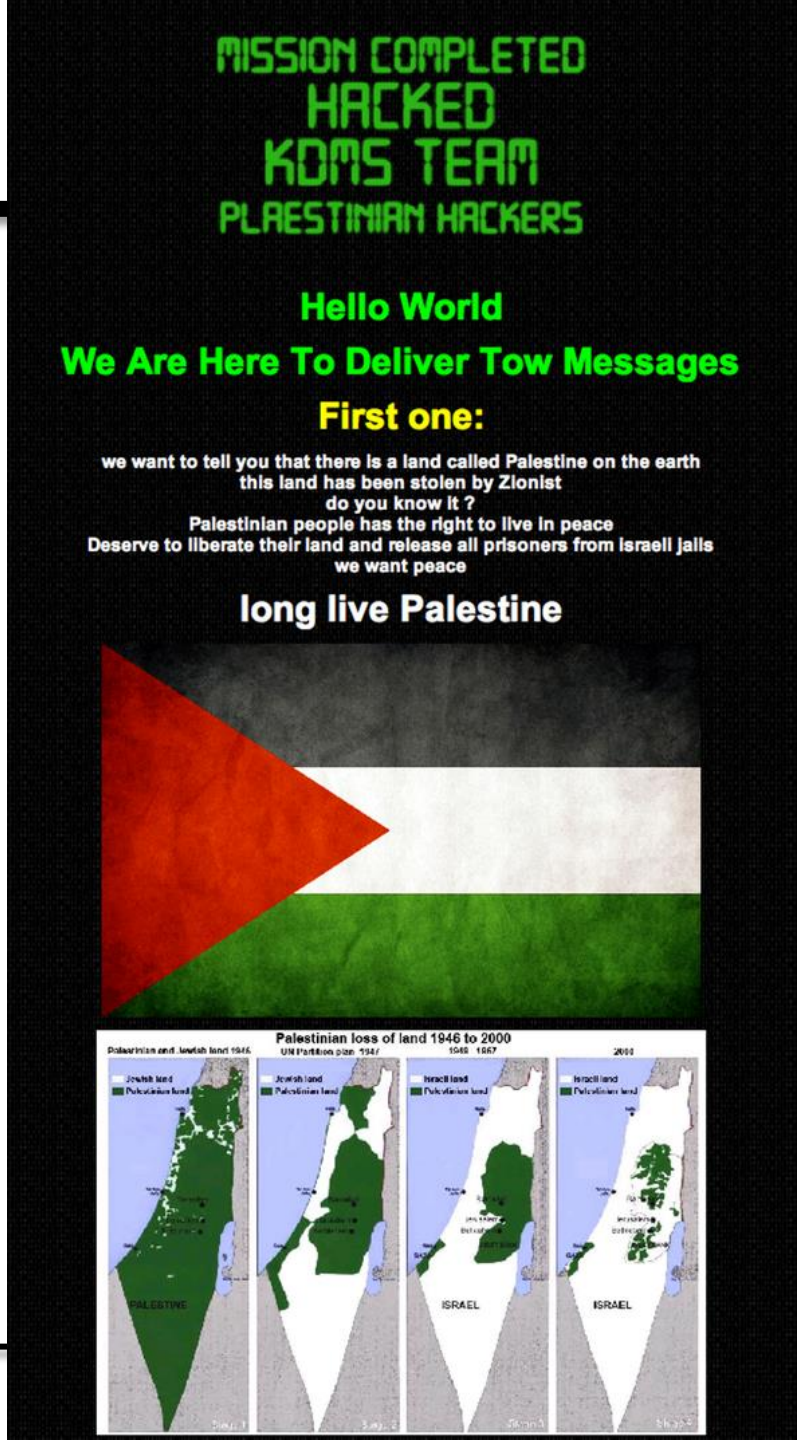
Hacktivists

Hacktivists attack systems for political goals.

- Deface websites to spread their message

  (defacement of

  avg.com shown)
- Take down sites in retribution for actions.



Vandals


[!] Struck by 1337
Google
Google Malaysia STAMPED by PAKISTANI LEETS
We are TeaM MADLEETS
H4x0r HuSY - KhantastiC HaXor - H4x0rL1f3 - InvectuS - Shadow008 - r00x - Don - MindCracker - Dr.Z0mbie - phpBuGz - MaD GirL
MaDCoDe - Sn!p3r_GS - DeXter - Neo Haxor - Darksnipper - Pain006 - b0x - R3DL0F - Sahrawi - 3thicaln00b - Hmei7 - MakMan - Sniffer - AL.MaX HaCkEr - Ch3rn0by1
==========
www.MaDLeeTs.com
| LeeTHaXor@Y7mail.com |
==========
Pakistan Zindabad

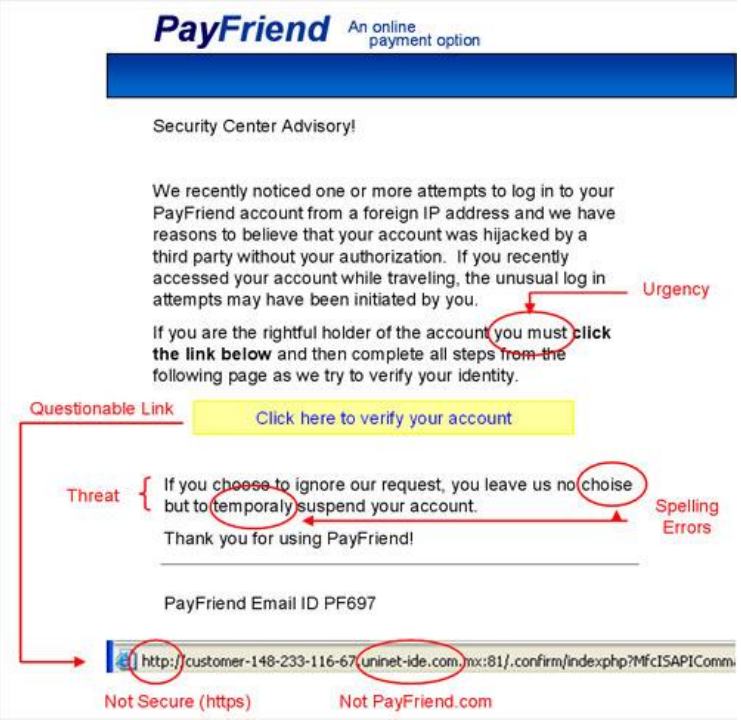
Cybercriminals

Focus on monetizing information via:

- Identity theft (phishing)
- Credit card or bank account fraud (phishing)
- Extortion (via ransomware or DDoS)
- Clickjacking
- Fraud (auction fraud, 419 scams, etc.)

Specialists who sell services to other criminals

- Distribute malware
- Rent botnet computing services



Cyberspies

Threats that work for a nation state:

- Obtain classified information
- Obtain technical information
- Install backdoors for later access
- Distract enemies from other operations
- Destroy physical devices (Stuxnet)

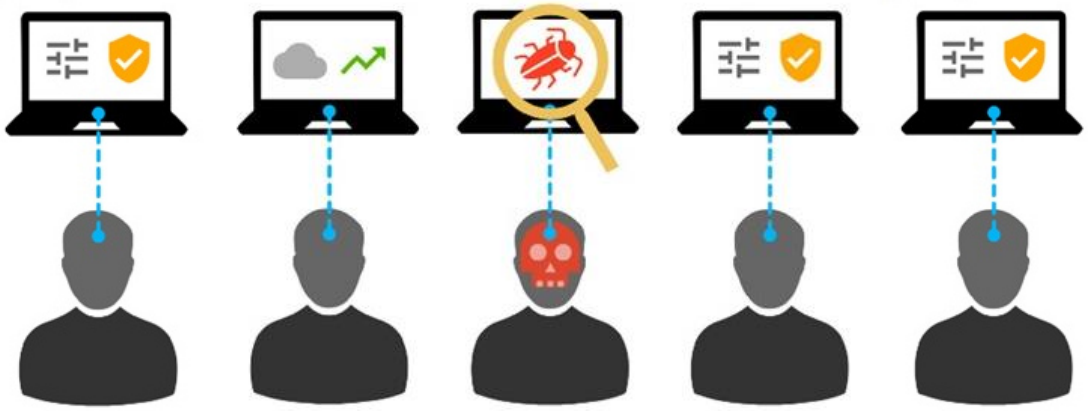
Terms: **Cyberespionage** and **cyberwarfare**

Insider Problem

Insiders are threats who are members of the organization that they are attacking.

Insiders are dangerous because they

- Are inside the security perimeter, so cannot be blocks by perimeter defenses like firewalls and locked doors.
- Have some level of legitimate access to systems.
- May have physical access to systems and information.



Inadvertent Insider Problems

Insiders are often responsible for data breaches without malicious intent, because they

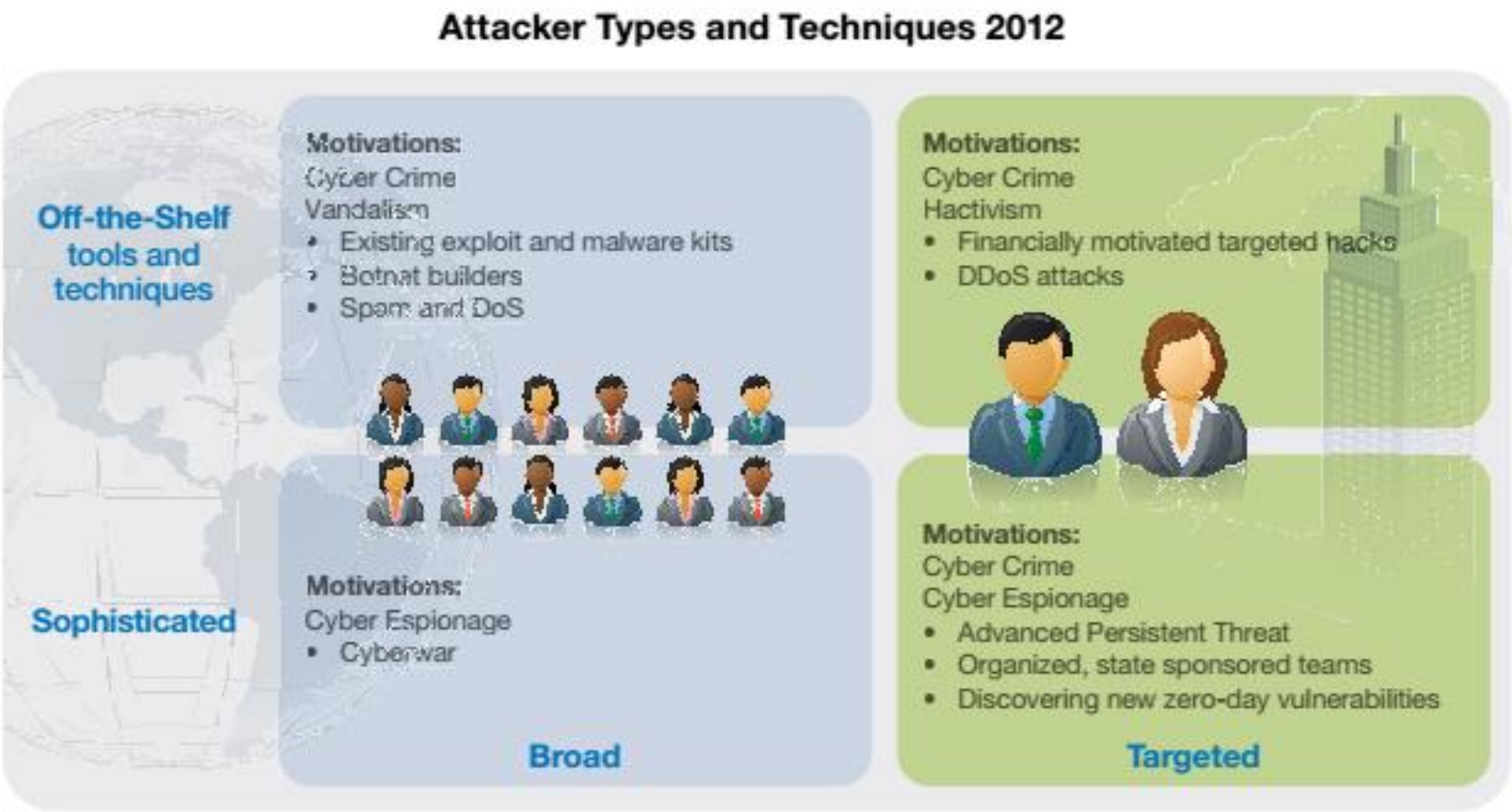
- Misconfigure cloud storage or databases, allowing anyone on the Internet to access systems.
- Click on links or attachments that install malware on their systems.
- Choose weak passwords that attackers can guess.

Threat Model

A **threat model** describes which threats exist to a system, their capabilities, resources, motivations, and risk tolerance. Also known as an **adversary model**.

- Four quadrant model: skill and targeting.
- Resources and capabilities.
- Do you keep enough data about historical incidents to know capabilities and motivations?

Four Quadrant Threat Modeling "assessment"



IBM X-Force 2012 Trend and Risk Report

Adversary Modeling “assessment”

- Motivations
- Intent
- Resources
- Capabilities
- Risk Aversion
- Access

Motivations

- Money
- Espionage
- Fame/status
- Learning
- Entertainment
- Hacktivism
- Sabotage
- Terrorism

Intent

The **intent** is the goal of the attacker, which could be

- Personal information for fraud or identity theft
- Business account credentials for wire fraud
- Computational resources for cryptocurrency mining
- Network resources for distributed denial of service
- Technical plans or data for software or hardware
- Defacement of a web site to reduce target reputation

Resources

- Skilled personnel
- Money
- Computational power
- Technology
- Infrastructure

Capabilities

Computational

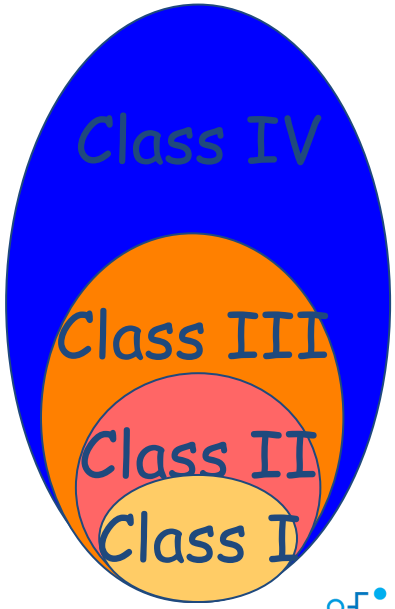
- Can try X keys/second or X passwords/second.

Informational

- Has access to {past, current, future} encrypted data.
- Has access to X GB of data.

Access

- Physical access.
- User access: none, authenticated, admin.
- Can read network data.
- Can inject packets into network.



Risk Aversion

Risk aversion is a tendency to avoid taking actions with negative consequences. Hackers don't want to be arrested, imprisoned, fined.

- Physical attacks are riskier than network attacks.
- Attacks from within the country of target are riskier, as it is easier to prosecute crimes within the same country.
- Attacks from a country with an extradition agreement with the country of the target are riskier than attacks from countries without such agreements.

Nation state attackers are typically less risk averse than cybercriminals, as they have resources and experience than criminals do not.

Access

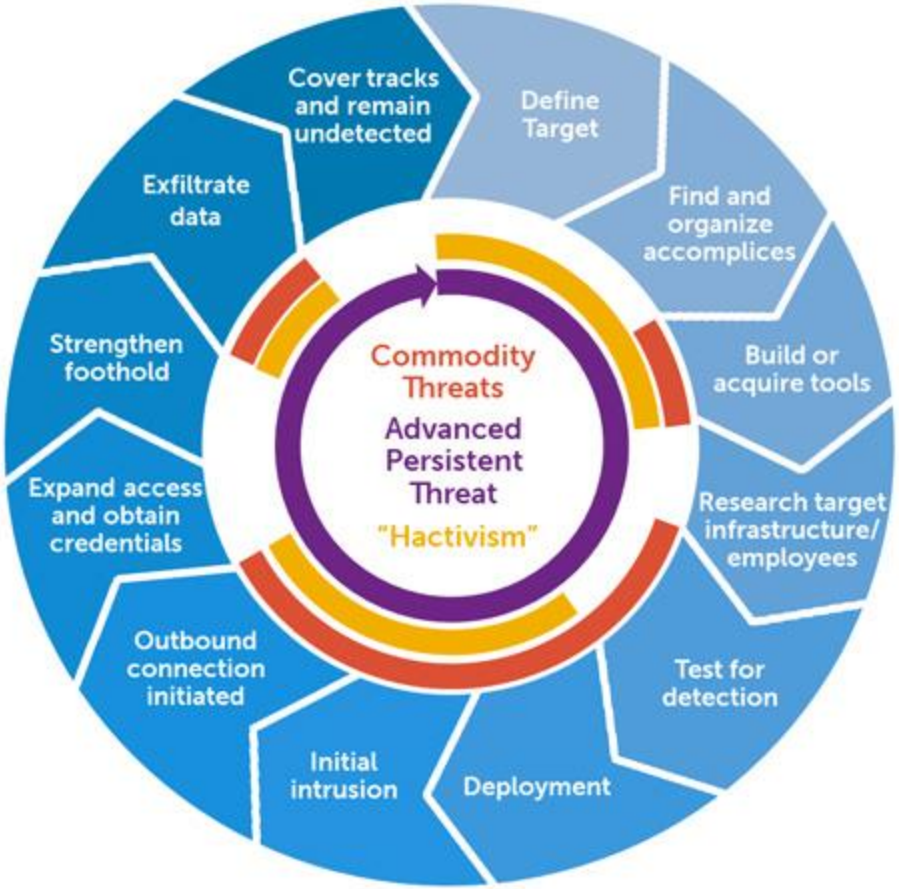
What level of access does threat already have to target?

- Insider with administrative privilege.
- Insider with privilege to access the desired target.
- Insider with ordinary user level access.
- Backdoors from previous attacks on same target.
- No access other than ability to make public contact via emails, public URLs, published phone numbers, etc.

Advanced Persistent Threat

Advanced persistent threat (**APT**) refers to a group that has the ability to maintain a constant presence inside a target's network.

- Sophisticated
- Targeted.
- Skilled personnel.
- May be backed with considerable budget.



Attacks

An **attack** is an action taken by a threat to gain unauthorized access to information or resources or to make unauthorized modifications to information or computing systems.

- Spoofing (pretending to be another entity)
- Packet sniffing (intercepting network traffic)
- Man in the middle (active interception of traffic)
- Injection Attacks (buffer overflows, sql injection, etc.)
- Denial of Service (resource depletion)
- Account Compromises (passwords, session hijacking)
- Social Engineering, etc.

How are Digital Attacks Different?

Automation

- Salami Attack from *Office Space*.

Action at a Distance

- Volodya Levin, from St. Petersburg, Russia, stole over $10million from US Citibank. Arrested in London.

Technique Propagation

- Criminals share attacks rapidly and globally.

Spoofing

A **spoofing** attack is when a threat masquerades as another entity on a telecommunications network.

Examples of spoofing include:

- E-mail spoofing
- MAC address spoofing
- ARP spoofing (MAC to IP address map spoofing)
- IP address spoofing
- Caller ID spoofing
- GPS spoofing

Sniffing

Packet sniffing is when a program records wired or wireless network packets destined for other hosts.

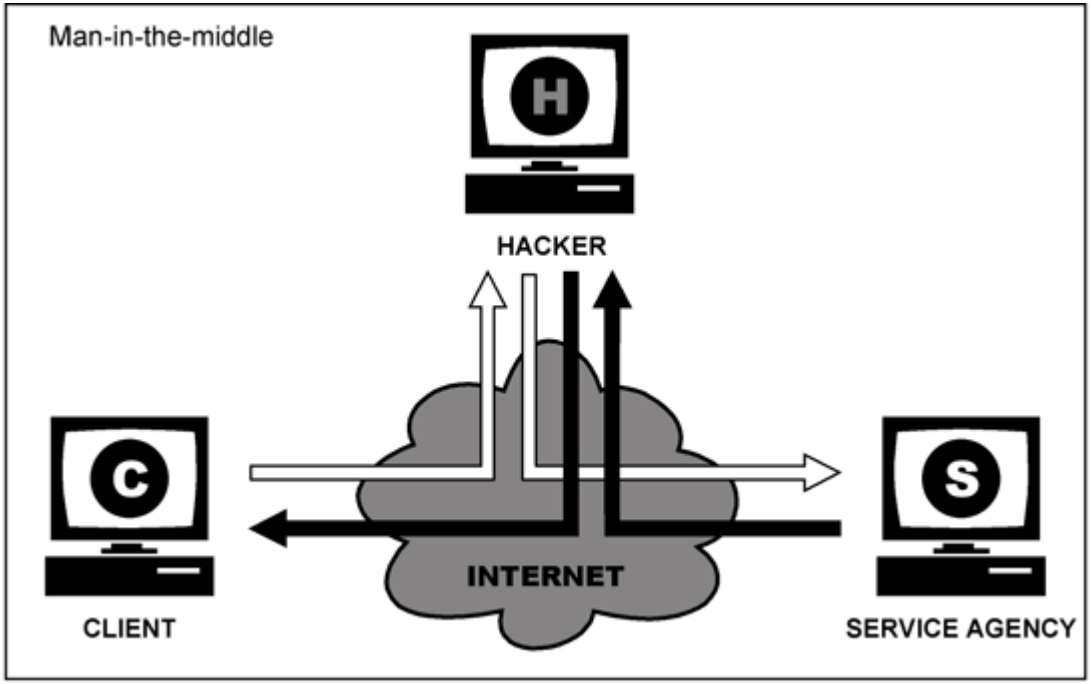
- Wireless traffic is available to everyone nearby.
- Antennas can extend range to miles.
- Wired traffic is accessible depending on network location.
- If network location unsatisfactory, ARP spoofing can redirect traffic to sniffing machine.

Sniffing used to

- Obtain passwords (ftp, imap, etc.)
- Obtain other confidential information

Man in the Middle

A **man-in-the-middle** attack is an active eaves-dropping attack, in which the attacker connects to both parties and relays messages between them.



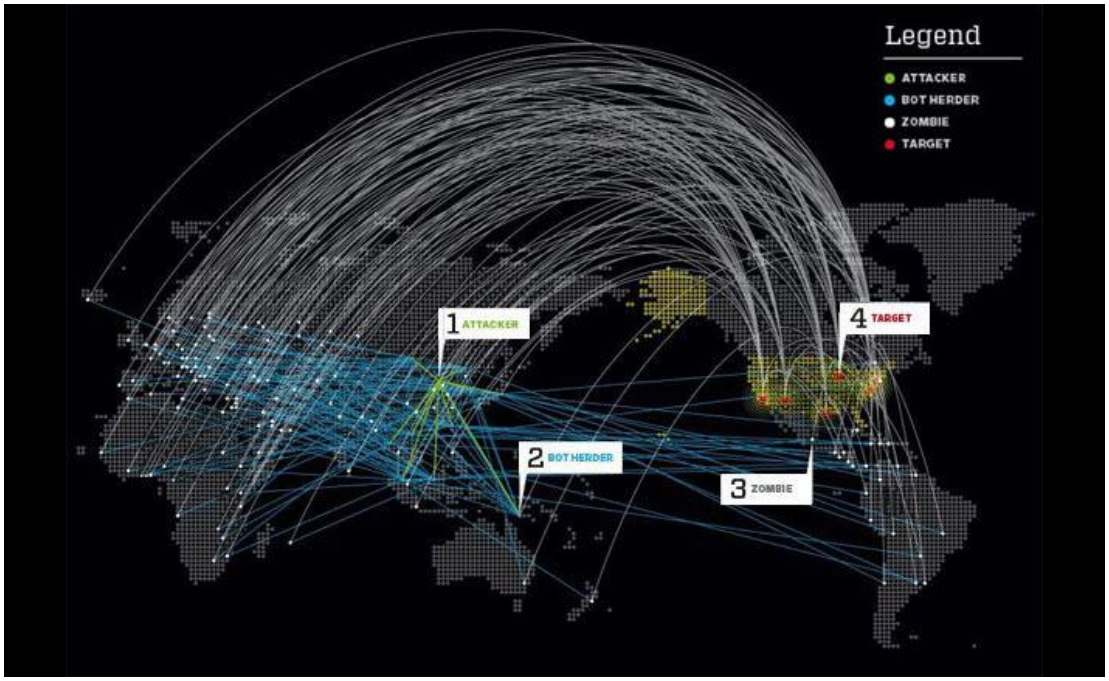
Injection Attacks

Injection attacks send code to a program instead of the data it was expected, then exploit a vulnerability in the software to execute the code.

- Buffer overflows inject machine code into a process.
- Cross-site scripting injects JavaScript code into a web page seen by another user.
- SQL injection injects SQL code into a database query run by an application.

Denial of Service

A **denial of service (DoS)** attack attempts to make computer or network resources unavailable to its intended users. A distributed DoS (DDoS) attack is a DoS attack coming from multiple sources.



Account Compromise

Attackers can take over a user's account and use that account's permissions to obtain or modify data. Account compromise often requires just a password obtained by:

- Guessing attacks with automated software.
- Reuse of passwords exposed in a data breach.
- Phishing.
- Keylogging.
- Password resets.

Attackers can temporarily compromise an attack by hijacking a user session via a MITM attack.

Social Engineering

Social engineering is the psychological manipulation of people to reveal confidential information or perform actions to violate security policy.

Web Application Attacks

Web applications are subject to a variety of attacks.

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

Wireless Attacks

Reconnaissance

- Finding and identifying wireless networks.

Sniffing and MITM

- Capturing and modifying network packets is easier.

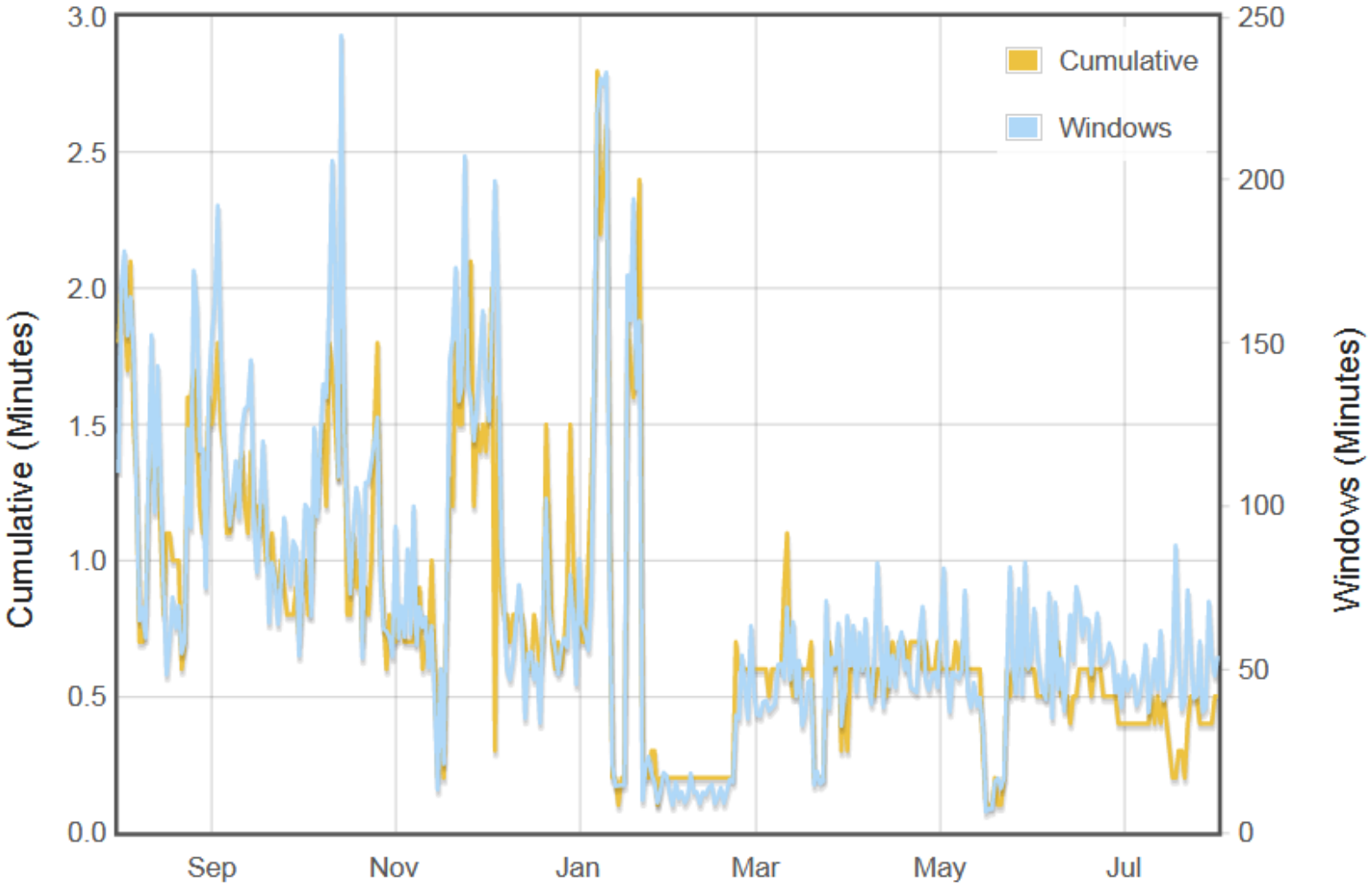
Rogue Access Points

- Rogue APs pretend to be another network, so they can capture login passwords, control client network configuration to easily do MITM attacks.

Wireless Security Flaws

- WEP and WPA encryption systems are broken
- WPA2 has serious flaws, so we are awaiting WPA3

Time to Attack after Deployment



Attack Vector

An **attack vector** is a means of delivering an attack.

- E-mail is an attack vector for spam or phishing.
- E-mail attachments are a vector for delivering malware.
- Malvertising is a vector to spread malware.
- Network access can be an attack vector for sniffing or network denial of service attacks.
- Remote access systems like VPNs can be a vector for account compromise attacks.
- Social engineering is an attack vector for phishing, etc.
- Supply chains can be an attack vector when an attacker compromises software that your system uses.

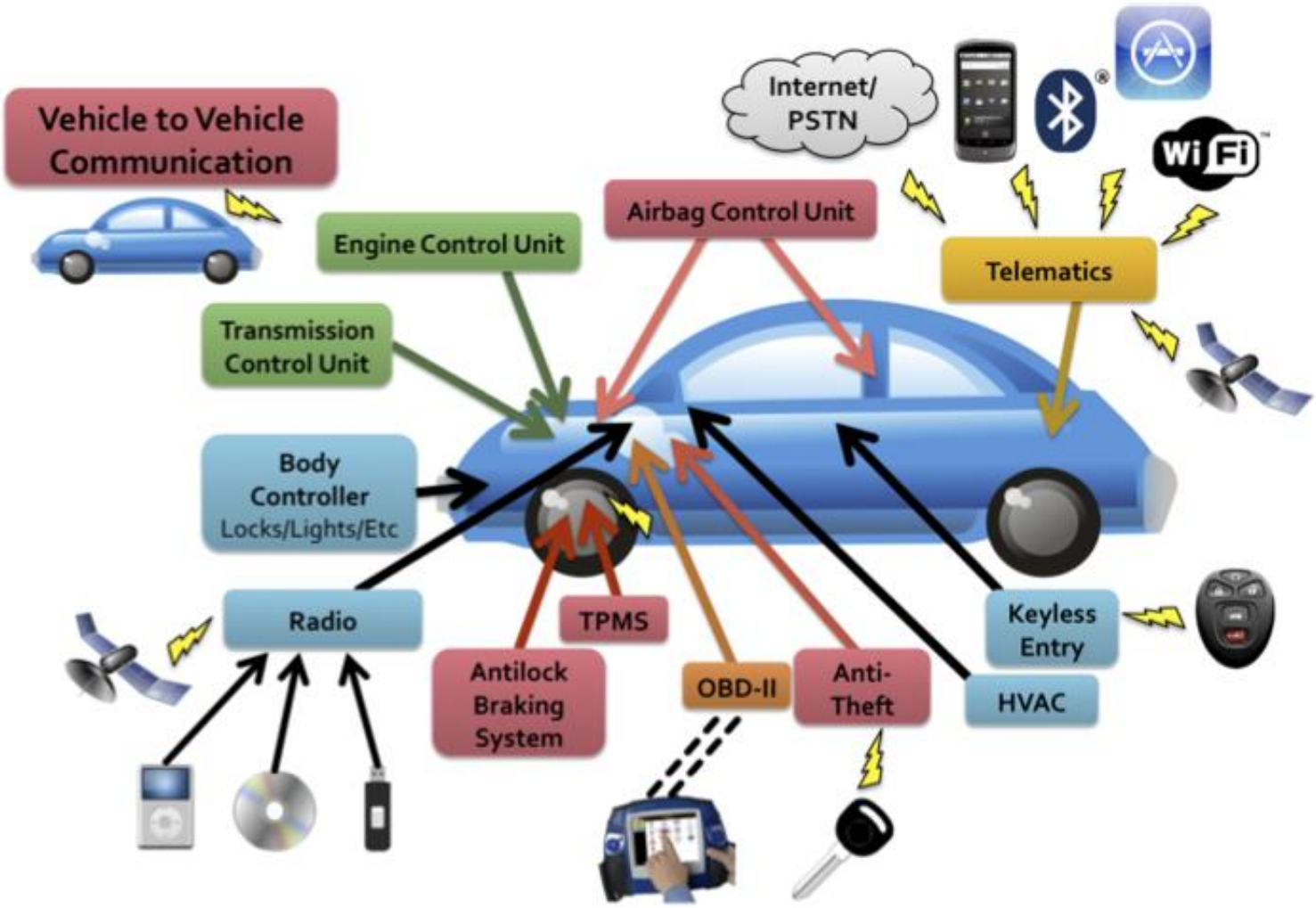
Attack Surface

Attack surface: the set of ways an application can be attacked.

Used to measure attackability of app.

- The larger the attack surface of a system, the more likely an attacker is to exploit its vulnerabilities and the more damage is likely to result from attack.
- Compare to measuring vulnerability by counting number of reported security bugs.
- Both are useful measures of security, but have very different meanings.

Automotive Attack Surface



http://marcoramilli.blogspot.com/2012/01/automotive-attack-surface.html

Why Attack Surface Reduction?

If your code is perfect, why worry?

- All code has a nonzero probability of containing vulnerabilities.
- Even if code is perfect now, new vulns arise.
  - Format string vulnerability was discovered in 1999.
  - A particular application was immune to XML injection until you added an XML storage feature.

Allows focus on more dangerous code.

- Address Space Randomization ASR eliminates unnecessary exposures.
- Allows focus on required exposures.

Attack Trees

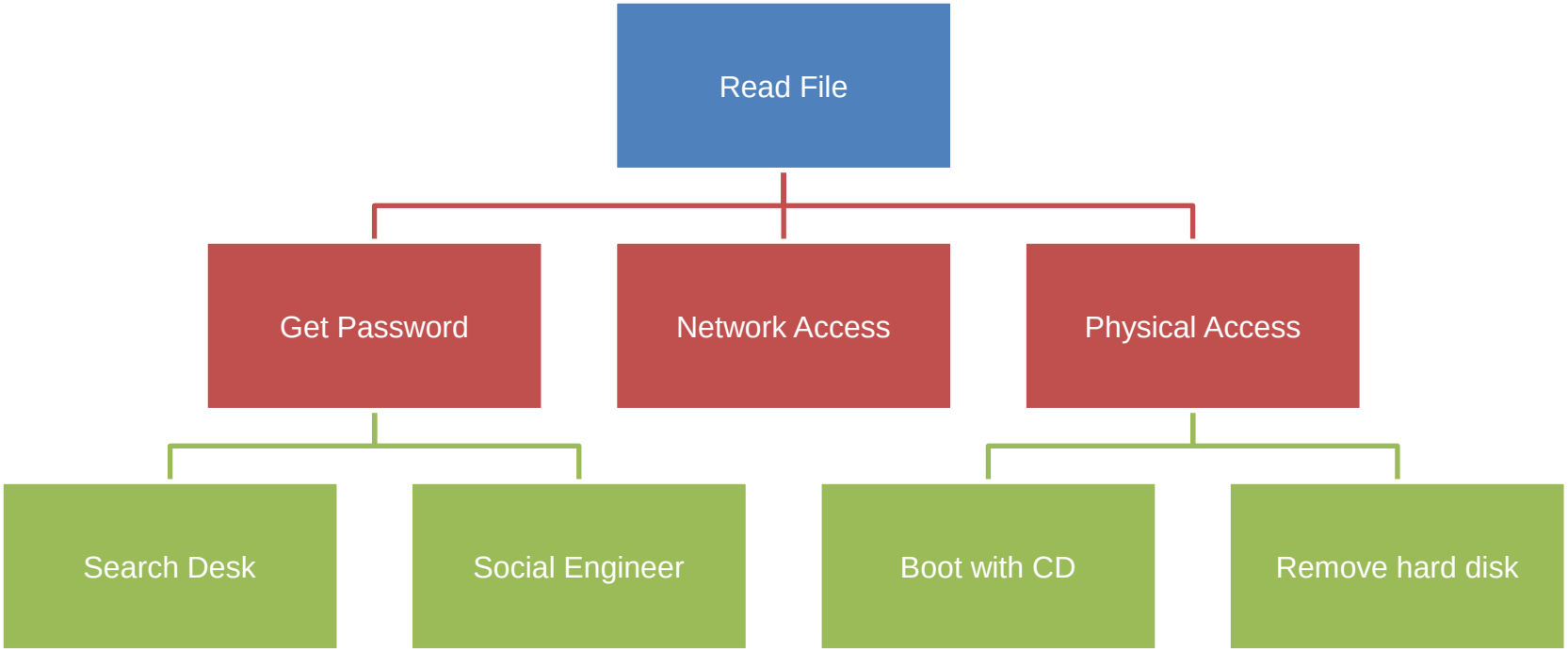
Attack Trees are a way to model possible attacks against a specific target or asset.

- Model attacks using a tree structure with target at top.
- AND nodes: all node actions must be completed for attack to be successful.
- OR nodes: any node action leads to a successful attack

Attack Trees—Graph Notation

Example of getting password

Goal: Read file from password-protected PC.



Attack Trees—Text Notation

Goal: Read message sent from one PC to another.

1. Convince sender to reveal message.
    - 1.1 Blackmail.
    - 1.2 Bribe.
2. Read message when entered on sender's PC.
    - 1.1 Visually monitor PC screen.
    - 1.2 Monitor EM radiation from screen.
3. Read message when stored on receiver's PC.
    - 1.1 Get physical access to hard drive.
    - 1.2 Infect user with spyware.
4. Read message in transit.
    - 1.1 Sniff network.
    - 1.2 Usurp control of mail server.

Attack Tree Activity

Create an attack tree for the following scenario.

- The target of the attack is a specific technical document available on a secured fileserver.
- The attacker is outside of the target's network.
- The target network perimeter is secured by a firewall.
- Many users work for the target who do not have access to the desired document.
- A specific user group who worked on the document are the only users who have access to it.
- System administrators have access to all files.

Your attack tree must

- Have at least 3 nodes below the root (goal) node.
- Use both AND and OR combined nodes.

Legal Issues for Cybercrime

- Computer crime laws exist at all levels
  - State level
  - Federal level: Computer Fraud and Abuse Act
  - International Convention on Cybercrime
- But it can be difficult or costly to track down and prosecute attackers, especially if international.
- Requirements exist to report data breaches
  - Different state-level laws exist in US.
  - In 2018, the General Data Protection Regulation (GDPR) EU regulation requires reporting and affects US businesses with customers from the EU.

Legal Issues for Cyberwar

Most nations treat cyber attacks as criminal matter as

- No international treaty exists to regulate cyber attacks.
- It is difficult to attribute attacks to a specific nation.
- It is uncertain which types of attacks would be considered acts of war: copying data, destroying data or denying service, defacement, or destruction of machinery controlled by computers.
- It is uncertain whether active response to an attack would be legal under international law.

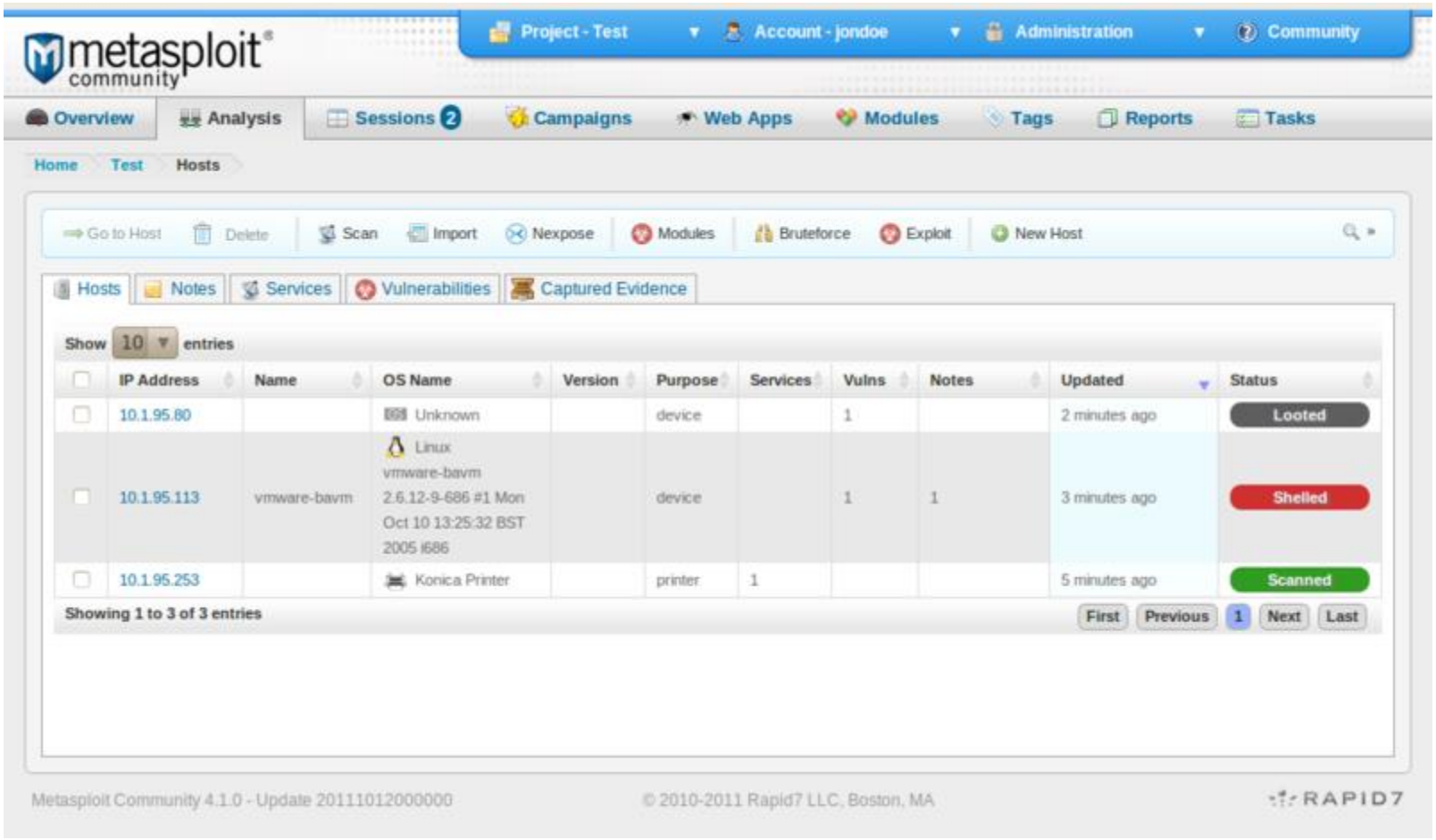
Exploits

An **exploit** is a technique or tool that takes advantage of a vulnerability to violate an implicit or explicit security policy.

Exploits can be categorized by

1. The type of vulnerability they exploit.
2. Local (runs on vulnerable host) or remote.
3. Result of exploit (elevation of privilege, DoS, spoofing, remote access, etc.)

Exploitation Frameworks



Indicators of Compromise

Indicators of compromise are artifacts found on a system that provide evidence of a successful attack.

- Malware signatures
- IP addresses used in malicious activity
- URLs or domain names used by botnets
- MD5 checksums of malicious files

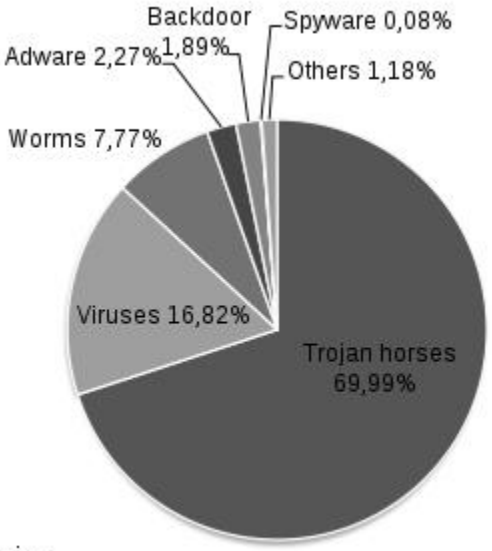
Malware

Malware, short for malicious software, is software designed to gain access to confidential information, disrupt computer operations, and/or gain access to private computer systems. Malware can be classified by how it infects systems:

- Trojan Horses
- Viruses
- Worms

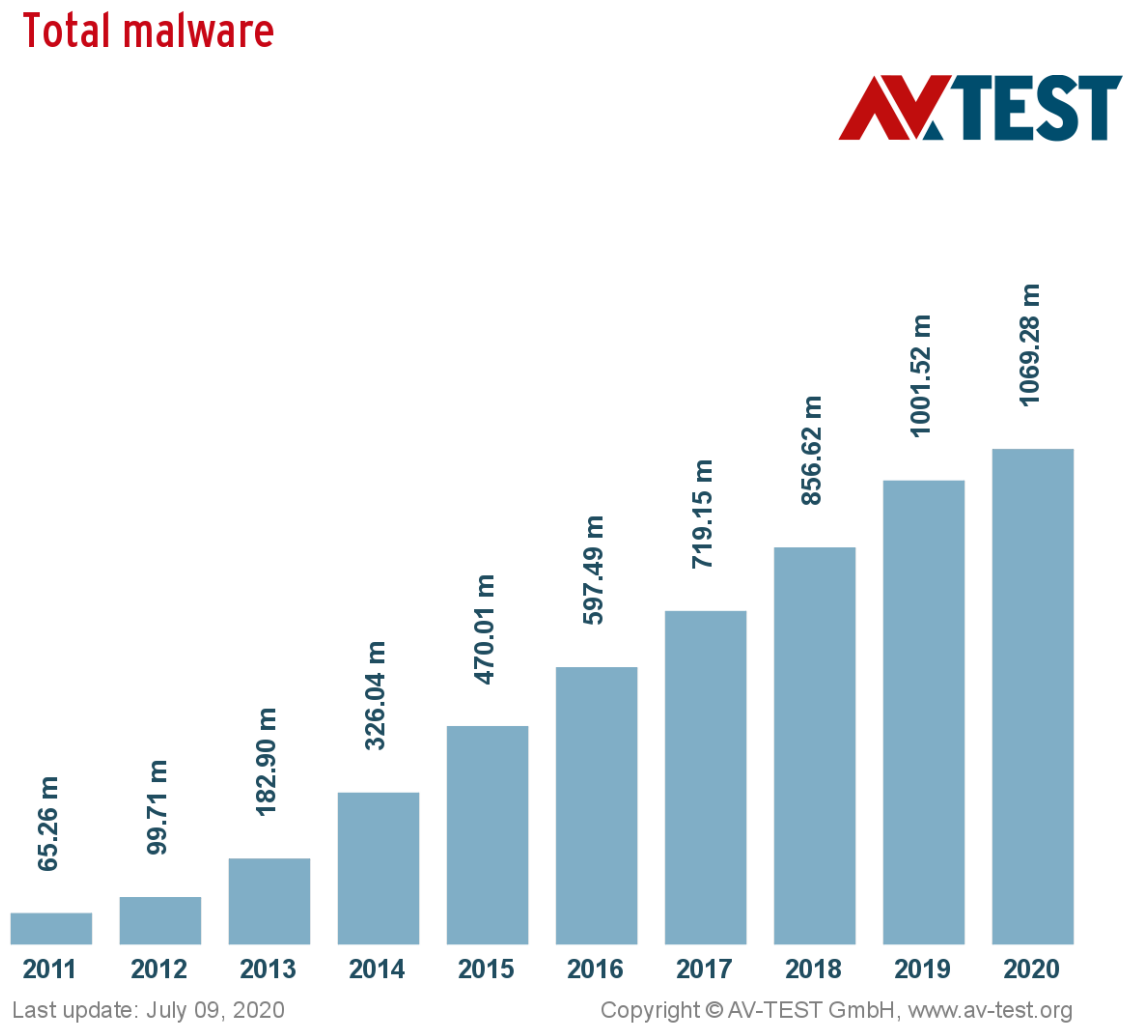
Or by what assets it targets:

- Ransomware
- Spyware and adware
- Backdoors
- Rootkits
- Botnets



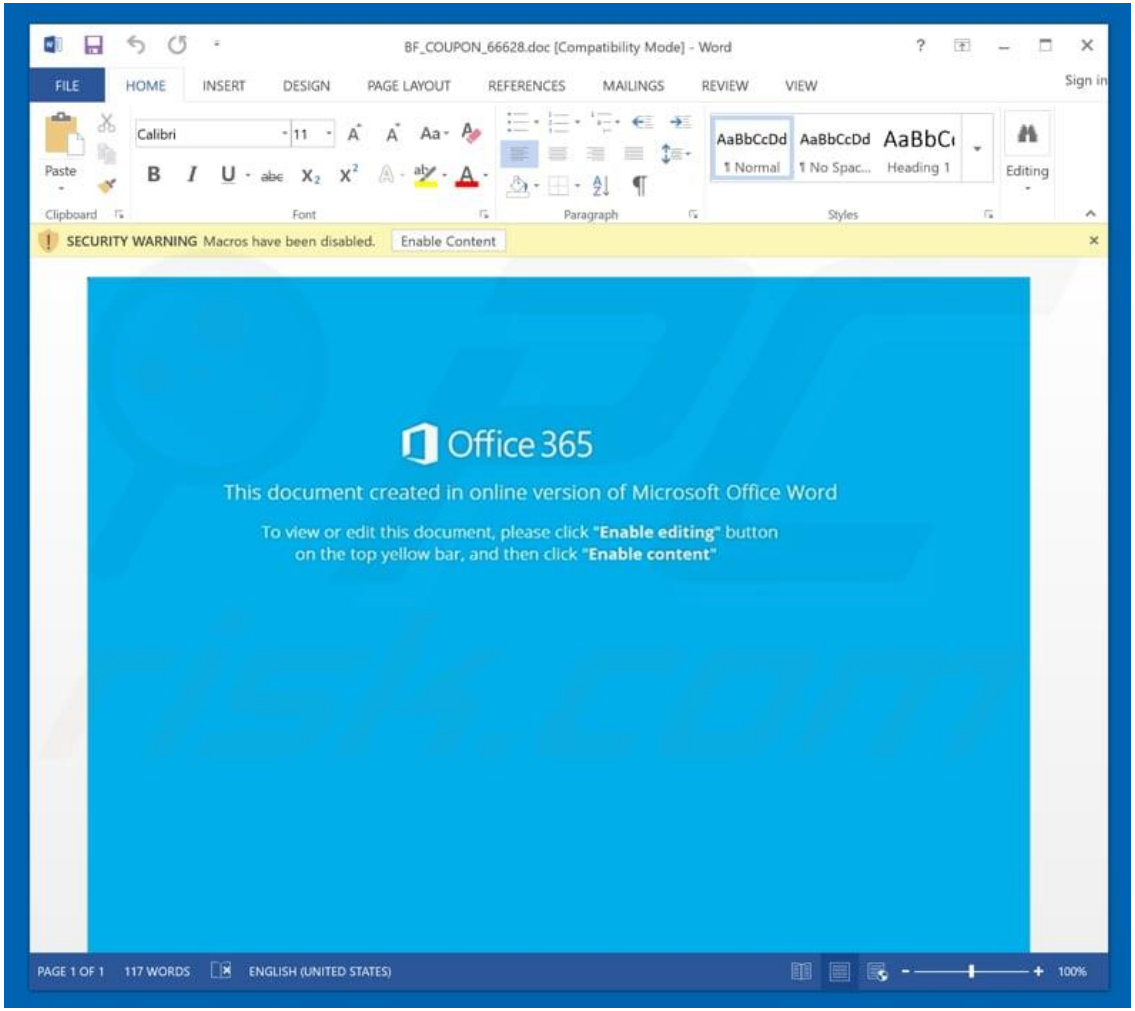
Malware by categories

How much malware is out there?



Trojan Horses

Trojan Horse Examples

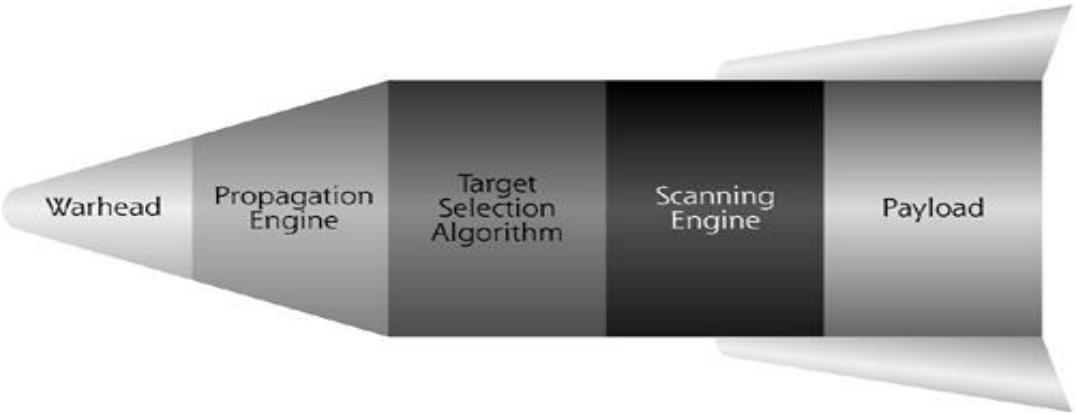


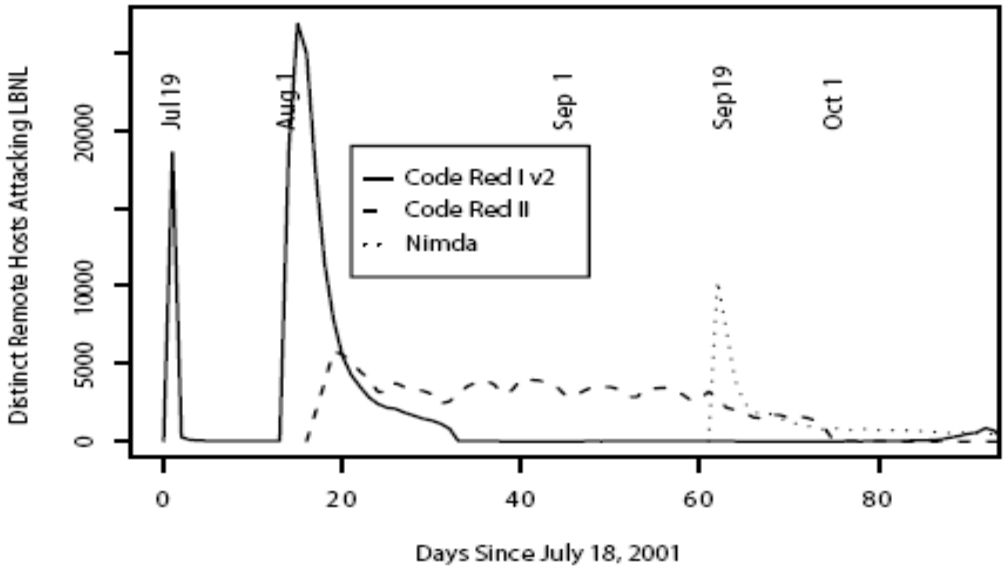
Viruses

A **computer virus** is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other files. This process is called **infecting**.

Worms

A **worm** is a type of malware that spreads itself to other computers.





Ransomware


CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
10/9/2013
4:25 PM
Time left
95 : 56 : 35
Next >>


Federal Bureau of Investigation
International Police Association
ATTENTION!
Your computer has been Locked
MoneyPak
Your PC is blocked due to at least one of the reasons specified below.
Pay with Moneypak:
Load Cash on a MoneyPak
Enter 200$ MoneyPak code:
Where I can buy MoneyPak?
Walmart
KASPERSKY lab
McAfee
Dr.WEB

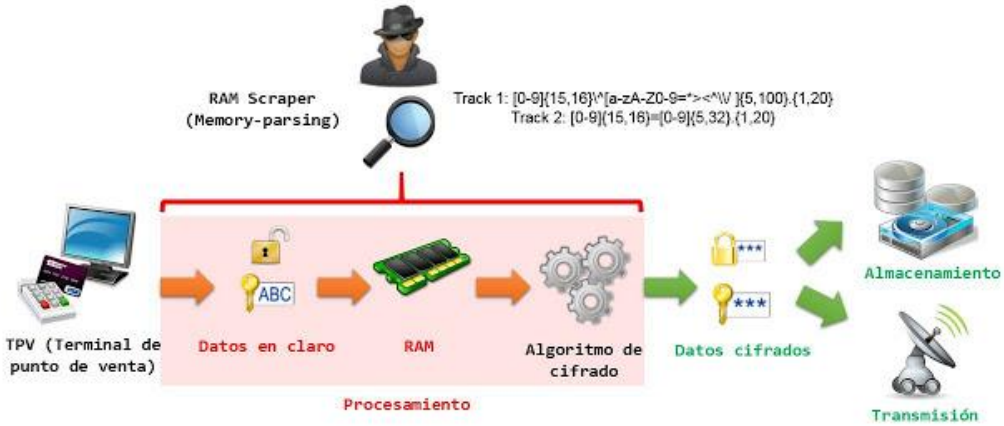
Ransomware


Your computer has been locked!
Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:
18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography
Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.
Technical details:
Involved IP address:
Involved host name:
Source or intermediary sites:
All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.
Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.
In order to resolve the situation in an above-mentioned way you should pay a fine of $300.
Permanent lock on
HOW TO UNLOCK YOUR COMPUTER:
1
Take your cash to one of this retail locations:
Walmart
CVS pharmacy
Walgreens
2
Get a MoneyPak and purchase it with cash at the register
MoneyPak
3
Come back and enter your MoneyPak code to unlock your computer (5 attempts available)
Code:
Submit
1 2 3
4 5 6
7 8 9
Delete 0 Enter
RE!oadit.
How do I unblock the PC using the Reloadit?
VONS
Dominick's
GENUARDI'S
Tom Thumb
PAVILIONS
CARRS
SAFEWAY
Randalls

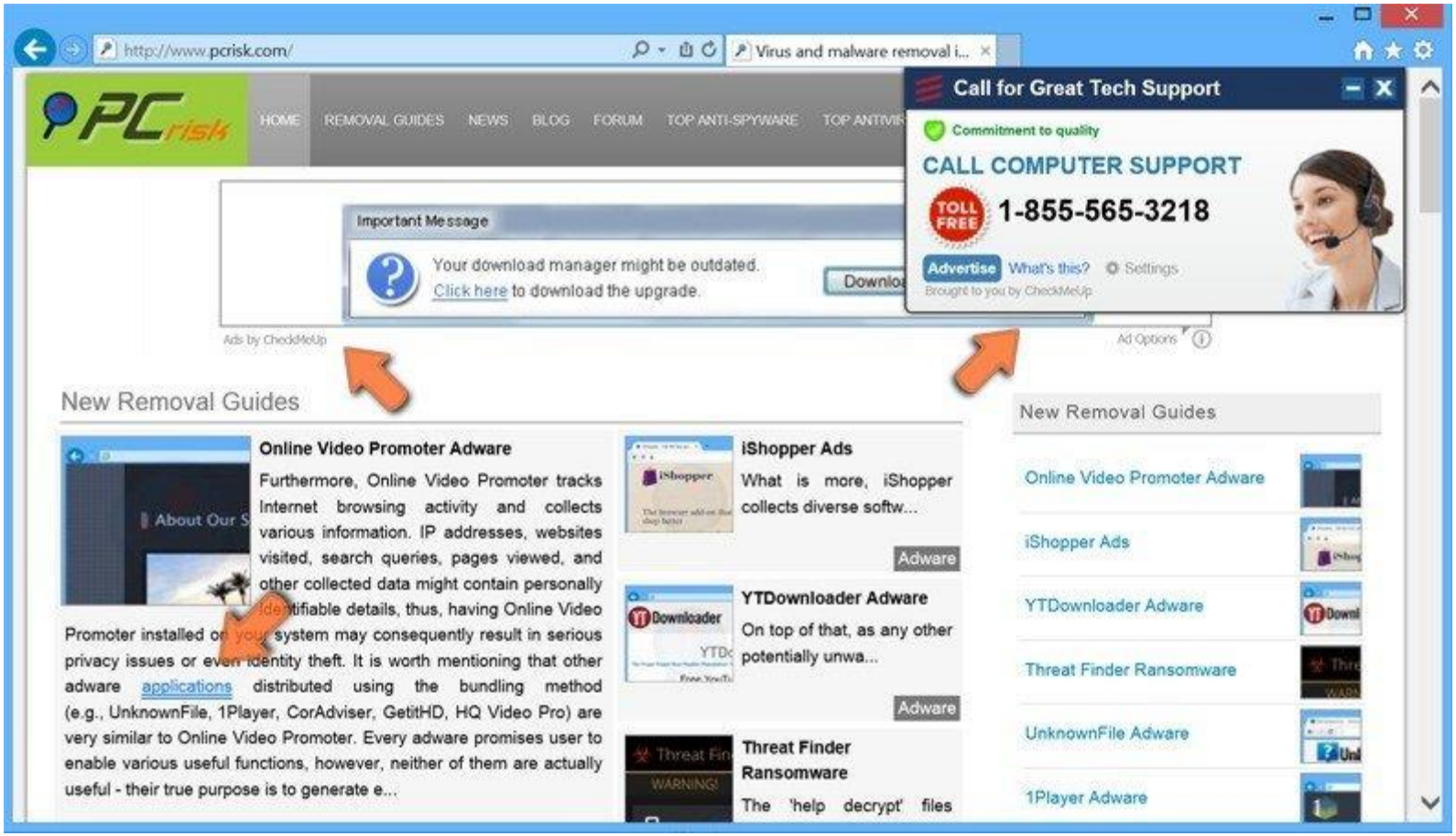
Information Stealers

Information stealers target specific types of information, such as passwords, financial credentials, private information, etc.

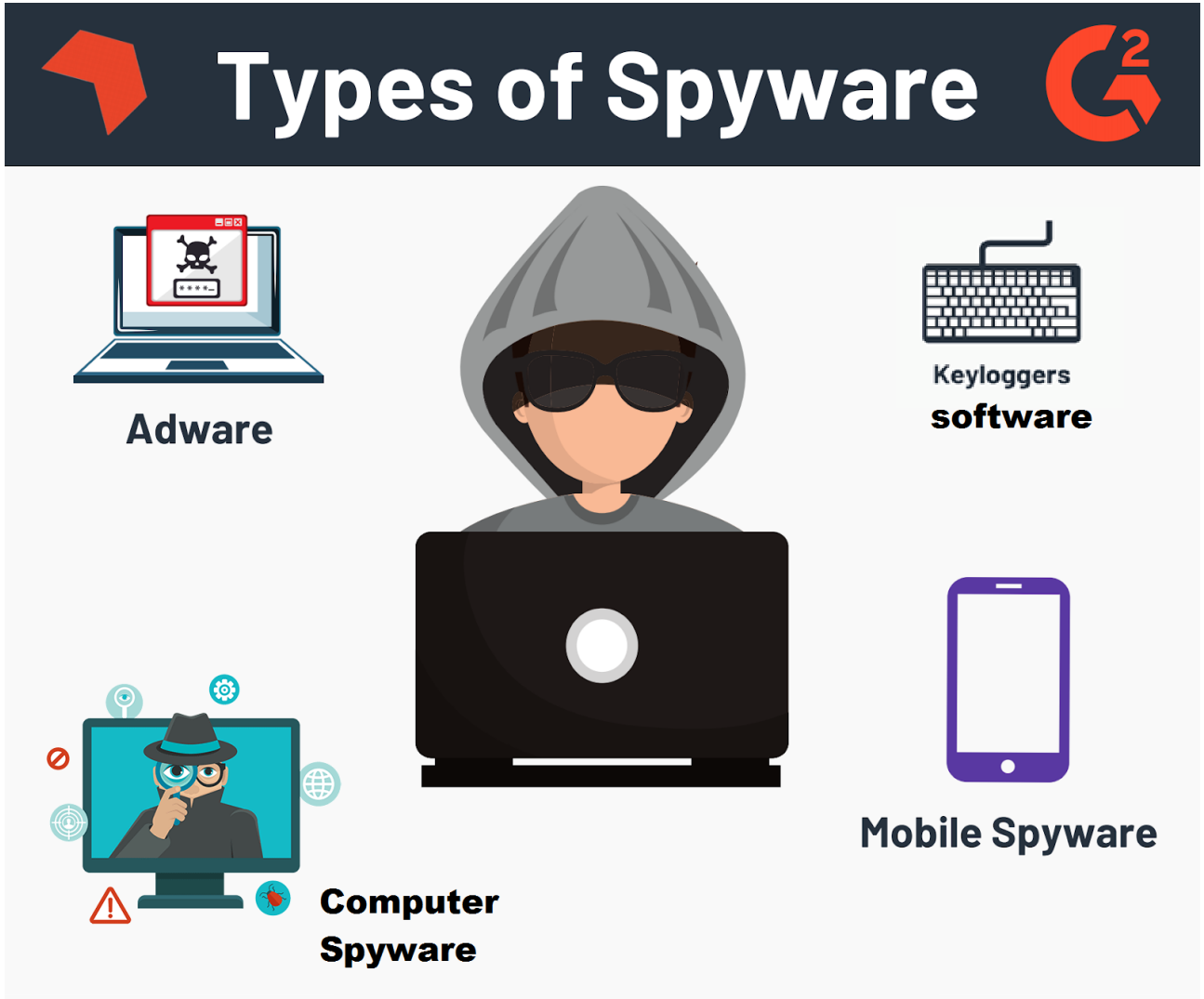
- Keyloggers (can be hardware too)
- Desktop recorders
- Memory scrapers



Spyware and Adware

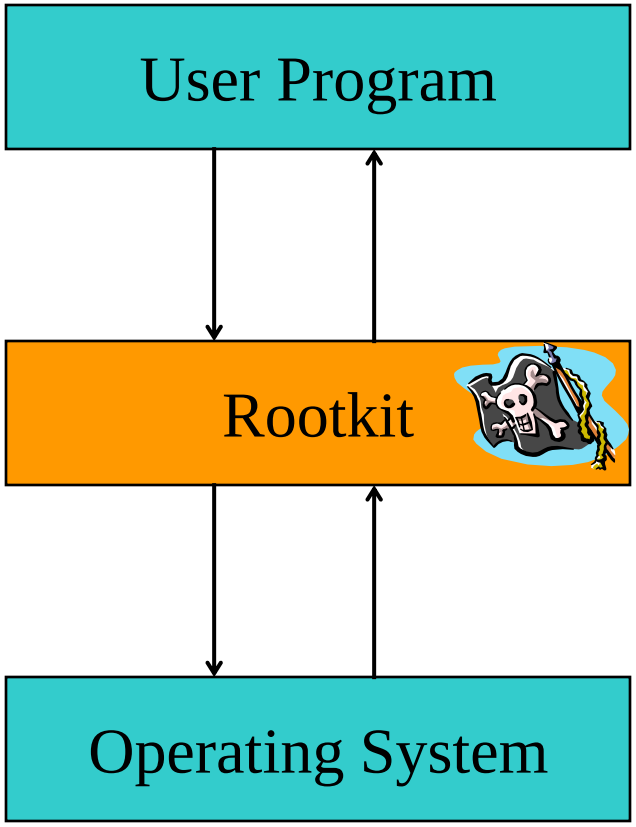


Spyware


Types of Spyware
Adware
Keyloggers
software
Mobile Spyware
Computer
Spyware

Rootkits

- Execution Redirection
- File Hiding
- Process Hiding
- Network Hiding
- Backdoor



Covert Channels

Covert channels enable communication using techniques not meant for information exchange.

- Malware could increase CPU usage to 100% to communicate a 1, regular usage is a 0.
- Malware could fill a storage device to 100% to communicate a 1, non-full device is a 0.
- Malware could send 2 packets/second to indicate a 1, 1 packet/second to indicate a 0.

Looks a legitimate channel

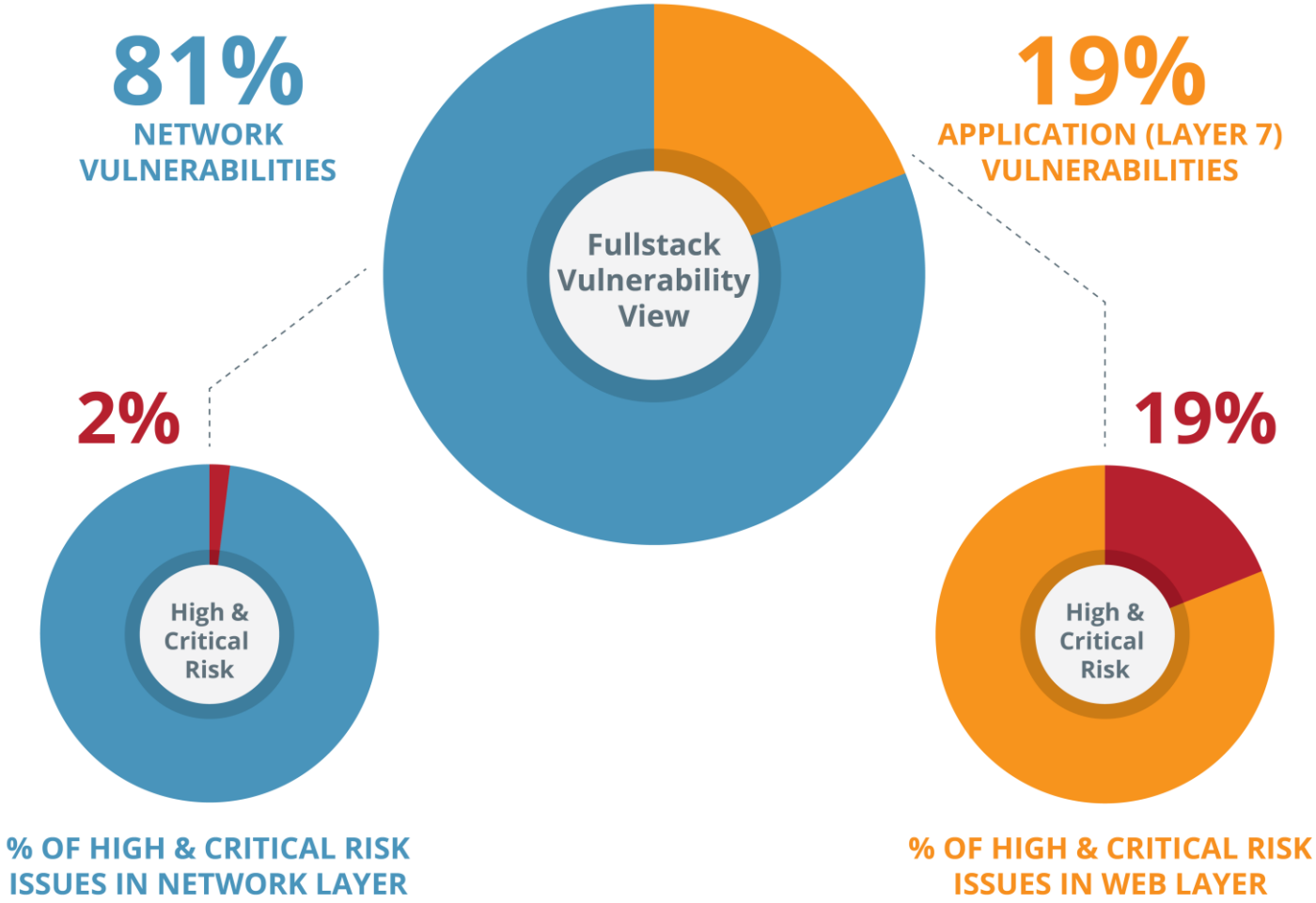
ex. http connection

Botnets

Vulnerabilities

Vulnerabilities can be found in ***any*** software:

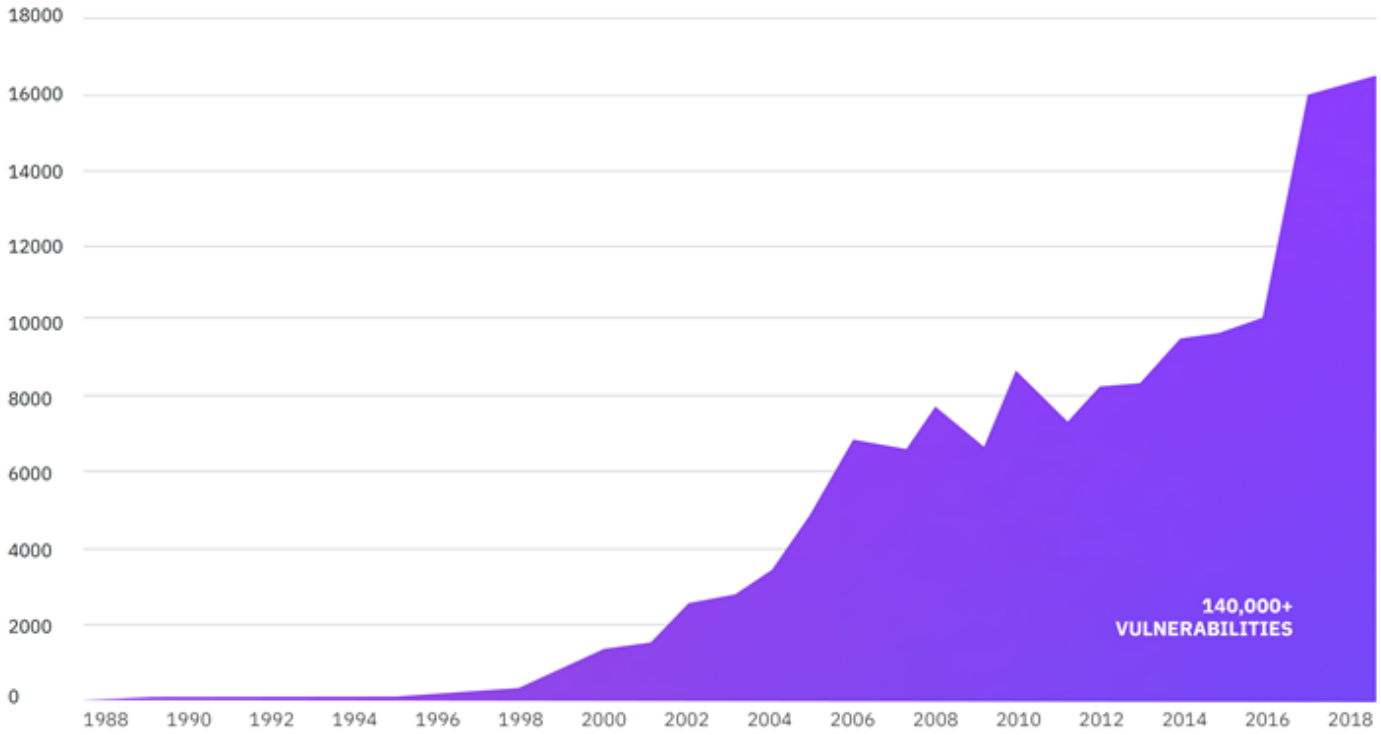
- **PC:** Office, Adobe Reader, web browsers
- **Server:** Databases, DNS, mail server software, web servers, web applications, etc.
- **Mobile:** Mobile phone OS, mobile applications
- **Embedded**: printers, routers, switches, VoIP phones, cars, medical devices, TVs, etc.
- **Third party software:** Web browser plugins, Ad affiliate network JavaScript include files, Mobile ad libraries


81%
NETWORK VULNERABILITIES
19%
APPLICATION (LAYER 7) VULNERABILITIES
Fullstack Vulnerability View
2%
High & Critical Risk
% OF HIGH & CRITICAL RISK ISSUES IN NETWORK LAYER
19%
High & Critical Risk
% OF HIGH & CRITICAL RISK ISSUES IN WEB LAYER

Software Vulnerabilities

Total Recorded Vulnerabilities Year Over Year

Source: X-Force Red Vulnerability Database

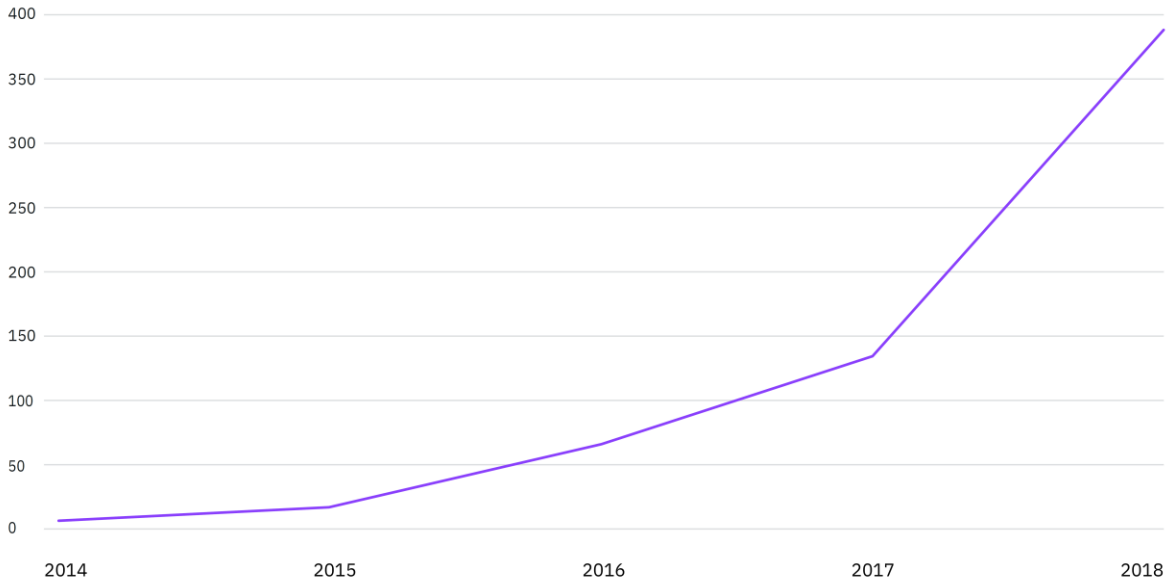


IBM X-Force 2019 Trend and Risk Report

IoT Vulnerabilities

Number of IoT Vulnerabilities Since 2014

Source: X-Force Red Vulnerability Database



IBM X-Force 2019 Trend and Risk Report

Embedded Vulnerabilities

SUNDAY, AUGUST 18TH

the security ledger

INTERNET OF THINGS | THREATS | PODCASTS | REPORTS | VIDEO

You are here: Home » Business » Security Hole in Samsung Smart TVs Could Allow Remote Spying

Security Hole in Samsung Smart TVs Could Allow Remote Spying

POSTED BY: PAUL DECEMBER 12, 2012 11:27 13 COMMENTS

The company that made headlines in October for publicizing zero day holes in SCADA product says it has uncovered a remotely exploitable security hole in Samsung Smart TVs. If left unpat the vulnerability could allow hackers to make off with owners' social media credentials and eve spy on those watching the TV using compatible video cameras and microphones.

In an e-mail exchange with Security Led Malta-based firm said that the previousl unknown ("zero day") hole affects Samsu Smart TVs running the latest version of company's Linux-based firmware. It cou an attacker the ability to access any file available on the remote device, as well as external devices (such as USB drives) connected to the TV. And, in a Orwellian twist, the hole could be used to access cameras and

Wireless Car Hacking Demonstrated in New Video

Comments

THURSDAY, AUGUST 08, 2013 CATEGORIES: GADGETS, OFFBEAT NEWS, REPORTS, VIDEO |

There really is no need to present the worst-case scenario, when it comes to the hacking of modern cars, because everybody's familiar with its implications. The more systems are controlled by software, the more vulnerable to "cyber attacks" the vehicle is.

Mitigations

A **mitigation** is a process, technique, tool, or software modification that can prevent or limit exploits against vulnerabilities.

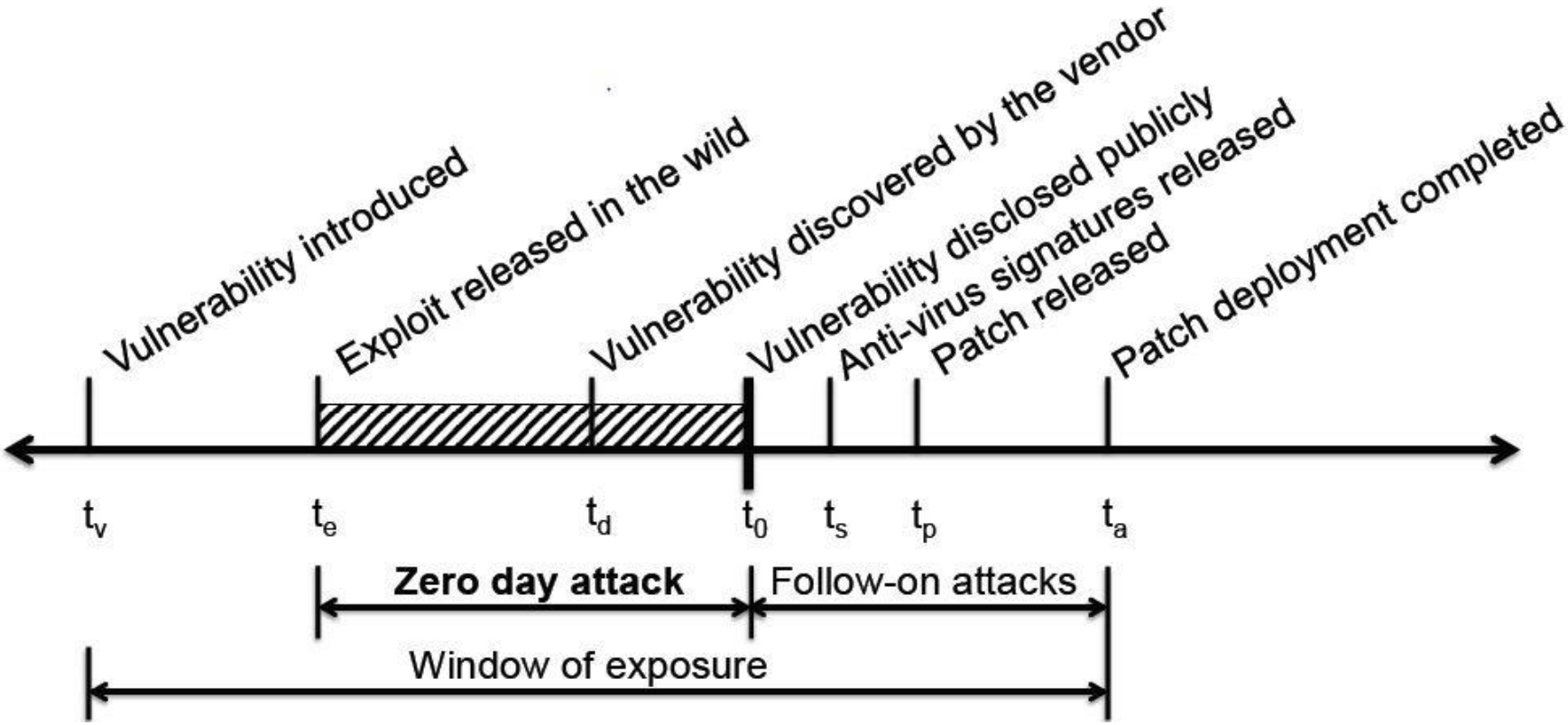
- A password length policy is a process mitigation to protect against password guessing attacks.
- A firewall is a tool mitigation that limits exploits by blocking certain types of network traffic.
- Checking for the lock icon in the location bar of your browser is a technique mitigation for verifying that web connections are encrypted.

Security Patches

A **security patch** is a software modification designed to prevent or limit a vulnerability. A patch is a type of mitigation.

- Administrator may have to apply manually.
- Some vendors specify certain days to patch, such as "Patch Tuesday," the 2nd Tuesday of the month when MS releases updates.
- Increasingly software auto updates itself with current patches.

Vulnerability Timeline



Zero Day

A **zero day** vulnerability, attack, or exploit is a newly discovered one for which no patch currently exists.

- Once a patch is released, the vulnerability, attack, or exploit is no longer a zero day.

Google's Project Zero focuses on finding zero day vulnerabilities in open source and commercial software before attackers do.

Summary

- Definitions
  - threat, threat model, APT, attack, attack surface, attack vector, indicators of compromise, exploit, vulnerability, mitigation, patch, zero day, malware
- Four Quadrant Threat Model
  - Expertise: off-the-shelf tool users up to sophisticated built your own
  - Focus: broad attack anyone to targeted attacks on high value victims
- Attack types: spam, phish, spoof, sniff, MITM, DoS
- Malware types: Trojan, virus, worm
- Vulnerability lifecycle
  - Introduction, zero-day, patch, window of exposure
- You can improve the security of a system by
  - Mitigating vulnerabilities
  - Reducing attack surface