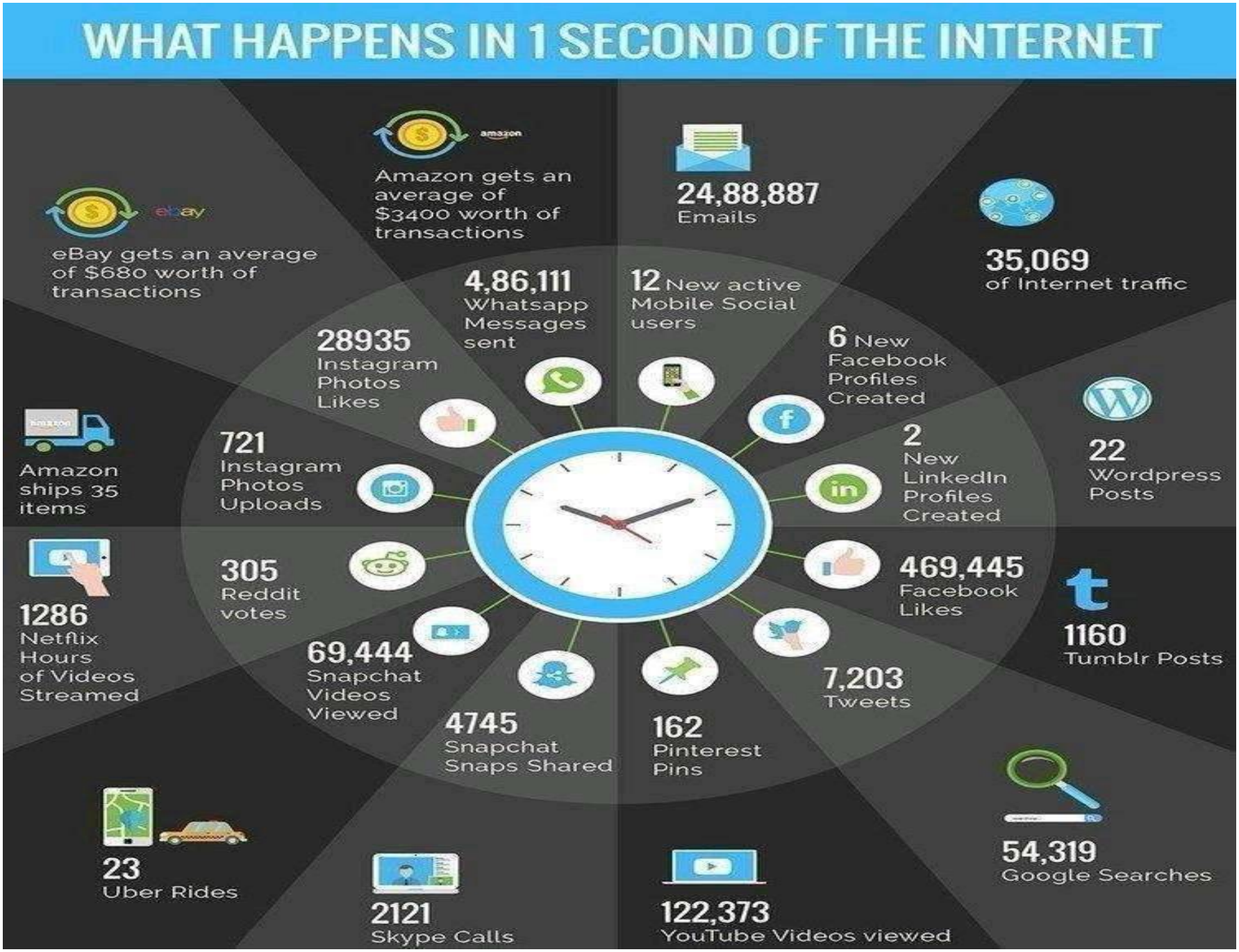
Internet Security Architectures: Research issues

Dr. Bhawana Rudra

NITK

Why are we talking about cybersecurity?

Disclaimer: Images and information has been taken from various resources of the web


WHAT HAPPENS IN 1 SECOND OF THE INTERNET
Amazon gets an average of $3400 worth of transactions
eBay gets an average of $680 worth of transactions
24,88,887 Emails
35,069 of Internet traffic
4,86,111 Whatsapp Messages sent
12 New active Mobile Social users
28935 Instagram Photos Likes
6 New Facebook Profiles Created
2 New LinkedIn Profiles Created
22 Wordpress Posts
721 Instagram Photos Uploads
Amazon ships 35 items
305 Reddit votes
469,445 Facebook Likes
1286 Netflix Hours of Videos Streamed
1160 Tumblr Posts
69,444 Snapchat Videos Viewed
7,203 Tweets
4745 Snapchat Snaps Shared
162 Pinterest Pins
54,319 Google Searches
23 Uber Rides
2121 Skype Calls
122,373 YouTube Videos viewed

What's in an internet minute? According to data from RiskIQ and threat researchers around the world, a lot of evil.

2018 COST OF CYBER CRIME

TOTAL COST

$600 BILLION[1]

$1,138,888/minute

$171,233/minute spend by business on information security[2]

Globally, for large businesses affected, the average cost was **$11.7 MILLION**/year[3]

Ranging from **$222**/minute

CYBERCRIME VICTIMS

2.7 MILLION/day[4]

1,861/minute

RANSOMWARE

costs to organizations

$8 BILLION/year[5]

$15,221/minute[5]

1.5 organizations/minute fall victim to ransomware attacks[6]

MALWARE

1,274 new malware variants/minute[7]

PHISHING EMAILS

22.9 attacks/minute[8]

RECORDS LEAKED

from publicly disclosed incidents

2.9 BILLION/year[9]

5,518/minute

- **Kevin** David Mitnick arrested in 1995 and five years in prison for various computer and communications-related crimes. Now a American computer security consultant, author, and convicted **hacker.**
- Vladimir Leonidovitch Levin is a Russian individual famed for his involvement in the attempt to fraudulently transfer USD 10.7 million via Citibank's computers
- **Gary** McKinnon a **Scottish** systems administrator and **hacker** who was accused in 2002 of perpetrating the biggest military computer **hack** of all time.

- 'Denial of Service' (DOS)1 attack on some of the popular e-commerce sites in 1999, caught national attentions.

- Attack resulted in people using transportation for free on 27-11-2016
  - < 2000 devices were compromised
- “You Hacked, ALL Data Encrypted. Contact For Key(cryptom28@yandex.com)ID:681, Enter”.
- Ransom of 100 Bitcoin ($70000)

San Francisco's local transport system was targeted over the weekend

San Francisco’s transport agency has been hit

Case 1: Internet Under Siege

- **February 7 - 9, 2000**
  Yahoo!, Amazon, Buy.com, CNN.com, eBay, E*Trade, ZDNet websites hit with massive DOS

- Attacks received the attention of president Clinton and Attorney General Janet Reno.

- **“A 15-year-old kid could launch these attacks, it doesn’t take a great deal of sophistication to do”**
  – Ron Dick, Director NIPC, February 9

- U.S. Federal Bureau of Investigation (FBI) officials have estimated the attacks caused $1.7 billion in damage

Case 2: Slammer Worm

- **January 2003**
  Infects 90% of vulnerable computers within 10 minutes
- **Effect of the Worm**
  - Interference with elections
  - Cancelled airline flights
  - 911 emergency systems affected in Seattle
  - 13,000 Bank of America ATMs failed
- **No malicious payload!**
- **Estimated ~$1 Billion in productivity loss**

Case 3: WorldCom

- **July 2002**
  WorldCom declares bankruptcy
- **Problem**
  WorldCom carries 13% - 50% of global internet traffic. About 40% of Internet traffic uses WorldCom's network at some point
- **October 2002**
  Outage affecting only 20% of WorldCom users snarls traffic around the globe
- **Congressional Hearings**
  Congress considers, but rejects, extension of FCC regulatory powers to prevent WorldCom shutdown

Vulnerabilities are not just technical

Case 4: September 11

- **Wireless Tower on Top of Trade Center Destroyed**
- **AT&T has record call volumes**
- **“Flash” usage severely limits availability**
- **Rescue efforts hampered**

Physical Vulnerability!

Legitimate Usage!

CYBERATTACK ON A GERMAN STEEL-MILL

UAE a target of 5 per cent of global cyber attacks

Rapid growth in digital transactions spurs 500% rise in online crimes in five years, security expert says

22 JAN 2014 NEWS

Energetic (Russian) Bear Attacking Western Energy Sector

Hacking into homes: 'Smart home' security flaws found in popular system

May 02, 2016 Contact Nicole Casal Moore

Top 10 Cyber Security Trends for 2019

01
The Coming Pain of GDPR

General Data Protection Regulation is expected to have a significant effect in 2019.

02
Increase in Sabotage, Espionage and Crime by Rogue Nation-States

The cyber security teams have to rely on techniques of breach detection.

03
Dark Ages of Single Factor Passwords

They are still the main security protection for most organizations in spite of the ease and low cost deployment of the multi-factor authentication solutions.

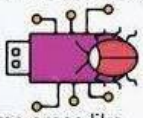
04
Insecure Clouds

Inspite of the continual publicity of repeated breaches, most organizations still fail to deploy and enforce good housekeeping across their entire cloud data estate.

05
Growth of Cyber Hygiene in companies

Response from the organizations will be in the form of cyber education combined with monitoring, measuring, and testing cyber behavior of staff.

06
Malware Challenges



Some areas like ransomware will see an increased sophistication together with increased malware volumes in some areas and new malware approaches.

07
Increased Risks with bad Housekeeping & Shadow IT Systems

Both cases are very easy attack surfaces with substantial oversight, budget challenges,internal politics and were seen in the past as a lower resolution priority.

08
More Challenges in IoT

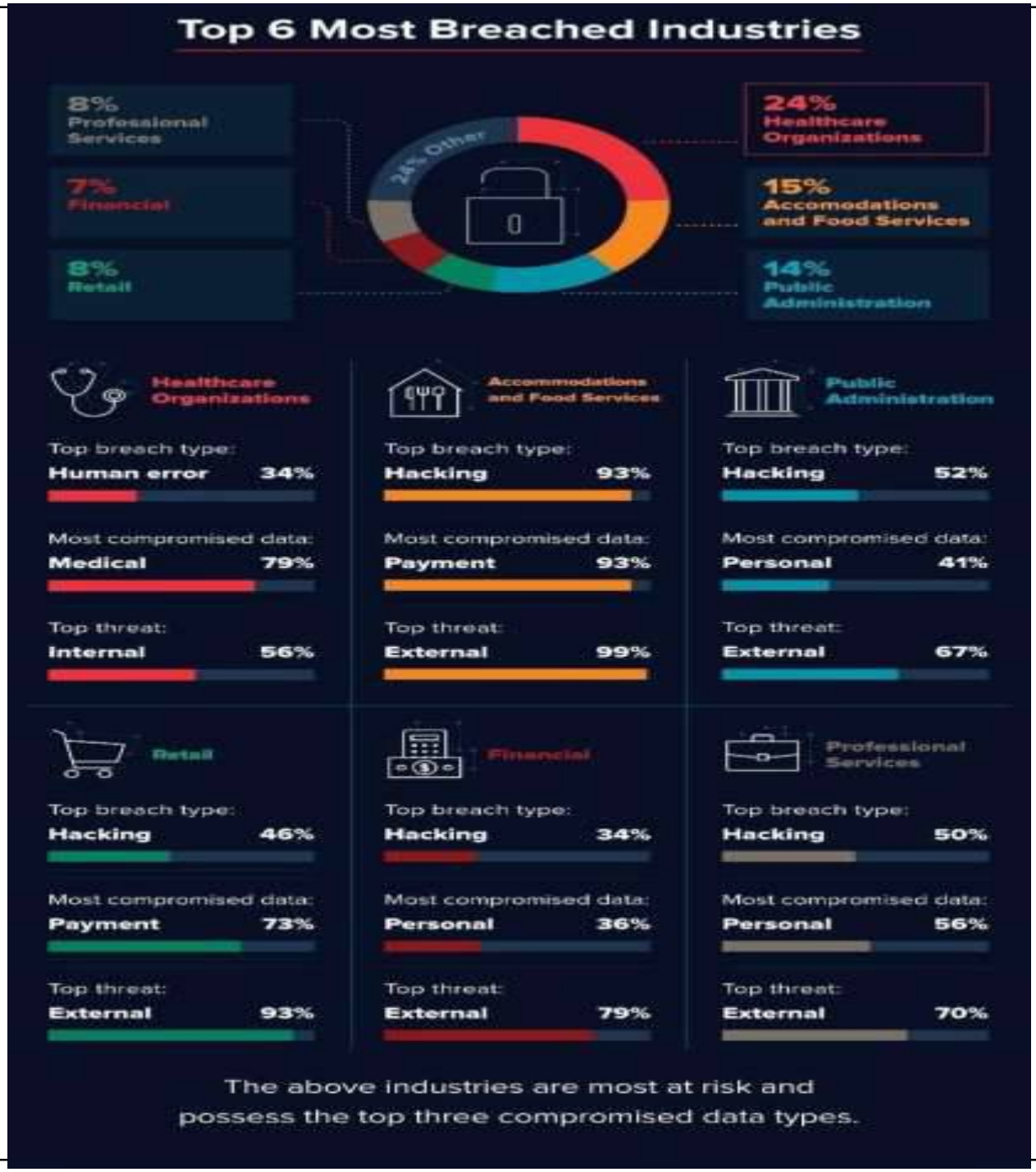
With the lack of standard or perceived security need, IoT is going to be deployed even more and create insecurity in areas which used to be secure.

09
Boardroom Cyber Security

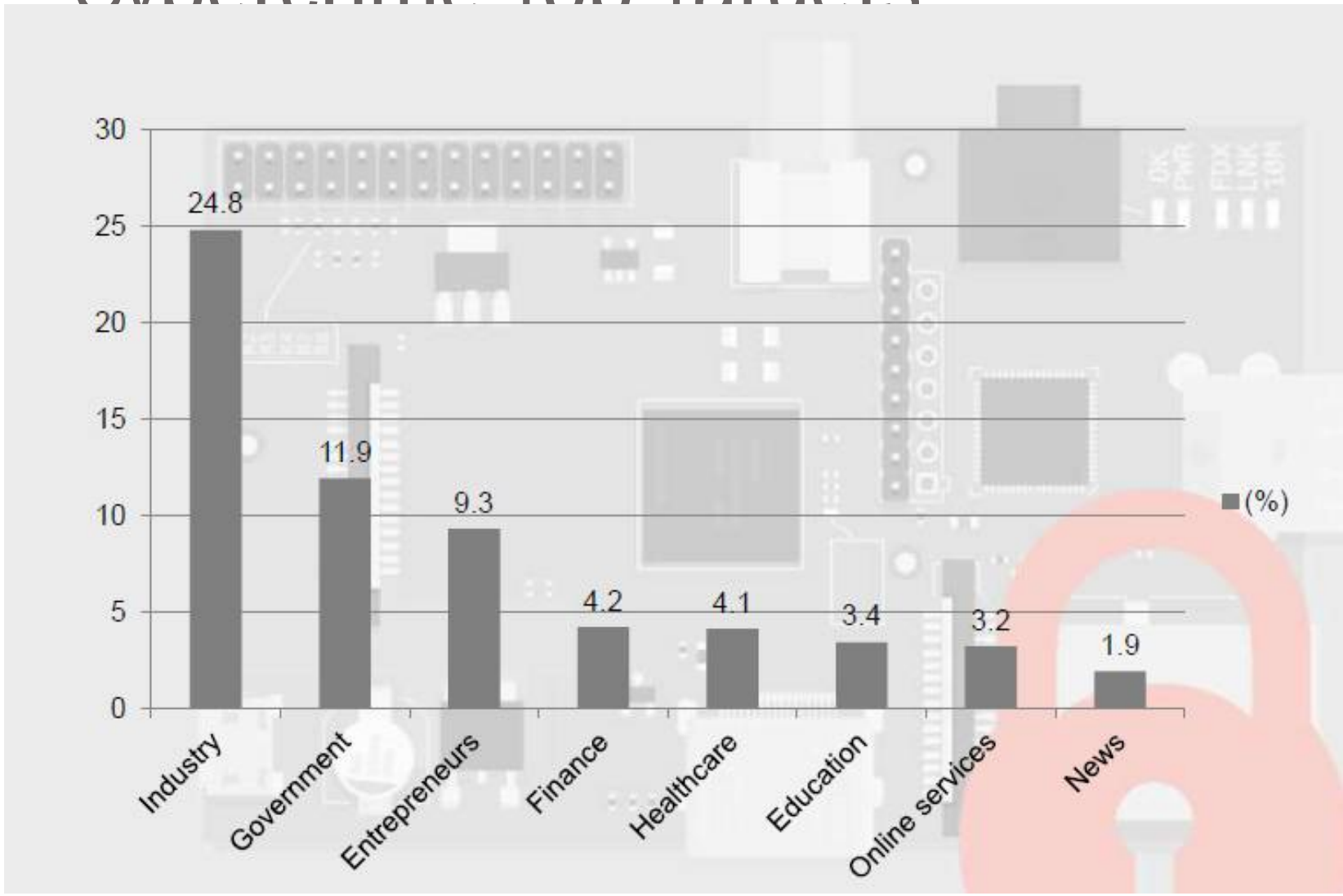
This trend will accelerate this 2019 with boards demanding understanding and clarity in an area which was often delegated as subcomponent of the role of CISOs.

10
Unseen Nightmare of DDoS

DDoS is a dirty secret for most organizations, with attacks continuing to grow in 2019 together with the price of defending against them.


Top 6 Most Breached Industries
8%
Professional Services
7%
Financial
8%
Retail
24% Other
24%
Healthcare Organizations
15%
Accomodations and Food Services
14%
Public Administration
Healthcare Organizations
Top breach type:
Human error 34%
Most compromised data:
Medical 79%
Top threat:
Internal 56%
Accommodations and Food Services
Top breach type:
Hacking 93%
Most compromised data:
Payment 93%
Top threat:
External 99%
Public Administration
Top breach type:
Hacking 52%
Most compromised data:
Personal 41%
Top threat:
External 67%
Retail
Top breach type:
Hacking 46%
Most compromised data:
Payment 73%
Top threat:
External 93%
Financial
Top breach type:
Hacking 34%
Most compromised data:
Personal 36%
Top threat:
External 79%
Professional Services
Top breach type:
Hacking 50%
Most compromised data:
Personal 56%
Top threat:
External 70%
The above industries are most at risk and possess the top three compromised data types.

Cybercrime Top Targets



Case 5: It's a Jungle Out There

- The Internet is highly, globally connected
- Viruses/worms are legion on the Internet and continue to scan for vulnerable hosts
- Hackers scan looking for easy targets to attack

Increasing Dependence

We are increasingly dependent on the Internet:

Directly

- **Communication (Email, IM, VoIP)**
- **Commerce (business, banking, e-commerce, etc)**
- **Control systems (public utilities, etc)**
- **Information and entertainment**
- **Sensitive data stored on the Internet**

Indirectly

- **Biz, Edu, Gov have *permanently* replaced physical / manual processes with Internet-based processes**

Security Not A Priority

Other design priorities often trump security:

Cost

Speed

Convenience

Open Architecture

Backwards Compatibility

Cybersecurity Roadblocks

- **No metrics to measure (in)security**
- **Internet is inherently international**
- **Private sector owns most of the infrastructure**
- **“Cybersecurity Gap”: a cost / incentive disconnect?**
  - Businesses will pay to meet business imperatives
  - Who’s going to pay to meet national security imperatives?

An Achilles Heel?

This level of dependence makes the Internet a target for **asymmetric attack**

Cyberwarfare

Cyberterrorism

Cyberhooliganism*

and a weak spot for **accidents and failures**

* Coined by Bruce Schneier, Counterpane

The Challenge

A solution to this problem will require both the right **technology** and the right **public policy**.

This is the cybersecurity challenge.

WHY SHOULD CYBER SECURITY BE YOUR TOP PRIORITY IN 2019

Cloud Control
www.c3m.io

Cybercrime damages to hit **$6 Trillion** by 2021

$ 117,000 average cost of a data breach for a small business in North America

$3.86 Million global average cost of a data breach

The overall global cost of cybercrime has exceeded **$600 Million**

71% of Americans say they worry about cybercrime

60 Million records breached due to misconfigured cloud

43% of security breaches occurred at small businesses

56% data breaches took more than a month to discover

2019 YEAR → 2022 YEAR

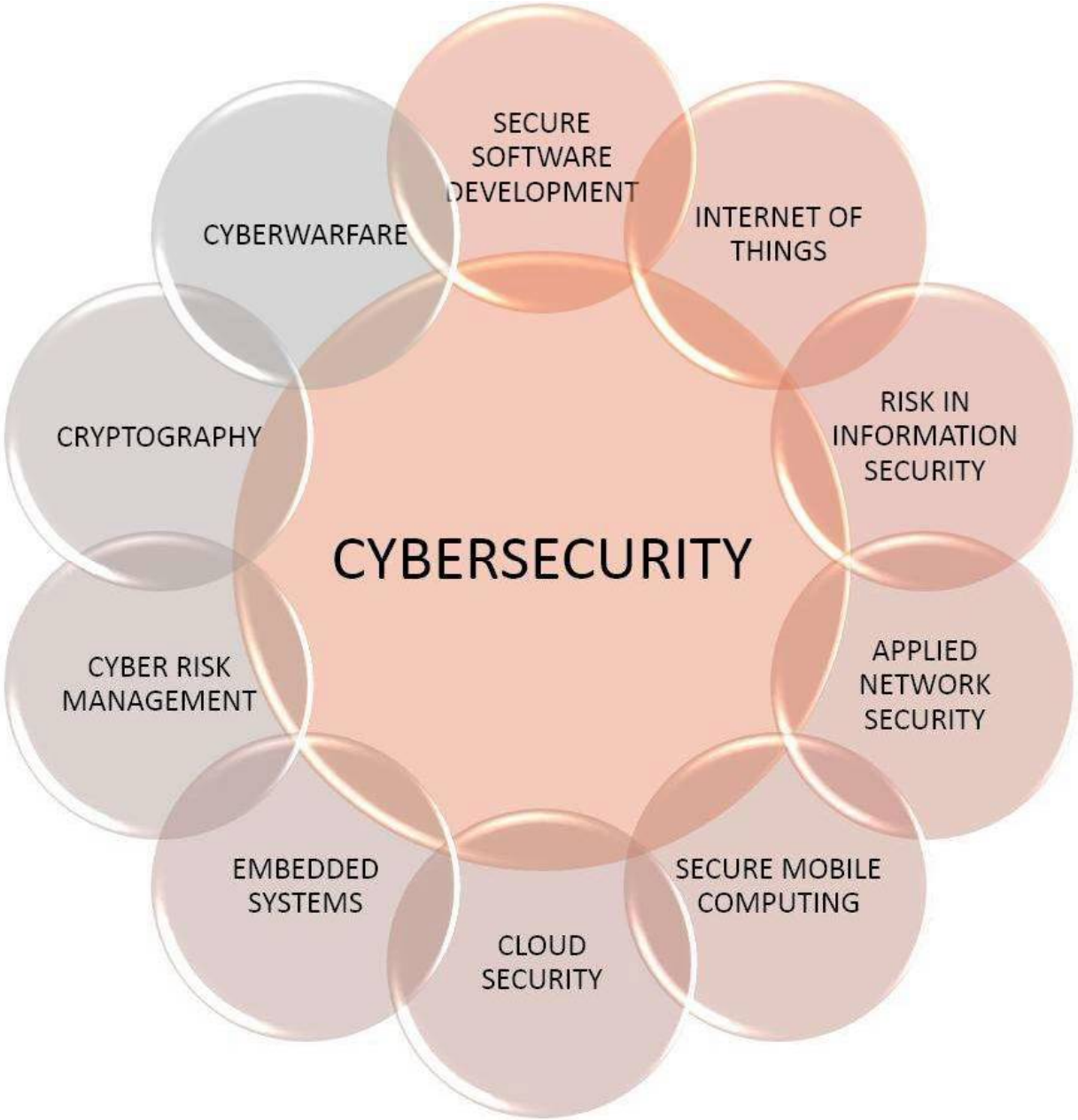
Through 2022, at least 95% of cloud security failures will be customers fault

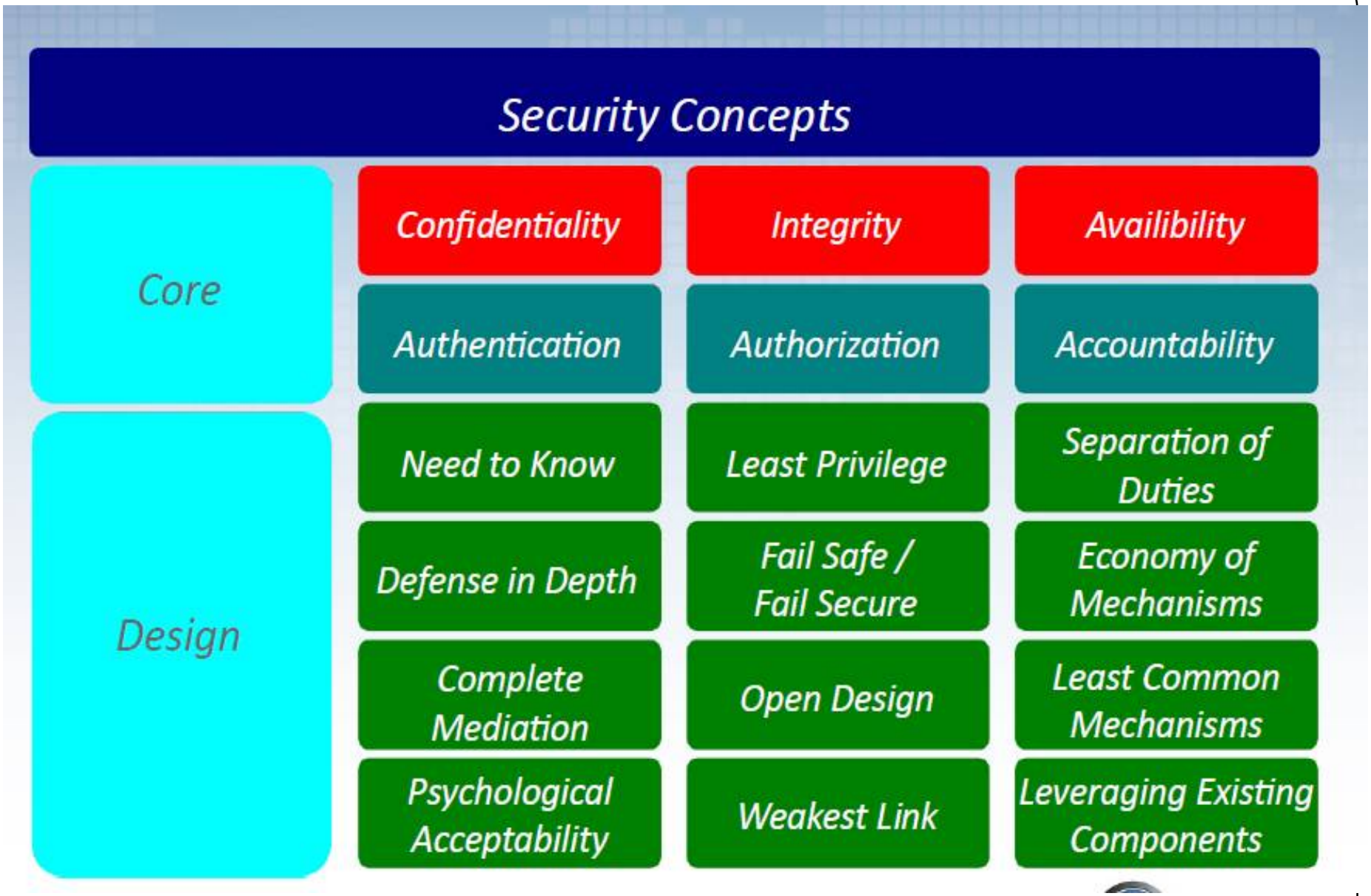
48% of UK businesses identified at least one breach or attack a month

1,903 breaches were reported in Q1 2019, exposing about 1.9 Billion records

74% of the breaches reported in Q1 2019 were a result of passwords being exposed to public

Source:
- Cybersecurity Ventures, Cisco, Ponemon, Verizon Data Breach Investigation Report, Risk Based Security's new study,
- Cyber Security Breaches Survey Department licensed under the Open Government Licence v3.0, Kaspersky Lab Report,
- 2019 Cost of a Data Breach Study, Ponemon.


CYBERSECURITY
SECURE SOFTWARE DEVELOPMENT
INTERNET OF THINGS
RISK IN INFORMATION SECURITY
APPLIED NETWORK SECURITY
SECURE MOBILE COMPUTING
CLOUD SECURITY
EMBEDDED SYSTEMS
CYBER RISK MANAGEMENT
CRYPTOGRAPHY
CYBERWARFARE


Security Concepts
Core
Design
Confidentiality
Integrity
Availibility
Authentication
Authorization
Accountability
Need to Know
Least Privilege
Separation of Duties
Defense in Depth
Fail Safe / Fail Secure
Economy of Mechanisms
Complete Mediation
Open Design
Least Common Mechanisms
Psychological Acceptability
Weakest Link
Leveraging Existing Components

One way to think about it

cybersecurity = availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

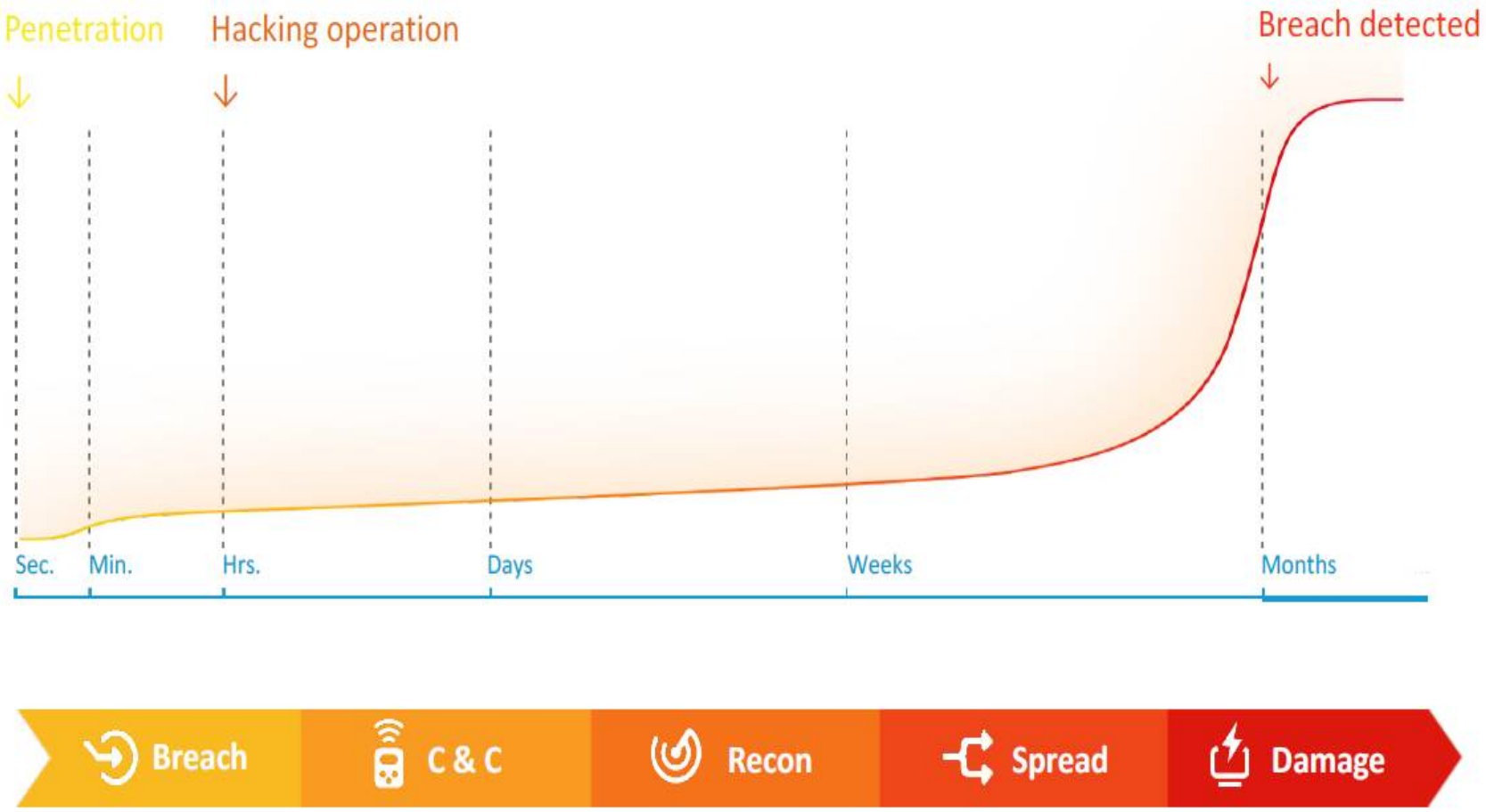
(Still a work in progress.)

In Context

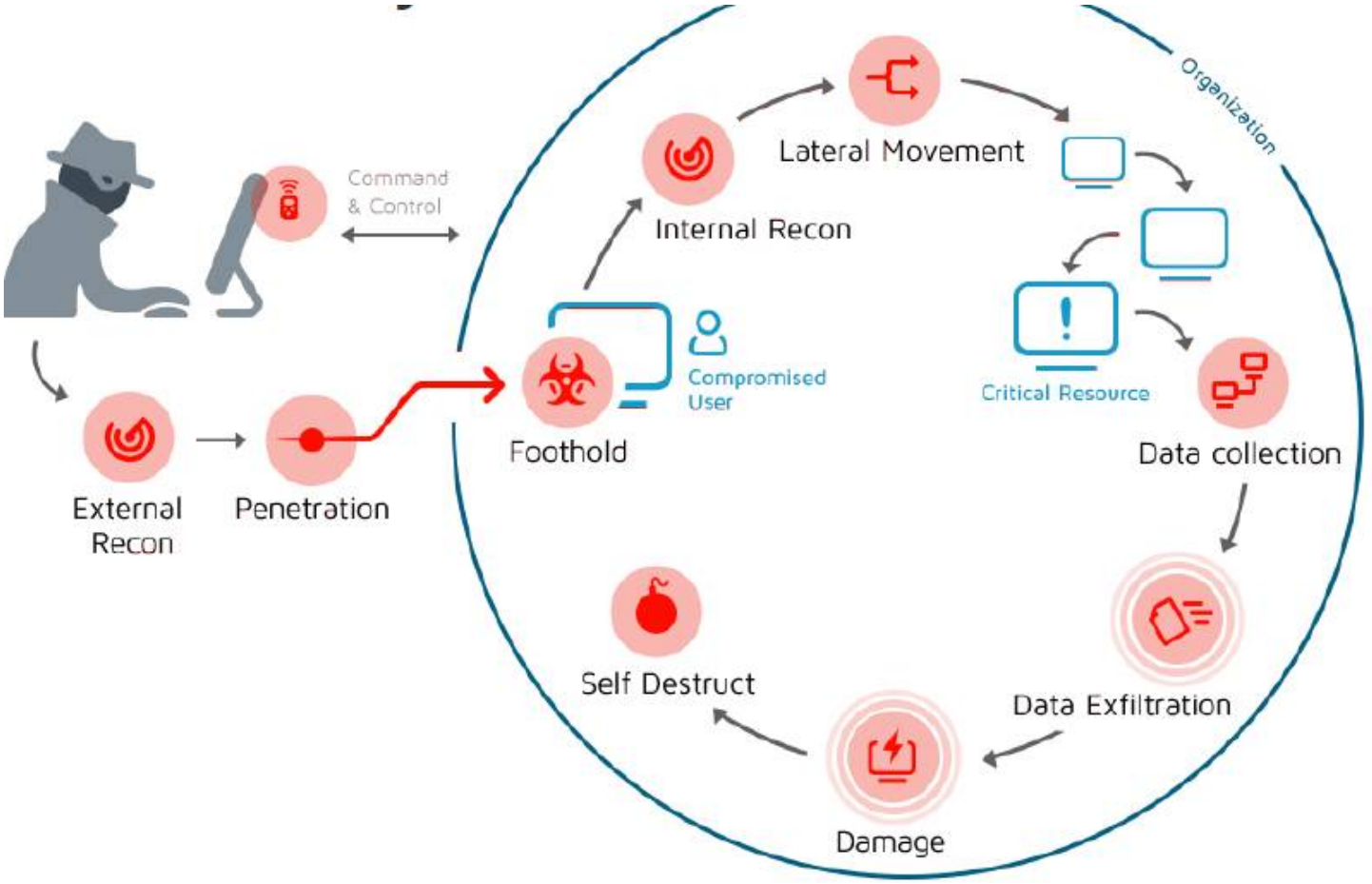
corporate cybersecurity = availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failures with the goal of protecting a corporation's operations and assets

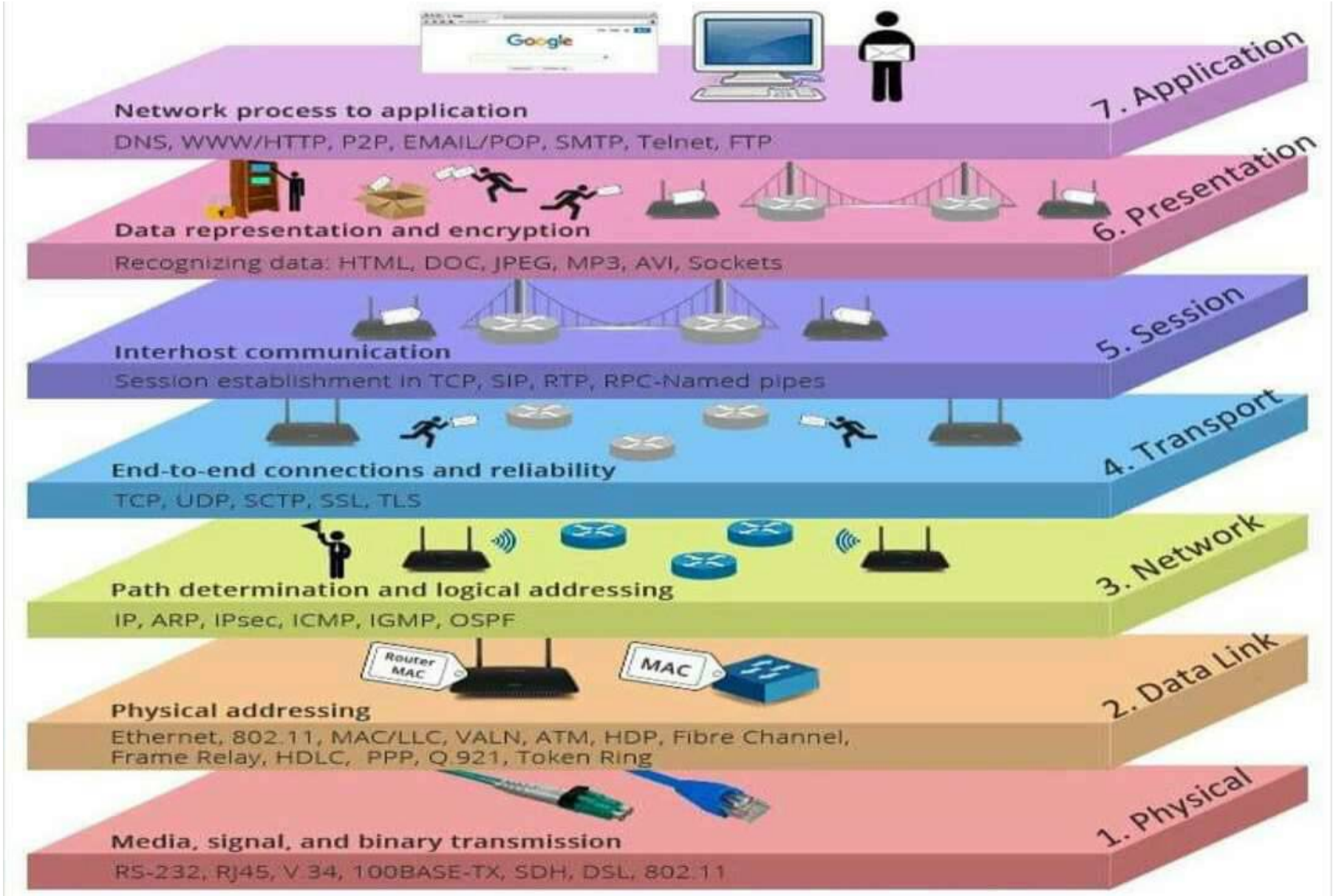
national cybersecurity = availability, integrity and secrecy of the information systems and networks in the face of attacks, accidents and failures with the goal of protecting a nation's operations and assets

The Attack (Full) Lifecycle

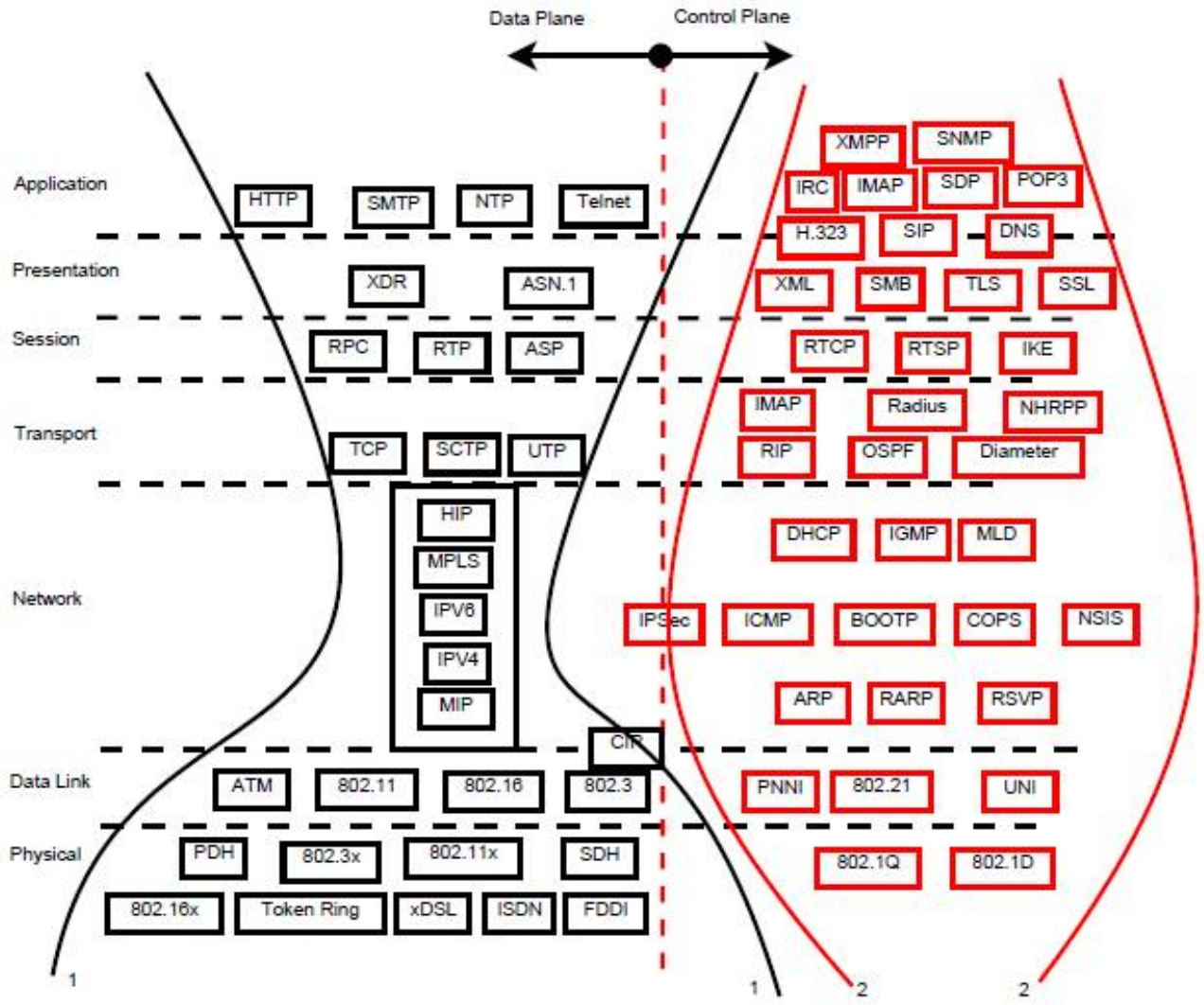


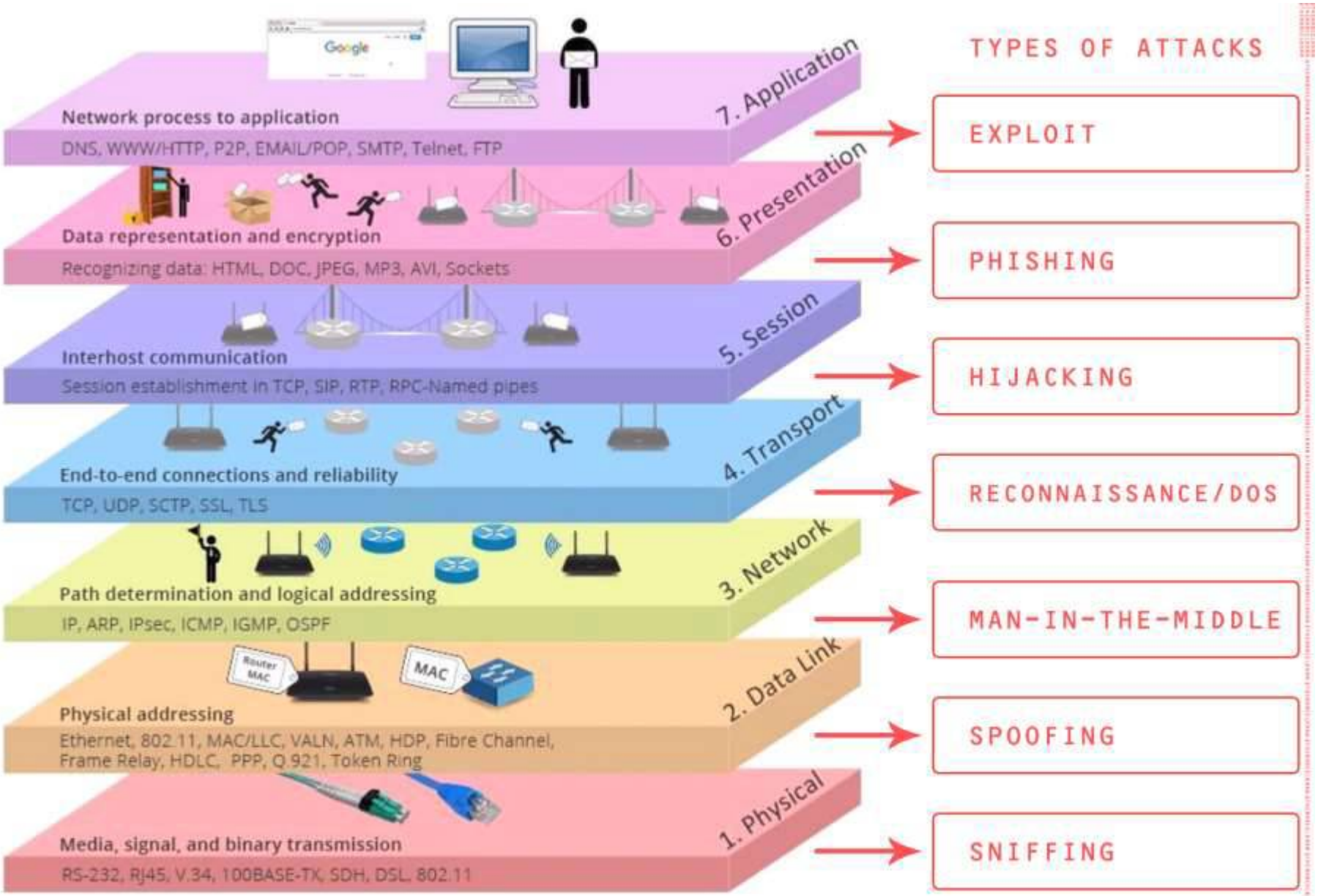
Attack Life cycle




Google
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
Router MAC
MAC
2. Data Link
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

Security protocols




TYPES OF ATTACKS
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
EXPLOIT
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
PHISHING
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
HIJACKING
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
RECONNAISSANCE/DOS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
MAN-IN-THE-MIDDLE
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
SPOOFING
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
SNIFFING

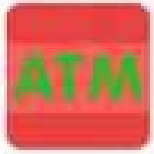
Challenges

- A number of trends illustrate why security is becoming increasingly difficult:
  - Speed of attacks
  - Sophistication of attacks
  - Faster detection of weaknesses
  - Distributed attacks
  - Difficulties of patching

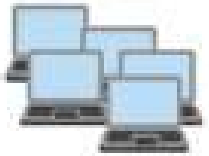
Threat Profiles

Trojans

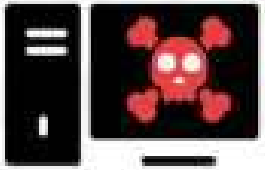
Android Malware



ATM Malware

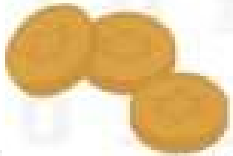


Botnets

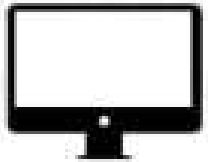


Ransomware

Point-of-Sale Malware

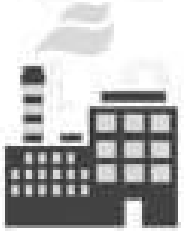


Cryptocurrency-Mining Malware



macOS Malware

iOS Malware



Industrial Control Systems Malware

Exploit Kits

Ransomware - Overview

1 WHAT IS RANSOMWARE?

- Ransomware is a type of malicious software that gains access to the victim's files or systems and blocks user access to them or releases the data for public download
- It uses different techniques but the most common is to encrypt the victim's files, making them inaccessible and demanding a ransom payment to decrypt them
- Recovering the files without the encryption key is an intractable problem (it would require huge resources and consequently is considered infeasible)

2 HOW DOES IT WORK?

1.- **Delivery Vectors:**
- Most ransomware is delivered via email (phishing emails with ransomware payloads) when the victim clicks a link or downloads an attachment that delivers the malicious software
- Other delivery mechanisms are drive-by-download attacks on compromised or malicious websites, bespoke Remote Desktop Protocol (RDP) attacks and social engineering leveraging social networks messaging
- Generic ransonware is rarely individually targeted

2.- **The Process:** most ransomware variants encrypt the files on the affected system, making them inaccessible and demanding a ransom payment using cryptocurrencies to make it difficult to trace and prosecute the perpetrators

BIGGEST ATTACKS

Although it was deemed one of the biggest malware threats of 2018, ransomware has been in decline over 2018 and 2019 (although infection decline does not match revenue earning). Bigger, better and more sophisticated strains are popping up. The most important ransomware attacks have been:

- **SamSam**
- **SimpleLocker**
- **WannaCry**
- **Cerber**
- **Ryuk**
- **TeslaCrypt**
- **NotPetya**
- **Katyusha**
- **PewCrypt**
- **LockerGoga**
- **Bad Rabbit**
- **Jigsaw**
- **GandCrab**
- **Dharma**

3

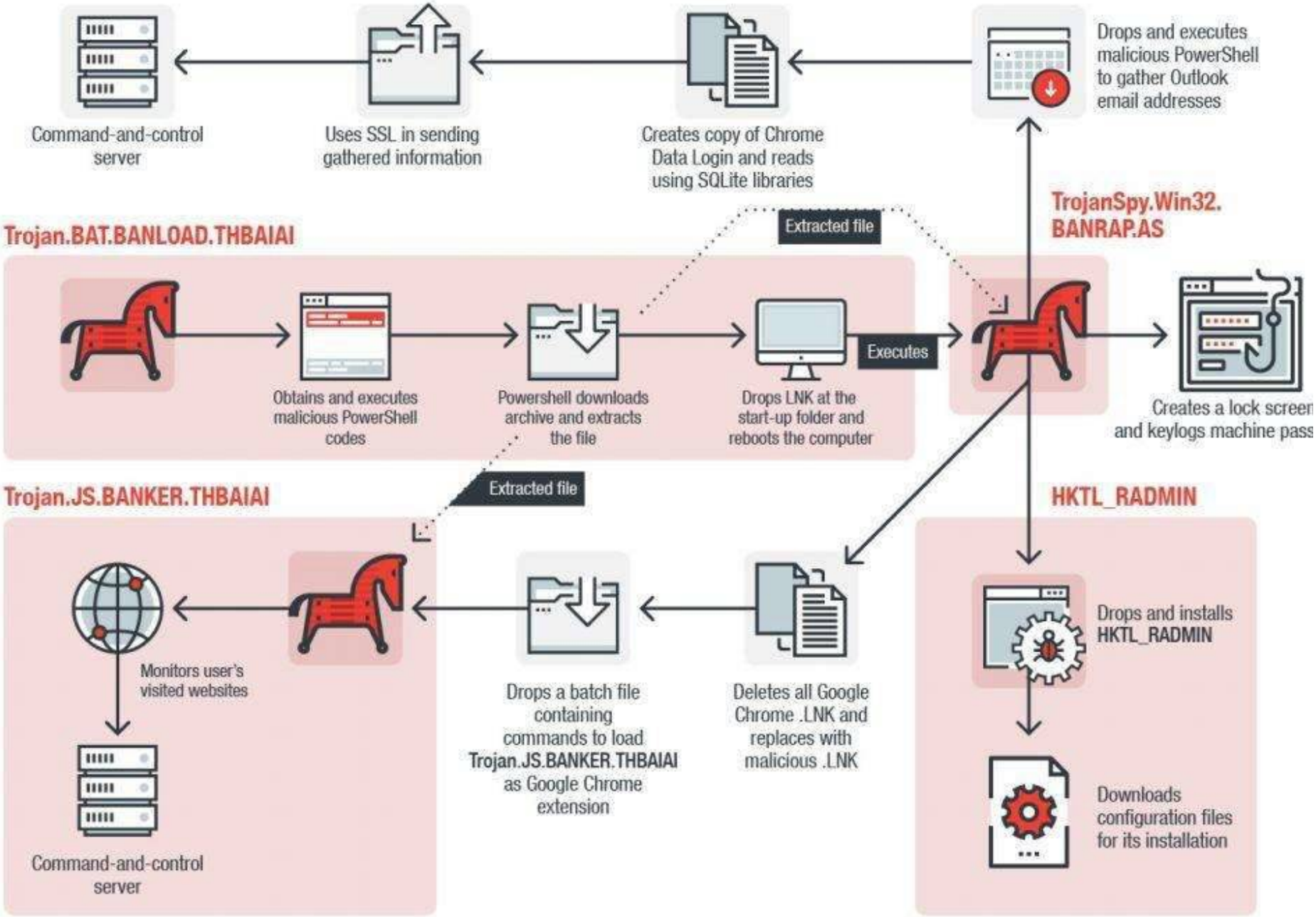
4 RANSOMWARE FACTS

- Over a quarter of cyber claims received in 2017 had ransomware as the primary cause of loss (AIG, 2018)
- The average ransom is dropping for small and medium-sized businesses but getting higher in the case of custom, targeted attacks
- Downtime is increasing and downtime costs are becoming substantial
- The healthcare industry is the most targeted, due to the sensitive information stored

5 PROTECTING AGAINST IT

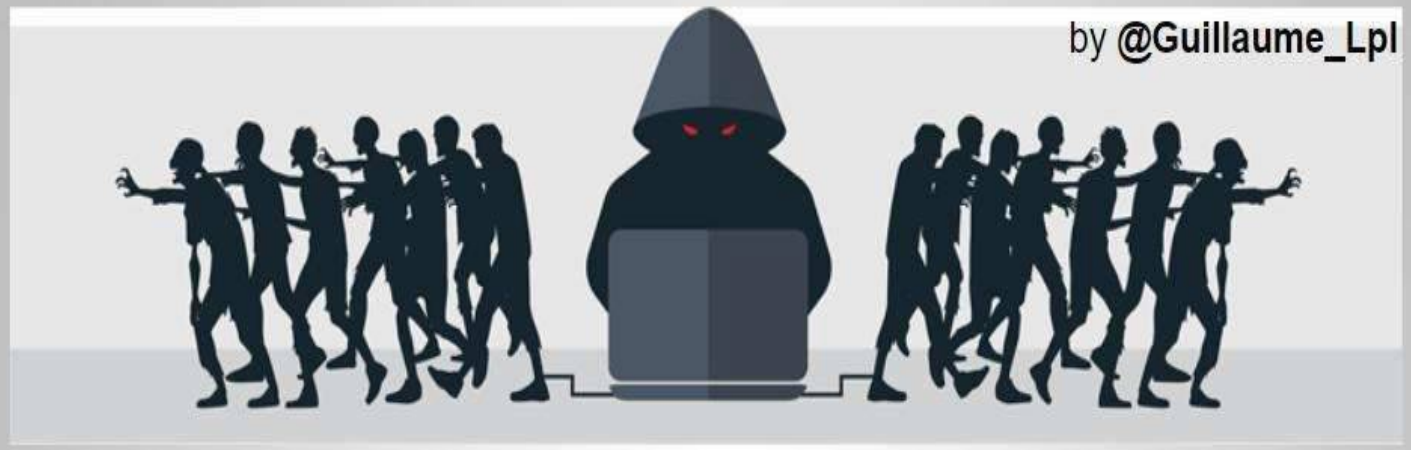
1.- **Reduce the risk of a ransomware attack:**
- Principle of Least Privilege: restrict users' permissions and conduct proper credential tracking
- Education and security awareness training
- Proper endpoint hygiene with proper configuration, regular updates and patches
- Leverage existing advanced threat prevention solutions to address all the delivery methods
- Up to date asset inventory and file integrity monitoring

2.- **Limit the fallout in case of attack:**
- Frequent and reliable backup and recovery
- Clear and regularly tested recovery plan
- Crisis management preparation, strategy and procedures


Command-and-control server
Uses SSL in sending gathered information
Creates copy of Chrome Data Login and reads using SQLite libraries
Drops and executes malicious PowerShell to gather Outlook email addresses
TrojanSpy.Win32. BANRAP.AS
Trojan.BAT.BANLOAD.THBAIAI
Extracted file
Obtains and executes malicious PowerShell codes
Powershell downloads archive and extracts the file
Drops LNK at the start-up folder and reboots the computer
Executes
Creates a lock screen and keylogs machine pass
Trojan.JS.BANKER.THBAIAI
Extracted file
HKTL_RADMIN
Monitors user's visited websites
Drops a batch file containing commands to load Trojan.JS.BANKER.THBAIAI as Google Chrome extension
Deletes all Google Chrome .LNK and replaces with malicious .LNK
Drops and installs HKTL_RADMIN
Downloads configuration files for its installation
Command-and-control server

What is a Botnet & How it works ? 1/2

by @Guillaume_Lpl



Definition :

♦ **Botnets** consist of a group of computers known as "**zombie**", computers that have been **compromised** and that can be **controlled** by attackers with malicious intent **whithout users knowing it**.

♦ Any **internet connected device is able to be infected** : Computers, Smartphones, IoTs (IP cameras, TV, routers, ...)

Some uses for a Botnets :

♦ Commit **advertising fraud**

♦ Steal your **private data**

♦ **DDoS** attack

♦ **CryptoCurrency** mining

♦ Send **spam emails**

♦ **Brute force** attack

Follow ***@Guillaume_Lpl*** for more

The most notorious Botnets :

♦ **Mirai** : he works by scanning the internet for IP add of **IoTs** devices.

- September 2016 attack on the **security blog of Bryan Krebs**. (DDoS attack)
- The October 2016 attack, where **Dyn DNS** was targeted : impact took **Twitter, Amazon, Netflix** ... (DDoS)

♦ **Zeus** : speards in the same way as Mirai.

- Zeus compromised **Bank of Ameriac, NASA, ABC, CISCO, Amazon** and others with **CyproLocker Ransomware spreading**

What is a Botnet & How it works ? 2/2

by @Guillaume_Lpl

1 Infection

♦ The botmaster sends out **malware** to **infect devices, by using social media, websites, emails, phising, ...**
♦ The mawlare will exploit **vulns** in your softwares, looking for **backdoor**..

Malware distribution

Infected machine

2 Connection

♦ Once in your device, the malware will use **your internet connection** to **make contact with the C2 server**, and **wait for his instructions**, without you knowing it.

Connects to 2C server

Attackers (Botmasters)

Sends orders

Command & Control (C2) Server

3 Control

♦ One the botmaster has a purpose for the botnet, he sends **instructions** to the bots **via the 2C server**.

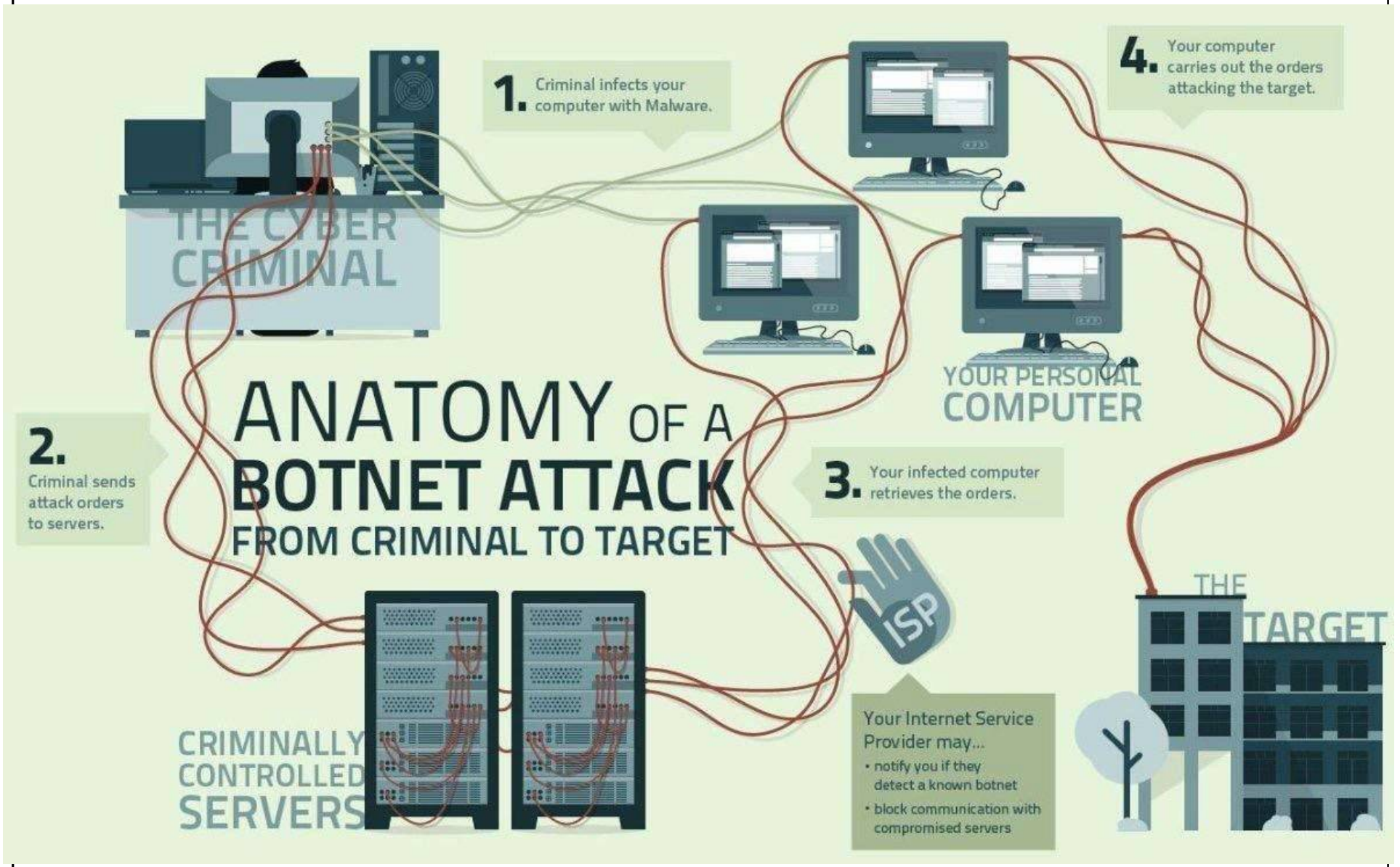
♦ Then the botnet starts carrying out malicious activities like **sending spam emails, DDoS attack...**

Botnet

4 Multiplication

♦ In the meantime, the botmaster will be focussed on **recruiting** more & more devices to **expand the botnet**
♦ As these devices don't appear to be doing anything, the botnet does **not attract intention**

Follow ***@Guillaume_Lpl*** for more


ANATOMY OF A
BOTNET ATTACK
FROM CRIMINAL TO TARGET
1. Criminal infects your computer with Malware.
2. Criminal sends attack orders to servers.
3. Your infected computer retrieves the orders.
4. Your computer carries out the orders attacking the target.
THE CYBER CRIMINAL
YOUR PERSONAL COMPUTER
CRIMINALLY CONTROLLED SERVERS
ISP
Your Internet Service Provider may...
• notify you if they detect a known botnet
• block communication with compromised servers
THE TARGET

What is Malvertising?

Malicious advertising ("malvertising") is a type of online attack wherein malicious code hidden within an online ad infects your computer with malware.

How Malvertising Works

You visit a website. It doesn't matter if the site is sketchy or legitimate -- the threat lies within the ads on the site.

Advertisements can come in a variety of shapes and sizes, though usually appear as banners or pop-ups.

Malvertising utilizes numerous tactics, such as using an iFrame, an invisible box that can secretly navigate to additional web pages.

The iFrame redirects to an "Exploit Landing Page."

The landing page is where malicious code attacks your system.

The attack code exploits your system and installs malicious software.

Malicious Bidding

Cyber Criminals are able to utilize malvertising by submitting booby-trapped advertisements to ad networks for a real-time bidding process.

After the ad wins the bid, it is propagated in real time through various publishers and will only trigger its malicious payload if specific conditions are met.

Hard to Catch

Malicious ads rotate in with normal ads. Therefore, when a user visits an infected site, they might not be attacked.

Because duplicating the infection is difficult, this can make it very hard for security researchers to study a malvertising attack.

Protection

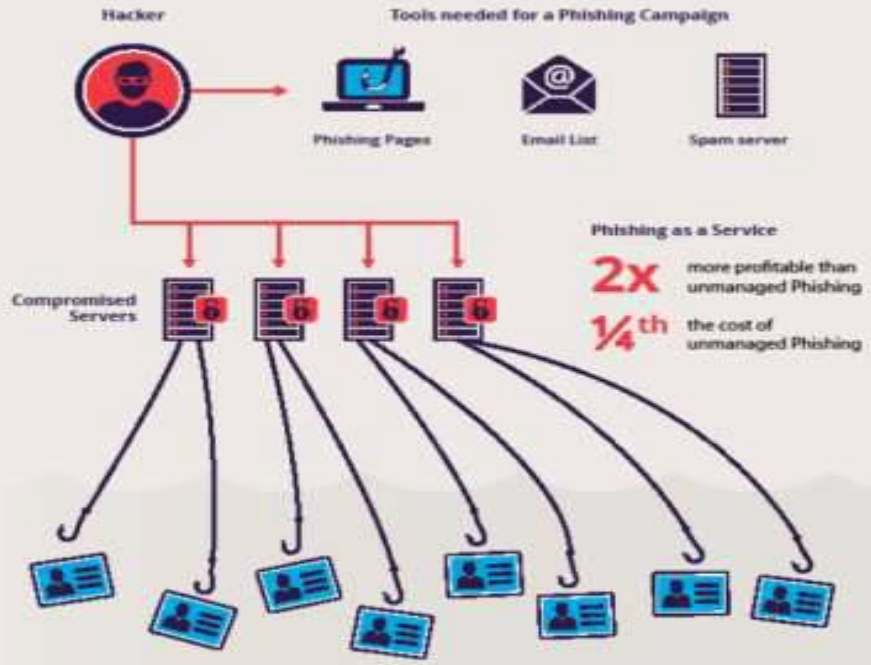
Using software like pop-up/ad blockers offers some protection against malvertising, but employing anti-exploit software in conjunction with an anti-malware is your best bet.

Learn more at www.malwarebytes.org.

Malwarebytes

PHISHING MADE EASY

Phishing is the starting point for most network and data breaches.



35% of all successful phishing attacks occur between 9am and 12pm

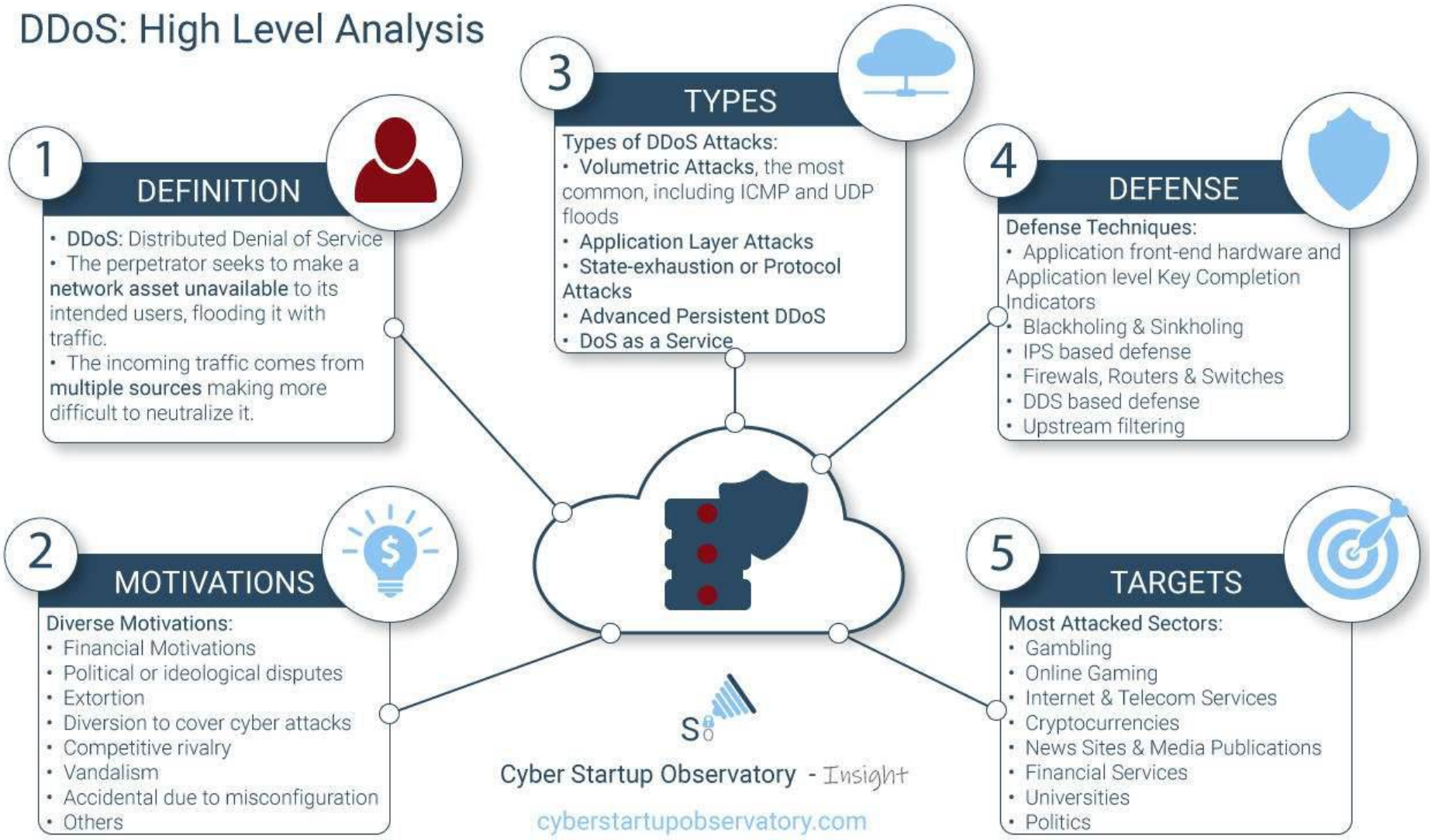
68% of accounts that were breached were not breached previously

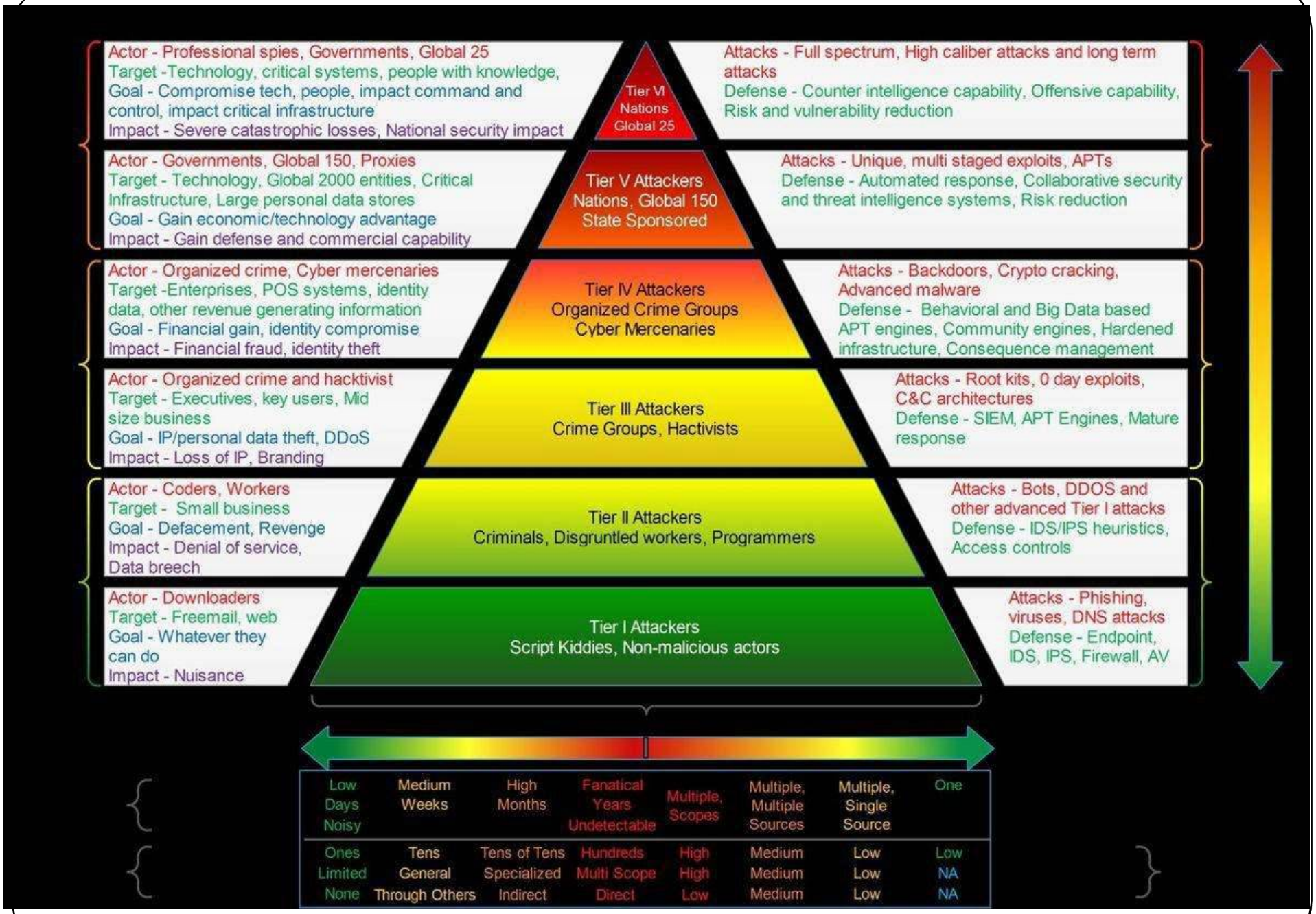
The best way to protect web servers from being compromised is to deploy web application firewalls (WAFs) that can detect and block advanced injection techniques. The phishing-based malware distribution mechanism relying on compromised servers can be contained only by increasing the security on web servers. If WAFs were deployed as ubiquitously as network firewalls, the cybercriminal industry would be seriously crippled.

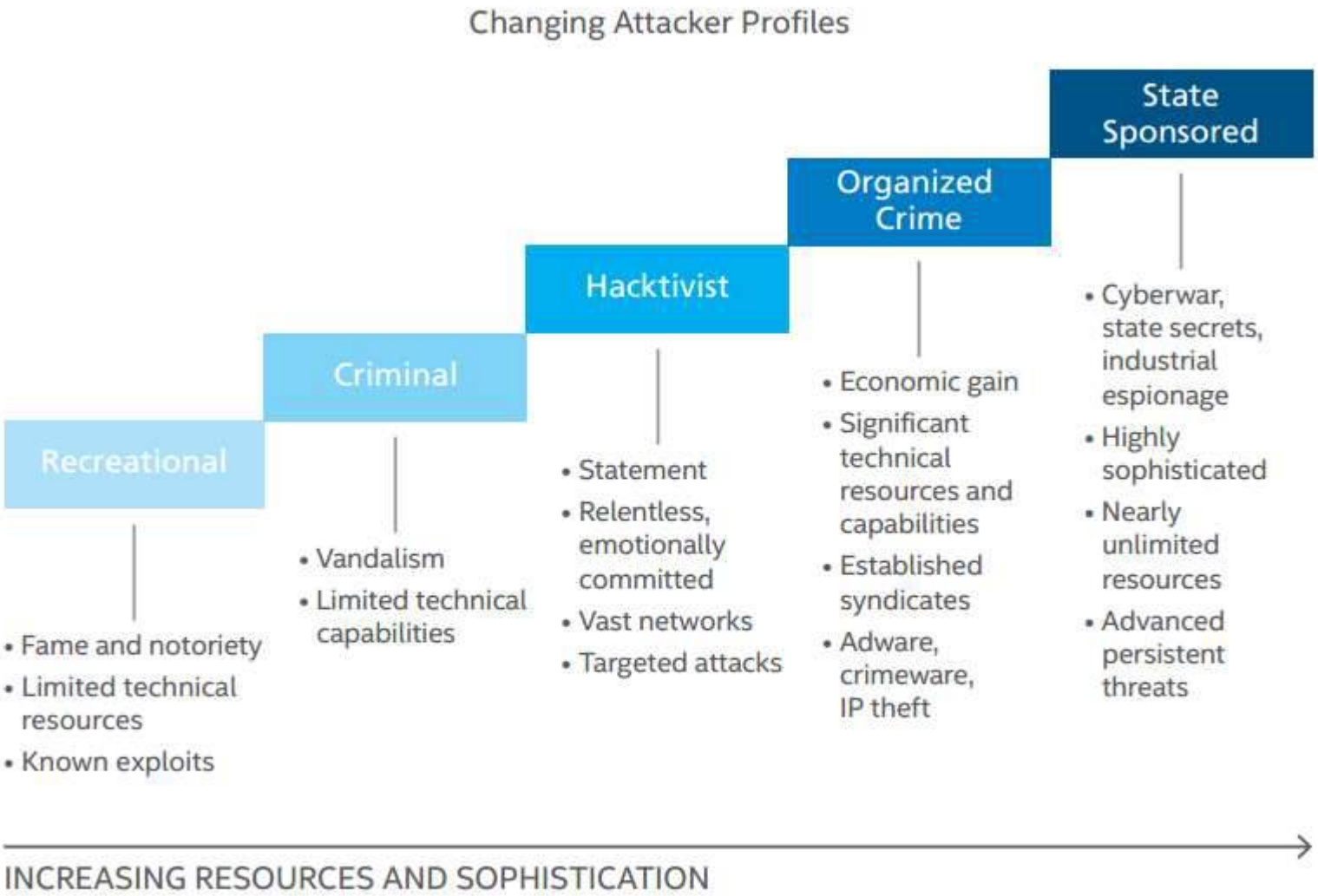
Read the full report and learn how you can protect yourself from Phishing attacks.

IMPERVA

DDoS: High Level Analysis




Actor - Professional spies, Governments, Global 25
Target -Technology, critical systems, people with knowledge,
Goal - Compromise tech, people, impact command and control, impact critical infrastructure
Impact - Severe catastrophic losses, National security impact
Tier VI Nations Global 25
Attacks - Full spectrum, High caliber attacks and long term attacks
Defense - Counter intelligence capability, Offensive capability, Risk and vulnerability reduction
Actor - Governments, Global 150, Proxies
Target - Technology, Global 2000 entities, Critical Infrastructure, Large personal data stores
Goal - Gain economic/technology advantage
Impact - Gain defense and commercial capability
Tier V Attackers Nations, Global 150 State Sponsored
Attacks - Unique, multi staged exploits, APTs
Defense - Automated response, Collaborative security and threat intelligence systems, Risk reduction
Actor - Organized crime, Cyber mercenaries
Target -Enterprises, POS systems, identity data, other revenue generating information
Goal - Financial gain, identity compromise
Impact - Financial fraud, identity theft
Tier IV Attackers Organized Crime Groups Cyber Mercenaries
Attacks - Backdoors, Crypto cracking, Advanced malware
Defense - Behavioral and Big Data based APT engines, Community engines, Hardened infrastructure, Consequence management
Actor - Organized crime and hacktivist
Target - Executives, key users, Mid size business
Goal - IP/personal data theft, DDoS
Impact - Loss of IP, Branding
Tier III Attackers Crime Groups, Hactivists
Attacks - Root kits, 0 day exploits, C&C architectures
Defense - SIEM, APT Engines, Mature response
Actor - Coders, Workers
Target - Small business
Goal - Defacement, Revenge
Impact - Denial of service, Data breech
Tier II Attackers Criminals, Disgruntled workers, Programmers
Attacks - Bots, DDOS and other advanced Tier I attacks
Defense - IDS/IPS heuristics, Access controls
Actor - Downloaders
Target - Freemail, web
Goal - Whatever they can do
Impact - Nuisance
Tier I Attackers Script Kiddies, Non-malicious actors
Attacks - Phishing, viruses, DNS attacks
Defense - Endpoint, IDS, IPS, Firewall, AV
Low Days Noisy
Medium Weeks
High Months
Fanatical Years Undetectable
Multiple, Scopes
Multiple, Multiple Sources
Multiple, Single Source
One
Ones Limited None
Tens General Through Others
Tens of Tens Specialized Indirect
Hundreds Multi Scope Direct
High High Low
Medium Medium Medium
Low Low Low
Low NA NA



The expansion of attacker types, their resources, and their sophistication.

Common Cyber Attacks:
Reducing The Impact

Most cyber attacks are composed of four stages: **Survey**, **Delivery**, **Breach** and **Affect**. The following **security controls**, applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

Who might be attacking you?

Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and **foreign intelligence services** interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

81%
OF LARGE COMPANIES REPORTING BREACH

£600K - £1.15m
AVERAGE COST OF SECURITY BREACH

Source: 2014 Information Security Breaches Survey sponsored by the Department for Business, Innovation and Skills.

User Education
Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

Controls For The Affect Stage
Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help. 10 Steps To Cyber Security outlines many of the features of a complete cyber risk management regime.

Patch Management
Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

Secure Configuration
Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

Monitoring
Monitor and analyse all network activity to identify any malicious or unusual activity.

User Access
Well maintained user access controls can restrict the applications, privileges and data that users can access.

Malware Protection
Malware protection within the internet gateway can detect malicious code in an imported item.

User Training
User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Network Perimeter Defences
Can block insecure or unnecessary services, or only allow permitted websites to be accessed.

Malware Protection
Can block malicious emails and prevent malware being downloaded from websites

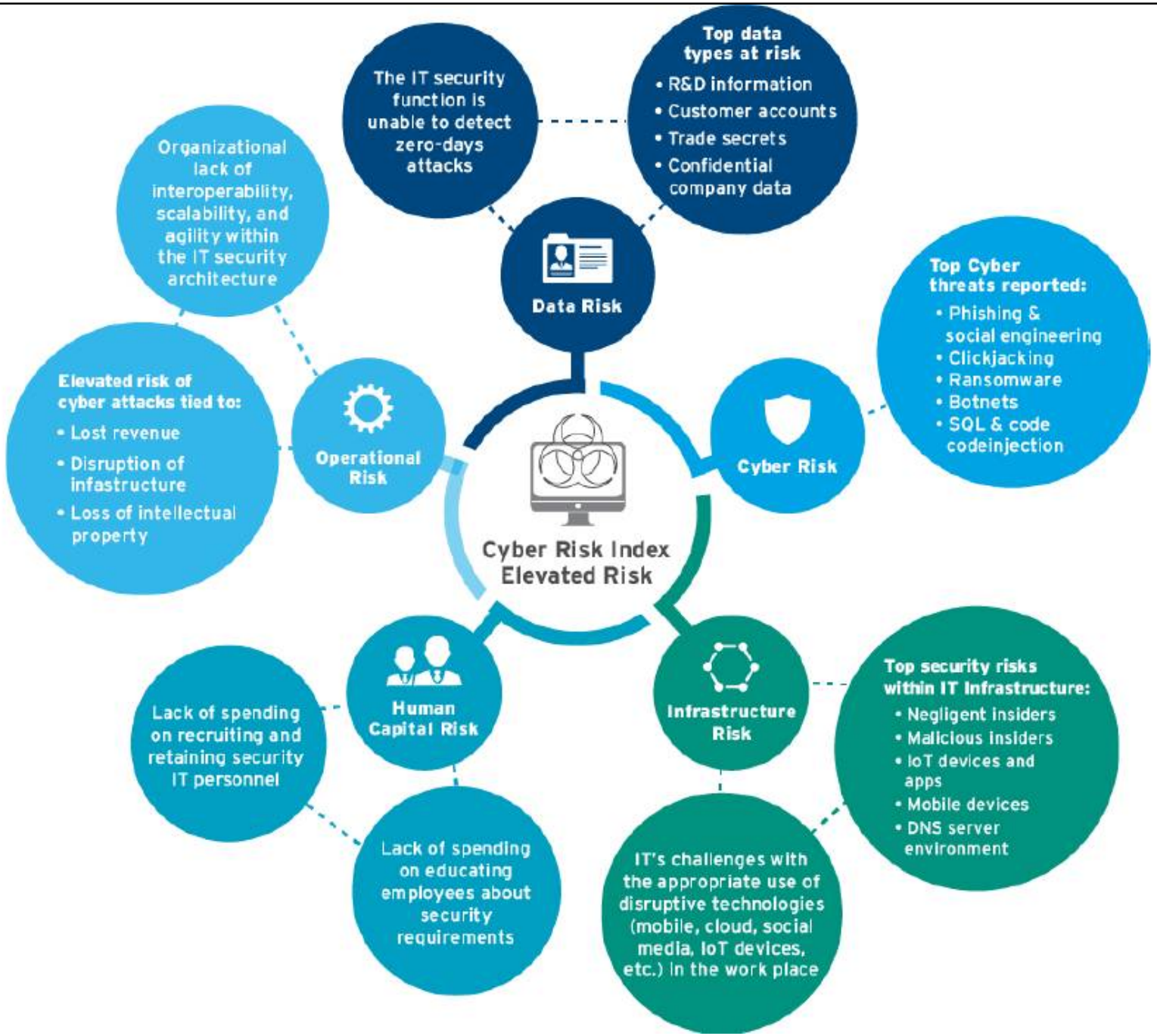
Password Policy
Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Device Controls
Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Secure Configuration
Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

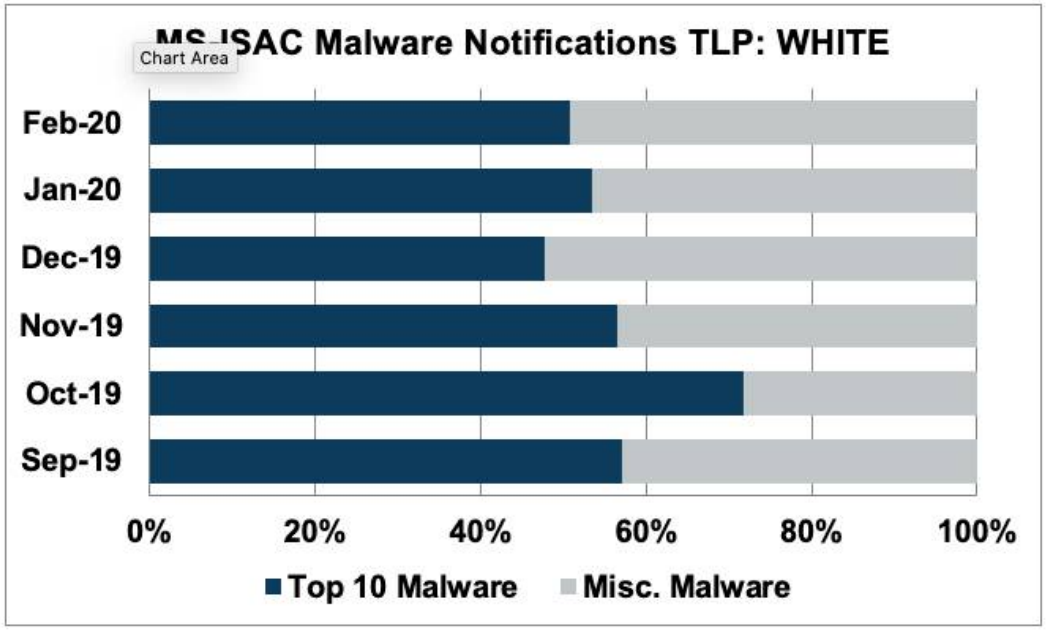
CESG

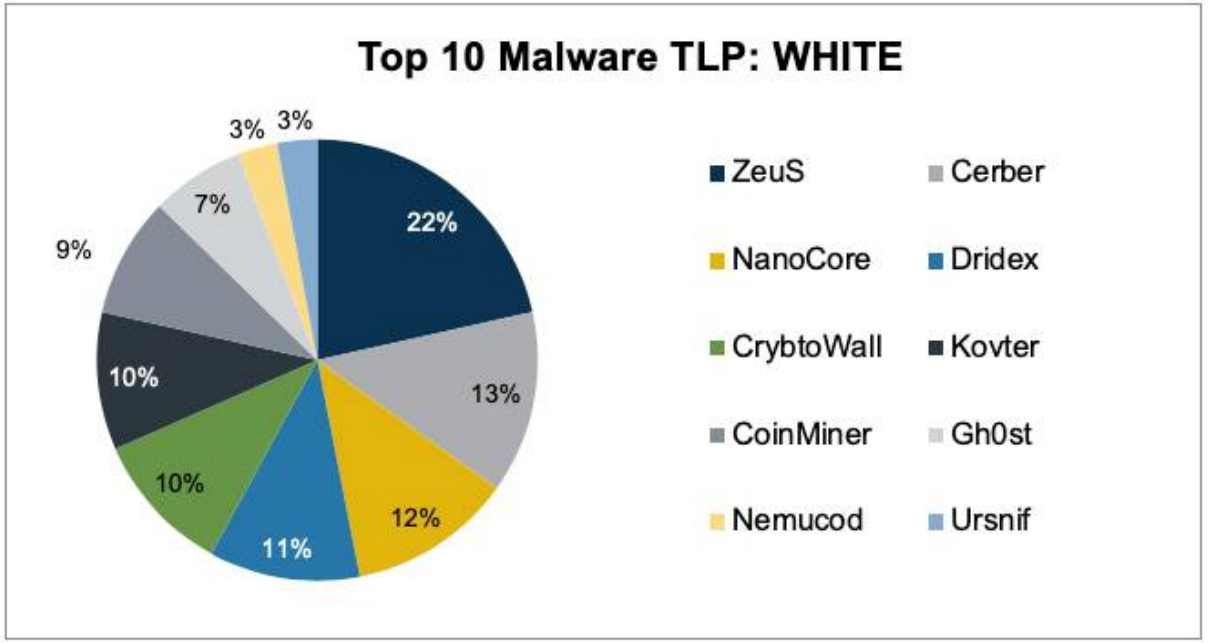
CERT-UK

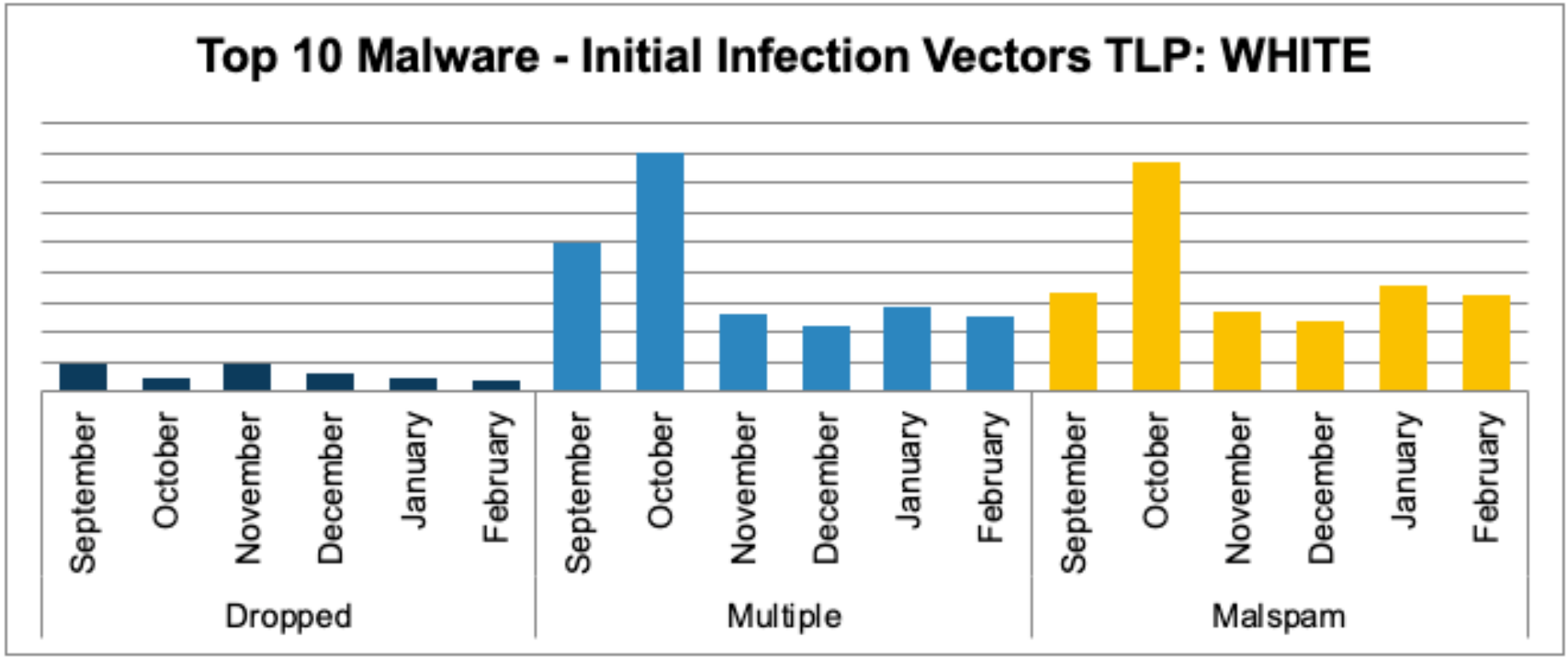

The IT security function is unable to detect zero-days attacks
Top data types at risk
• R&D information
• Customer accounts
• Trade secrets
• Confidential company data
Organizational lack of interoperability, scalability, and agility within the IT security architecture
Data Risk
Top Cyber threats reported:
• Phishing & social engineering
• Clickjacking
• Ransomware
• Botnets
• SQL & code codeinjection
Elevated risk of cyber attacks tied to:
• Lost revenue
• Disruption of infastructure
• Loss of intellectual property
Operational Risk
Cyber Risk
Cyber Risk Index
Elevated Risk
Lack of spending on recruiting and retaining security IT personnel
Human Capital Risk
Infrastructure Risk
Top security risks within IT Infrastructure:
• Negligent insiders
• Malicious insiders
• IoT devices and apps
• Mobile devices
• DNS server environment
Lack of spending on educating employees about security requirements
IT's challenges with the appropriate use of disruptive technologies (mobile, cloud, social media, IoT devices, etc.) in the work place

Top 10 Malware February 2020

- Top 10 Malware composition is very consistent with January 2020 with the exception of Ursnif.
- Nemucod remained, for the second month in a row, in the Top 10 despite remaining relatively quiet since 2017.
- This is likely to a lack of activity associated with more prominent malwares regularly seen on the list.
- Overall, the Top 10 Malware variants comprised 51% of Total Malware activity in February, down slightly from 53% in January.
- ZeuS and its variants continue to drive the number of infections to start out the new year.


MS-ISAC Malware Notifications TLP: WHITE
Chart Area
Feb-20
Jan-20
Dec-19
Nov-19
Oct-19
Sep-19
0%
20%
40%
60%
80%
100%
Top 10 Malware
Misc. Malware


Top 10 Malware TLP: WHITE
22%
13%
12%
11%
10%
10%
9%
7%
3%
3%
ZeuS
Cerber
NanoCore
Dridex
CrybtoWall
Kovter
CoinMiner
Gh0st
Nemucod
Ursnif


Top 10 Malware - Initial Infection Vectors TLP: WHITE
September
October
November
December
January
February
Dropped
September
October
November
December
January
February
Multiple
September
October
November
December
January
February
Malspam

- ***Dropped*** *– Malware delivered by other malware already on the system, an exploit kit, infected third-party software, or manually by a cyber threat actor.*
- ***Multiple*** *– Refers to malware that currently favors at least two vectors.*
- ***Malspam*** *– Unsolicited emails, which either direct users to download malware from malicious websites or trick the user into opening malware through an attachment.*
- ***Network*** *– Malware introduced through the abuse of legitimate network protocols or tools, such as SMB or remote PowerShell.*

- **ZeuS** is a modular banking trojan which uses keystroke logging to compromise victim credentials when the user visits a banking website. Since the release of the ZeuS source code in 2011, many other malware variants have adopted parts of it's codebase, which means that events classified as ZeuS may actually be other malware using parts of the ZeuS code.
- **Cerber** is an evasive ransomware that is capable of encrypting files in offline mode and is known for fully renaming files and appending them with a random extension. There are currently six versions of Cerber, which evolved specifically to evade detection by machine learning algorithms. Currently, version 1 is the only version of Cerber for which a decryptor tool is available.
- **NanoCore** is a Remote Access Trojan (RAT) spread via malspam as a malicious Excel XLS spreadsheet. As a RAT, NanoCore can accept commands to download and execute files, visit websites, and add registry keys for persistence.
- **Dridex** is a banking trojan that uses malicious macros in Microsoft Office with either malicious embedded links or attachments. Dridex is disseminated via malspam campaigns.
- **CryptoWall** is a ransomware commonly distributed through malspam with malicious ZIP attachments, Java Vulnerabilities, and malicious advertisements. Upon successful infection, CryptoWall will scan the system for drive letters, network shares, and removable drives. CryptoWall runs on both 32-bit and 64-bit systems.

- **Kovter** is a fileless click fraud malware and a downloader that evades detection by hiding in registry keys. Reporting indicates that Kovter can have backdoor capabilities and uses hooks within certain APIs for persistence.
- **CoinMiner** is a cryptocurrency miner that uses Windows Management Instrumentation (WMI) and EternalBlue to spread across a network. CoinMiner uses the WMI Standard Event Consumer scripting to execute scripts for persistence. CoinMiner spreads through malspam or is dropped by other malware.
- **Gh0st** is a RAT used to control infected endpoints. Gh0st is dropped by other malware to create a backdoor into a device that allows an attacker to fully control the infected device.
- **Nemucod** is a trojan that downloads additional malware onto an infected system. It is primarily spread via malspam and is known to drop ransomware such as Teslacrypt.
- **Ursnif**, and its variant Dreambot, are banking trojans known for weaponizing documents. Ursnif recently upgraded its web injection attacks to include TLS callbacks in order to obfuscate against anti-malware software. Ursnif collects victim information from login pages and web forms

Objectives of Security

- Security modules should be flexible and extendable and able to recover from possible attacks.
- Communication that takes place across the network must be free from attacks like eaves dropping, modification DOS etc.
- The architecture that is flexible and loosely coupled should be robust from attacks
- Architecture must able to recover from possible attacks
- Different architectures follow different security policies that are to be supported by the architecture.
- The basic services like authentication, confidentiality, trust, integrity etc are to be made available.
- According to the requirements of the user different levels of security has to be provided

Security Requirements

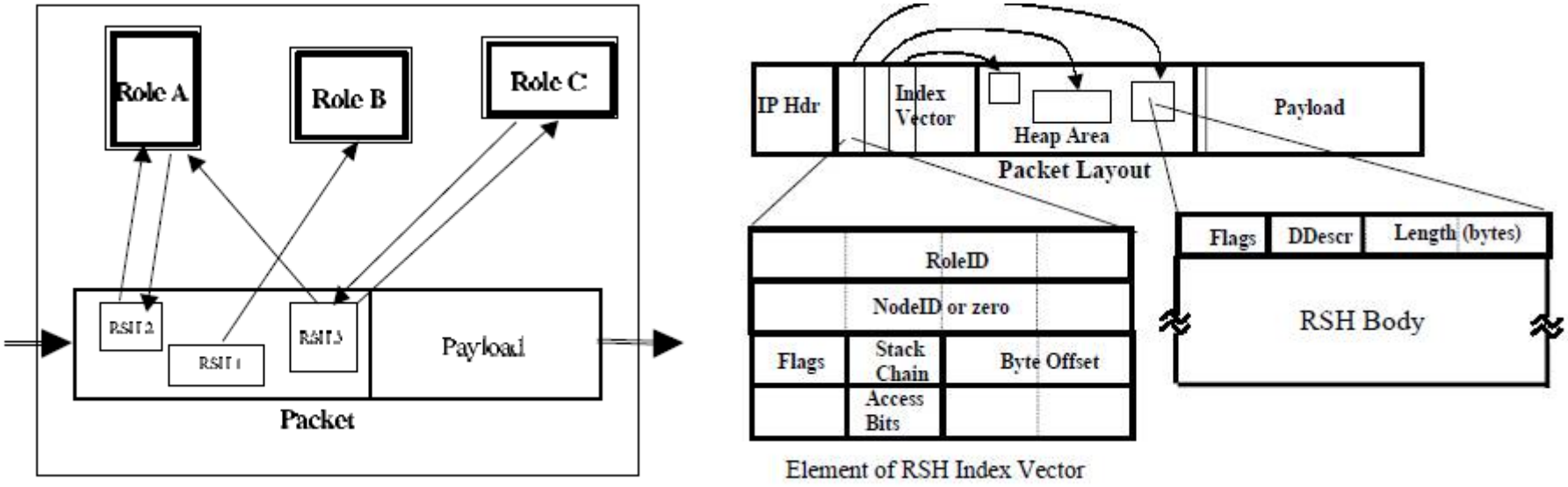
- Confidentiality
- Integrity
- Privacy
- Non-Repudiation
- ID Management
- Access Control
- Detection
- Recovery
- Security Management
- Authentication

Architecture-Approaches

- Clean State Approach--- Design from scratch
- Evolutionary Approach--- Search line by line and modify the protocol
- Re-engineering – ADD Extensions

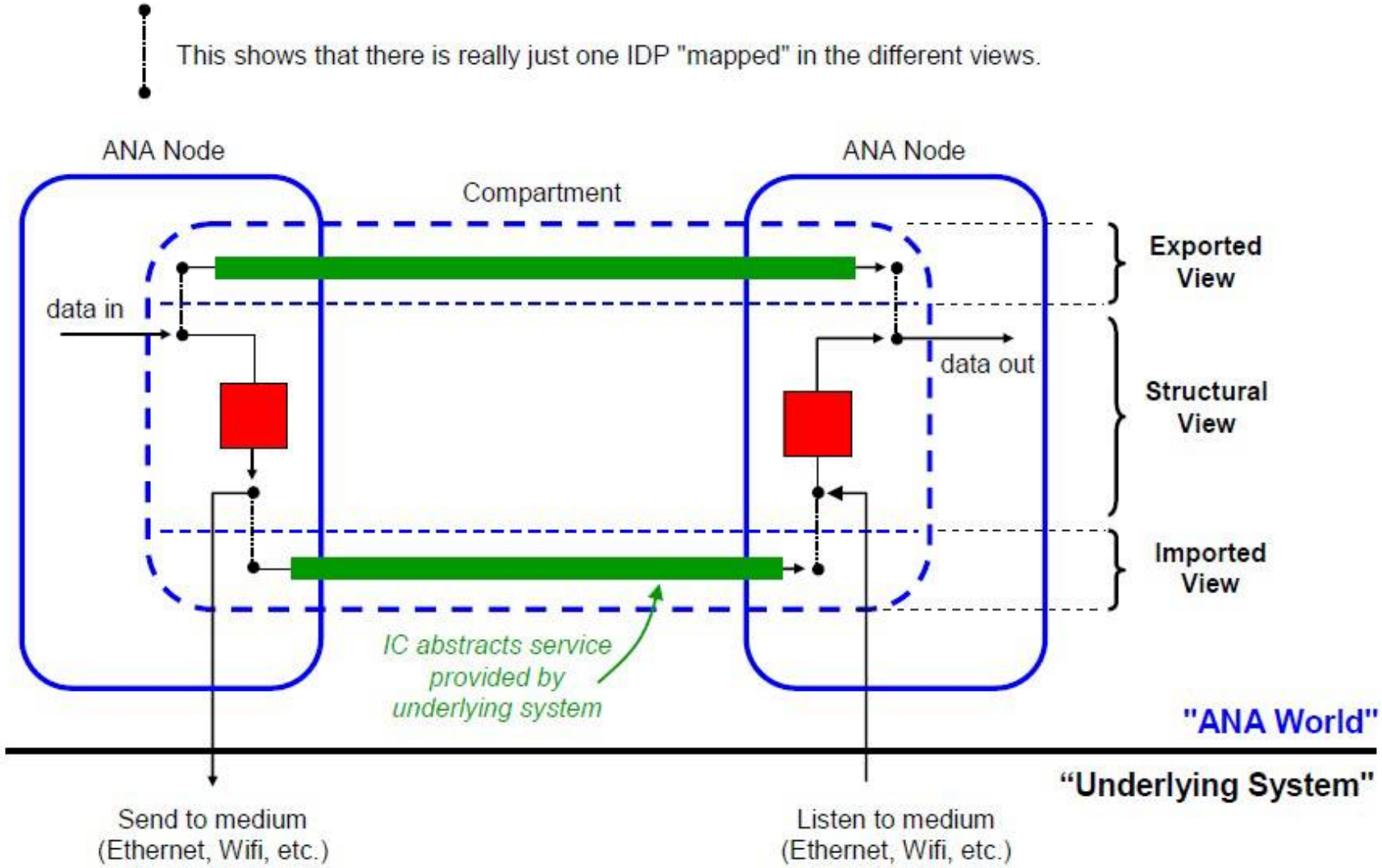
RBA: Role Based Architecture

- It follows heap instead of stack as followed by TCP/IP for the flow of information.
- Encryption and authentication are treated as one Role.
- Encapsulations reserved and has a special building block which takes care of forwarding and packet processing.


Role A
Role B
Role C
RSH 2
RSH 1
RSH 3
Payload
Packet
IP Hdr
Index Vector
Heap Area
Payload
Packet Layout
RoleID
NodeID or zero
Flags
Stack Chain
Byte Offset
Access Bits
Element of RSH Index Vector
Flags
DDescr
Length (bytes)
RSH Body

ANA: Autonomic Network Architecture

- Separation of mechanics from networking logic and it is an example of network meta architecture.
- It extracts and refracts core networking concepts to support heterogeneous addressing and naming of network nodes and networks
- system has got evolvability and dynamic reconfiguration capability


This shows that there is really just one IDP "mapped" in the different views.
ANA Node
ANA Node
Compartment
Exported View
data in
data out
Structural View
Imported View
IC abstracts service provided by underlying system
"ANA World"
"Underlying System"
Send to medium (Ethernet, Wifi, etc.)
Listen to medium (Ethernet, Wifi, etc.)

RNA: Recursive Network Architecture

- This is a new approach developed based on the combination of the above mentioned two methods
- Uses dynamic service composition, cleaner cross-layer interaction, and the impact of layers of architecture

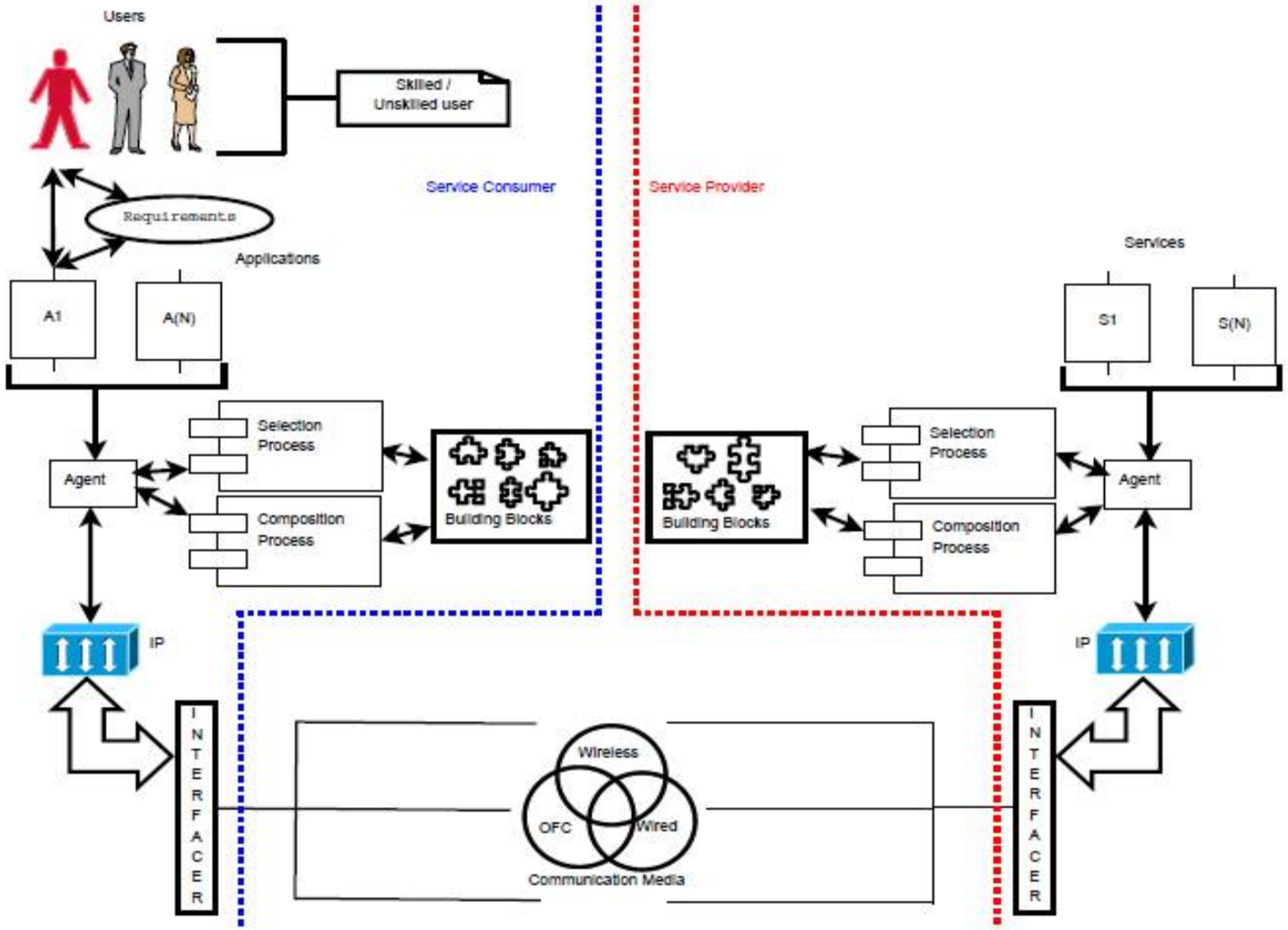
GENI: Global Environment for Network Innovations /FIND: Future Internet Design

- One of the major project of the US National Science Foundation is GENI
- Aiming to design, development and implementation of a realistic, large scale, open experimental facility for the evaluation of new network architectures, services and applications.

PONA: Policy Oriented Naming Architecture

- It envisions the next generation Internet to be dynamic, secure, heterogeneous, flexible to support innovations and implementation of policies at the end and core of the system
- This architecture uses advanced mechanisms of security like biometrics, larger key size, tokens

SONATE: Service Oriented Network Architecture



RINA: Recursive Inter Network Architecture

- It is secure and resistant to the attacks like port scanning, data transfer and connection opening.
- It focused on developing the security modules for access control, data transfer etc. to overcome the vulnerabilities.
- It decouples various functions of security like authentication, confidentiality and integrity

ChoiceNet

- The three principles of the architecture for performing the functionalities are ***Encourage alternatives,Vote with your wallet and Know what happened***

- ***Other Architectures are AKARAI,*** **Future Internet Assembly (FIA) of the European Union, Future Internet Design (FIND), NetSE & GENI of the United States, Future Internet Forum (FIF) of Korea**

The Internet is Hard to Secure

- **Extreme complexity, minimal understanding**
- **High global connectivity**
- **Weak attribution (who's doing what?)**
- **Hard to tell malicious uses from legitimate ones**

THANK YOU