How to combat Emerging Cyber-Threats

Alexandros Kaniklides,
akaniklides@odysseyc.com
IthacaLabs© Lead Researcher

ODYSSEY Cyber Security
Impossible Challenges, Possible Solutions!

Agenda

1 About Odyssey

2 Cyber-Crime & Motivations

3 Emerging Cyber-Threats

4 Combat: A Multidimensional Process

5 Conclusion

About Odyssey

Founded in 2002

With the main objective to provide "**High-Quality, Cutting-Edge, Information Security, Infrastructure and Risk Management Services**" to Organizations that value their Information Assets.

Regional Leader

In the provision of **cyber security solutions and services**, helping organizations in effectively and efficiently managing information security risk.

Offices in 4 countries

In **Cyprus, Greece, Serbia and Dubai** employing 88 people and delivering our services through multiple strategically located security operation centers.

Certifications

Certified with **ISO 27001** and accredited by the Payment Card Industry Security Standards Council (PCI SSC) as a **Qualified Security Assessor (QSA)** and an **Approved Scanning Vendor (ASV)**

Cyber-Crime & Motivations

Low Cost, Low Risk with High Returns

Cyber-Crime produces high returns at low risk and (relatively) low cost for the Cyber-Criminals.

- The rate of return on Cyber-Crime favors Cyber-Criminals; the incentive is to steal more
- The most common **"Surprisingly Cheap"** exploitation techniques are:
  - Social Engineering &
  - Vulnerability Exploitation

Cyber-Crime & Motivations

Who are these Cyber-Criminals?

Today's Cyber-Criminals are:

- Well organized,
- Well funded,
- Highly skilled &
- Have access to sophisticated tools

Cyber-Crime & Motivations

Type of Cyber-Attacks?

While you're watching this presentation, Cyber-Criminals are trying to circumvent your **Organization's** security defenses in order to conduct:

- Industrial Espionage,
- Undermine Business and Financial Operations,
- Extortions,
- Sabotage normal business operations and
- Steal Sensitive Information.

ODYSSEY Cyber Security
Impossible Challenges, Possible Solutions!

Cyber-Crime & Motivations

Who do hackers targets?

- Financial Institutions, Retailers, Utility Companies & Governments are the main target of these Cyber-Attacks
- ANY other type or size of an organization with ANY valuable INFORMATION is a TARGET as well.
- So the perception that Cyber-Criminals are targeting only big organizations is a **MYTH**.

We are ALL targets....

ODYSSEY Cyber Security
Impossible Challenges, Possible Solutions!

Cyber-Crime & Motivations

Who do hackers targets?

- Contractors – 40%.
- IT Administrators – 30%.
- Non-executive Employees – 16%.
- Executive Administrators – 8%.
- Executives – 6%.

Source: Thycotic Black Hat 2014 Survey

Cyber-Crime & Motivations

Cost of Cyber-Attacks to organizations

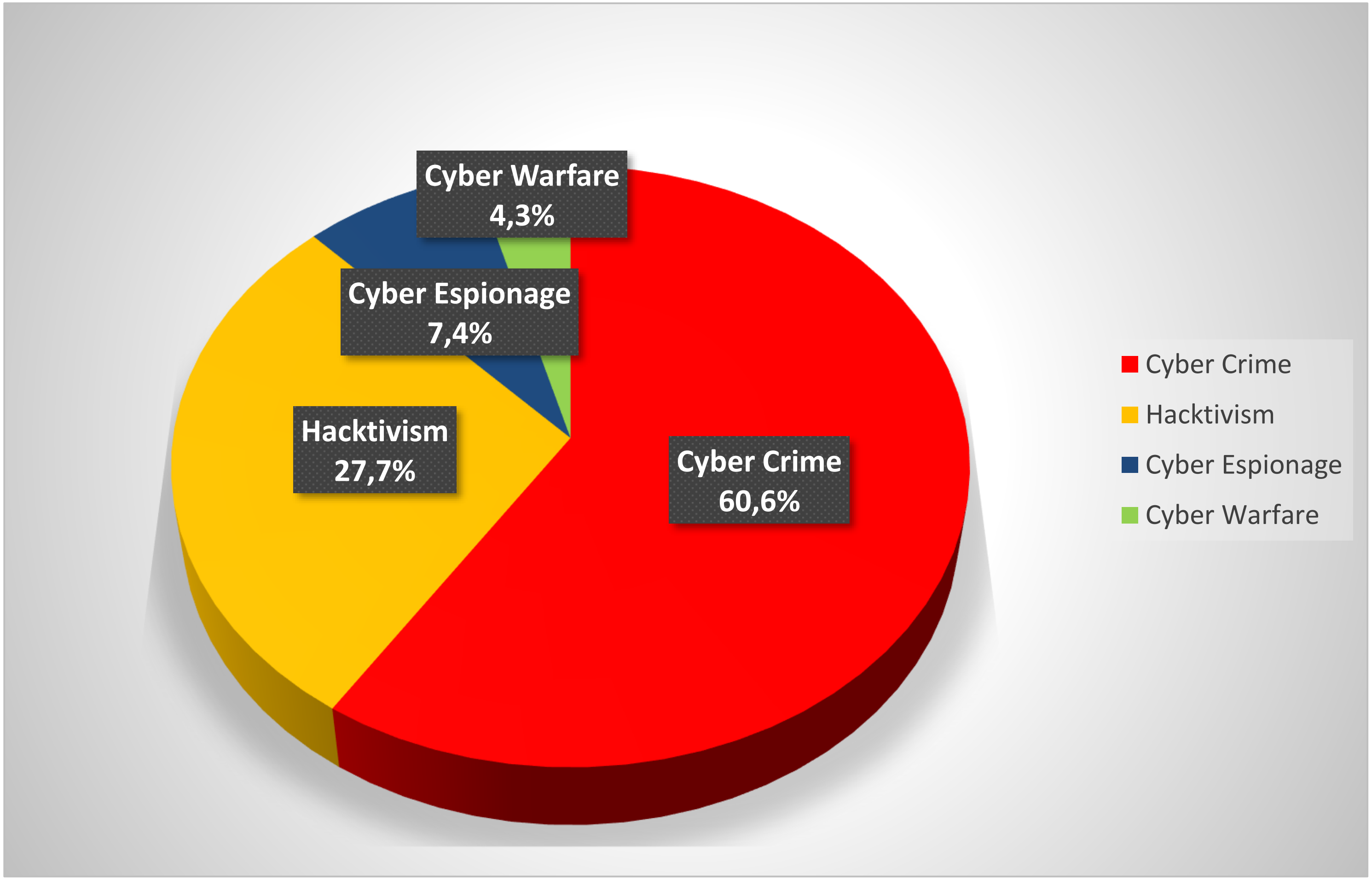
- The likely annual cost to the global economy from Cyber-Crime cost organizations more than **$400 billion** in 2015.

- From 2013 to 2015 the Cyber-Crime costs quadrupled, and it looks like there will be another quadrupling from **2015 to 2019** to **$2.1 trillion** by 2019.

Source: British insurance company Lloyd's, 2015, Juniper research

Cyber-Crime & Motivations

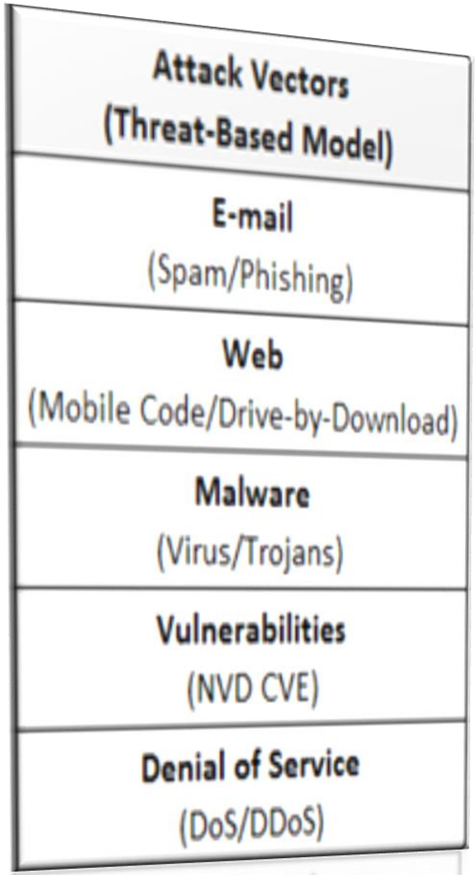
Type of Cyber-Attacks - January 2016



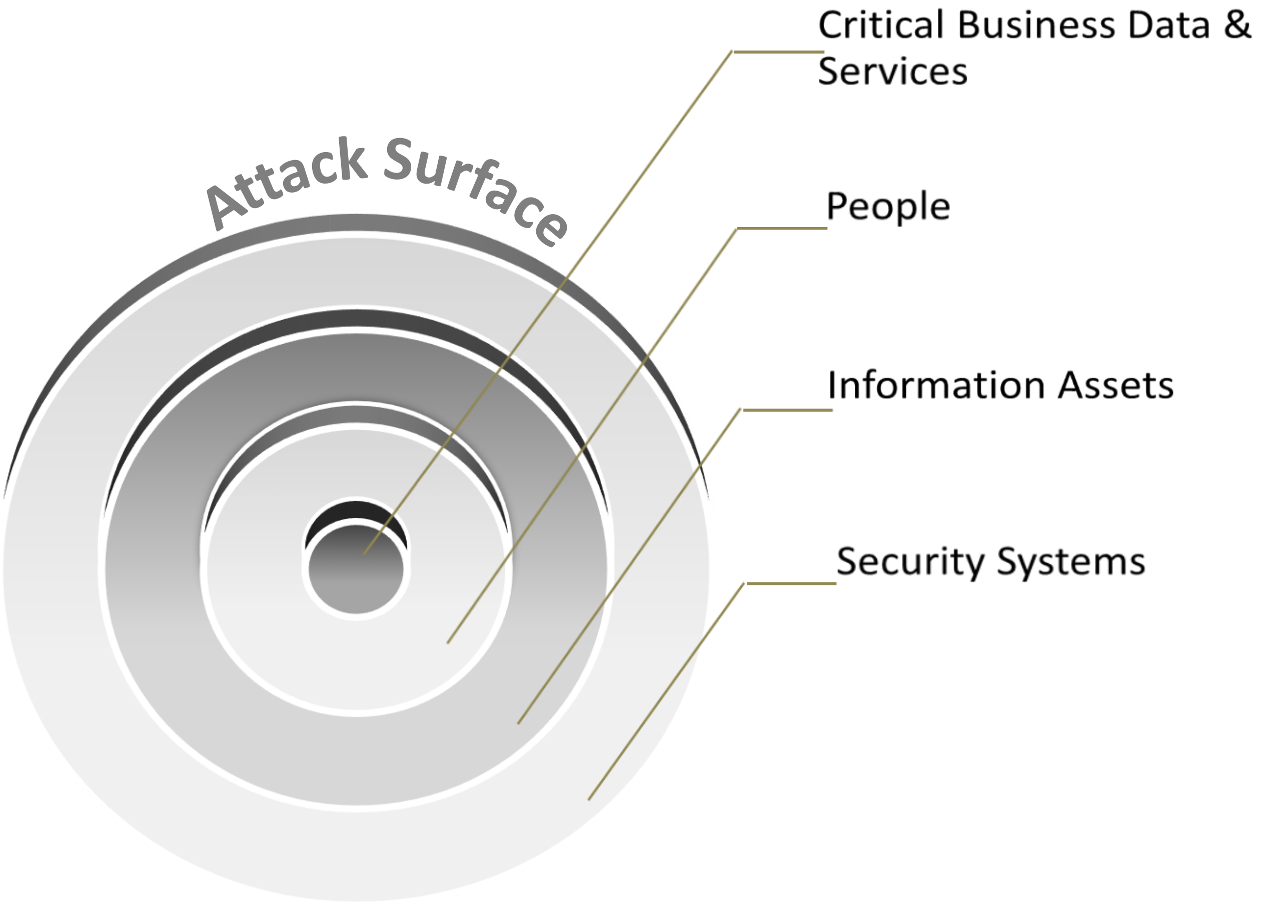
Source: Hackmageddon, Information Security Timelines & Statistics

Emerging Cyber-Threats

Cyber-Threats Landscape



Attack Vectors (Threat-Based Model)
E-mail (Spam/Phishing)
Web (Mobile Code/Drive-by-Download)
Malware (Virus/Trojans)
Vulnerabilities (NVD CVE)
Denial of Service (DoS/DDoS)



Emerging Cyber-Threats

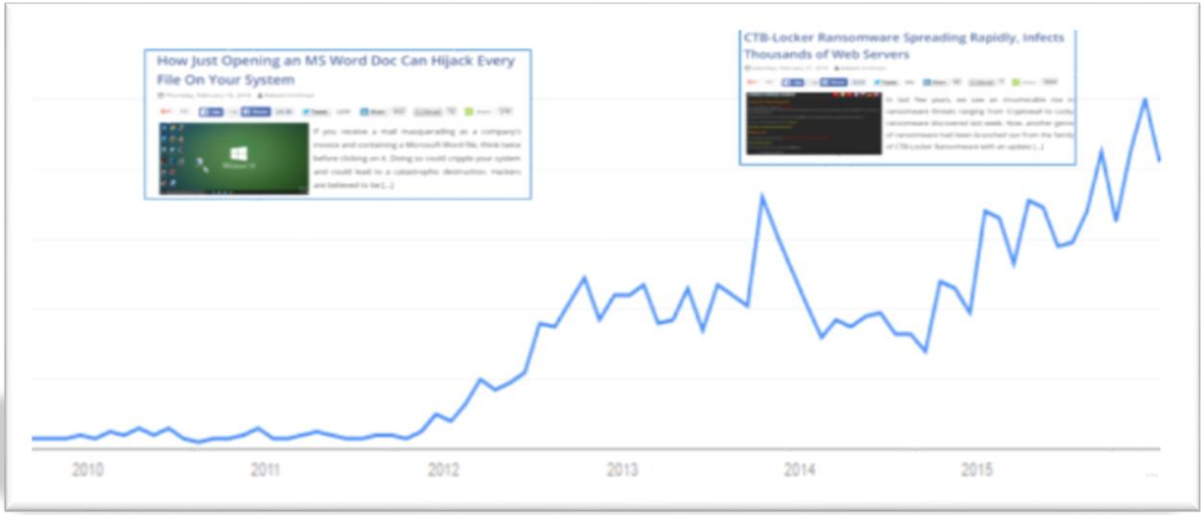
Rise of Ransomware:

- Email-born: Social Engineering, Spear Phishing, ExploitKits (Angler, Blackhole).
- Web-born: Drive-by download attacks (malvertising).

News headline:

"Hollywood hospital pays hackers $17,000 ransom to restore computers"

Interest over Time: "**Ransomware**"



How Just Opening an MS Word Doc Can Hijack Every File On Your System

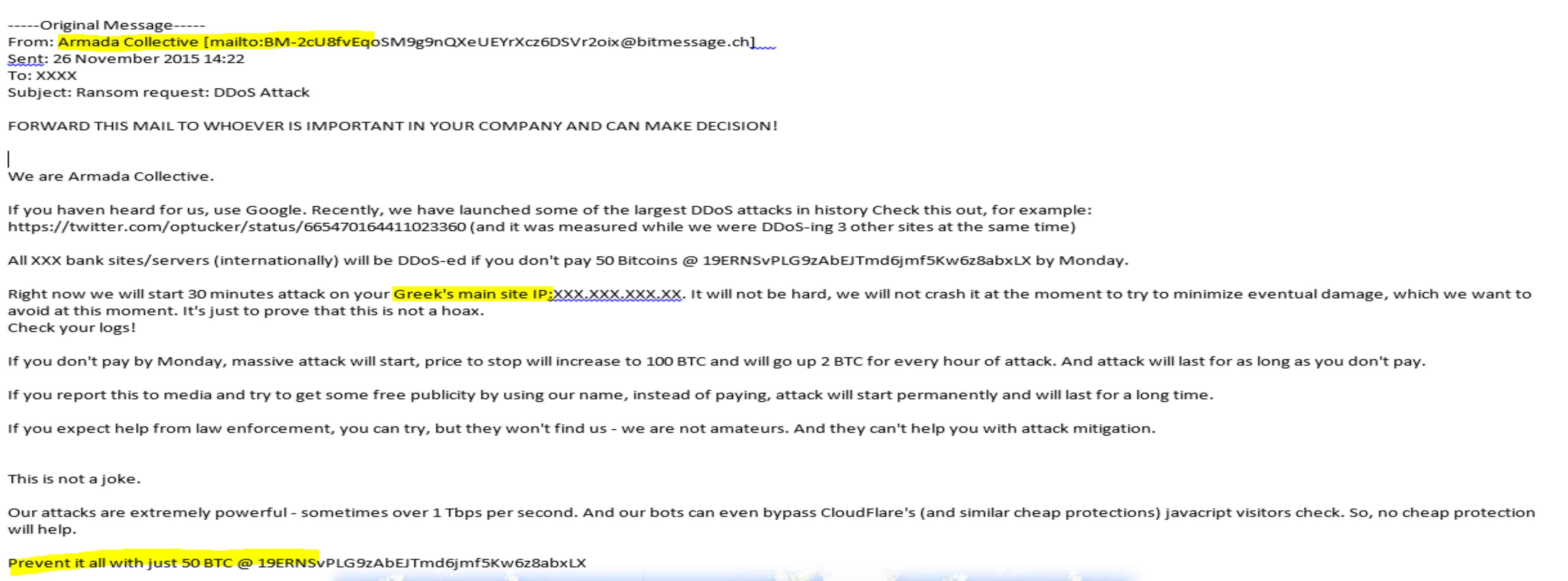
If you receive a mail masquerading as a company's invoice and containing a Microsoft Word file, think twice before clicking on it. Doing so could cripple your system and could lead to a catastrophic destruction. Hackers are believed to be [...]

CTB-Locker Ransomware Spreading Rapidly, Infects Thousands of Web Servers

In last few years, we saw an innumerable rise in ransomware threats ranging from Cryptowall to Locky ransomware discovered last week. Now, another genre of ransomware had been branched out from the family of CTB-Locker Ransomware with an update [...]

Emerging Cyber-Threats

DDoS Extortion: Ransomware's Older Cousin



-----Original Message-----
From: Armada Collective [mailto:BM-2cU8fvEqoSM9g9nQXeUEYrXcz6DSVr2oix@bitmessage.ch]
Sent: 26 November 2015 14:22
To: XXXX
Subject: Ransom request: DDoS Attack

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

If you haven heard for us, use Google. Recently, we have launched some of the largest DDoS attacks in history Check this out, for example: https://twitter.com/optucker/status/665470164411023360 (and it was measured while we were DDoS-ing 3 other sites at the same time)

All XXX bank sites/servers (internationally) will be DDoS-ed if you don't pay 50 Bitcoins @ 19ERNSvPLG9zAbEJTmd6jmf5Kw6z8abxLX by Monday.

Right now we will start 30 minutes attack on your Greek's main site IP:XXX.XXX.XXX.XX. It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax.
Check your logs!

If you don't pay by Monday, massive attack will start, price to stop will increase to 100 BTC and will go up 2 BTC for every hour of attack. And attack will last for as long as you don't pay.

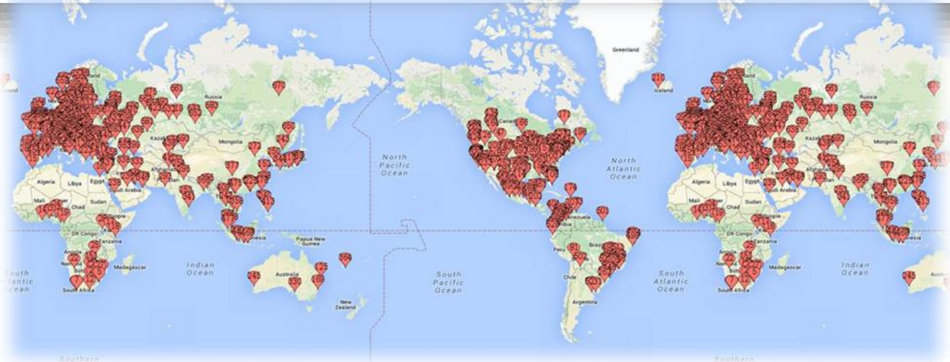
If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

If you expect help from law enforcement, you can try, but they won't find us - we are not amateurs. And they can't help you with attack mitigation.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second. And our bots can even bypass CloudFlare's (and similar cheap protections) javacript visitors check. So, no cheap protection will help.

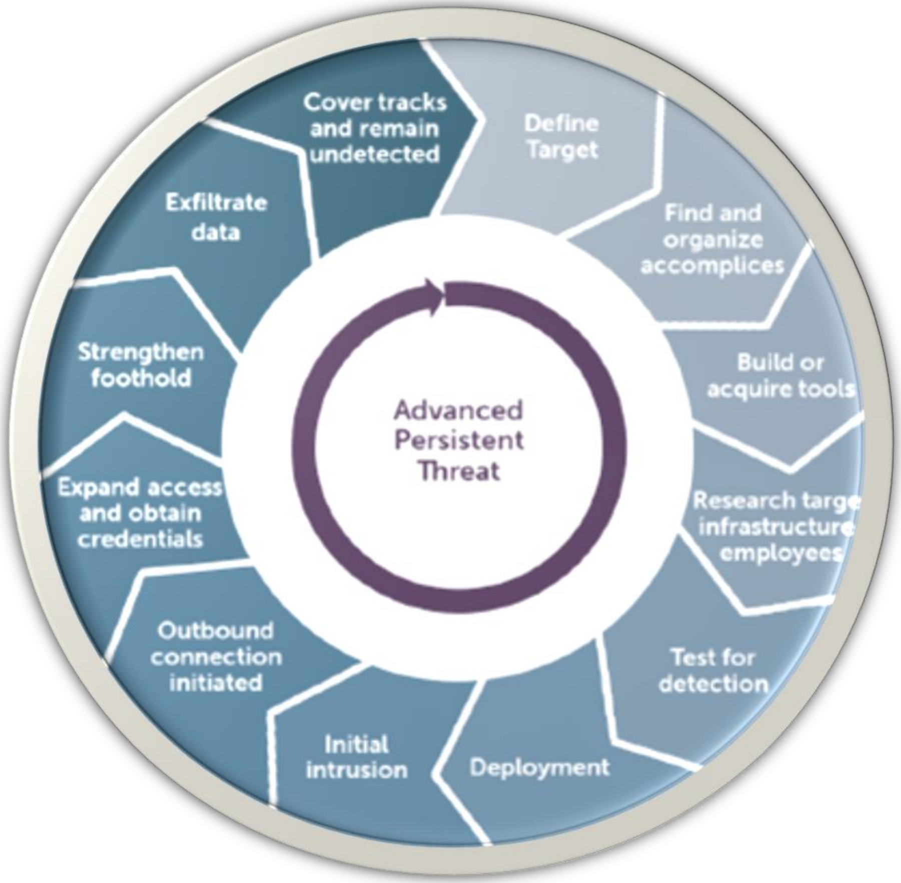
Prevent it all with just 50 BTC @ 19ERNSvPLG9zAbEJTmd6jmf5Kw6z8abxLX



Emerging Cyber-Threats

Advanced Persistent Threats (APTs)

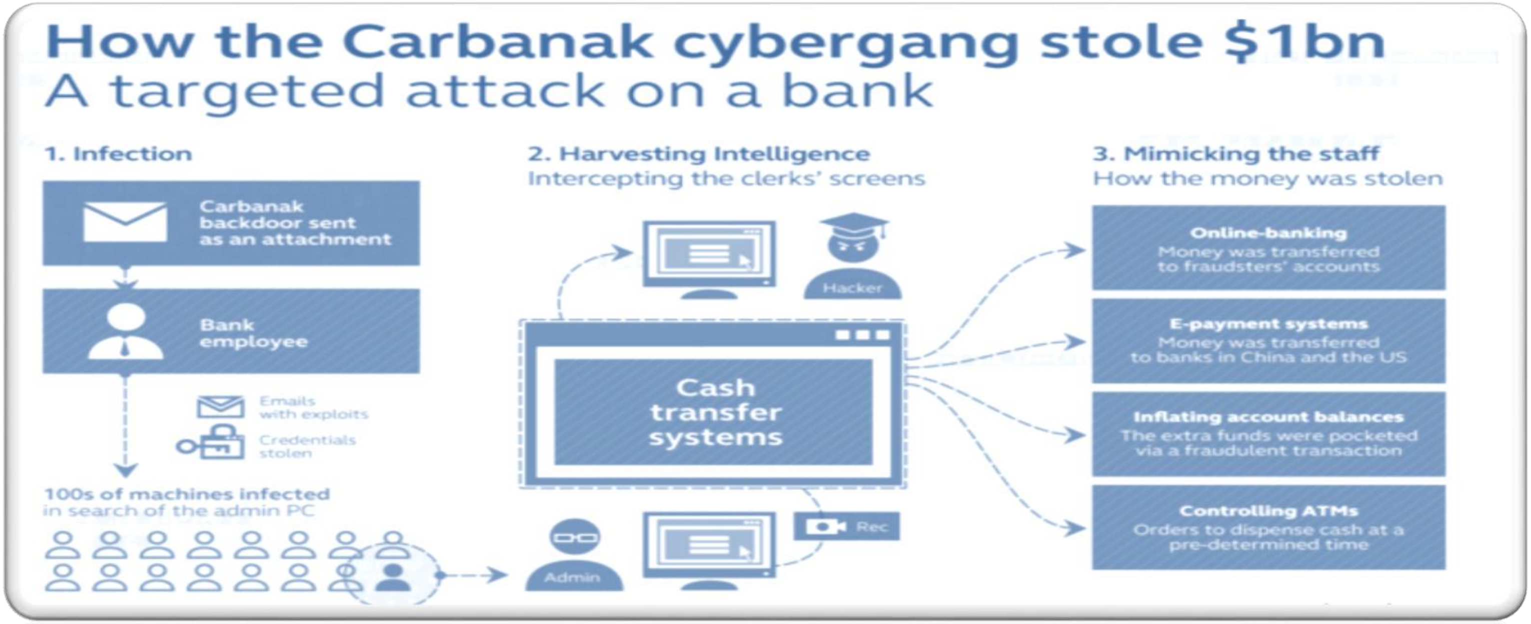
The term is commonly used to refer to Cyber-Threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attack.



Advanced Persistent Threat
Define Target
Find and organize accomplices
Build or acquire tools
Research targe infrastructure employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected

Emerging Cyber-Threats

Economic Impact of Advanced Persistent Threats (APTs)



How the Carbanak cybergang stole $1bn

A targeted attack on a bank

1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected in search of the admin PC

2. Harvesting Intelligence

Intercepting the clerks' screens

3. Mimicking the staff

How the money was stolen

Online-banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the US

Inflating account balances
The extra funds were pocketed via a fraudulent transaction

Controlling ATMs
Orders to dispense cash at a pre-determined time

Carbanak

"The loss is due to an APT campaign targeting dozens of global financial institutions totalled to $1 billion"

Kaspersky, 2015, The greatest heist of the century: hackers stole $1 billion

Combat: A Multidimensional Process

Predictive Approach

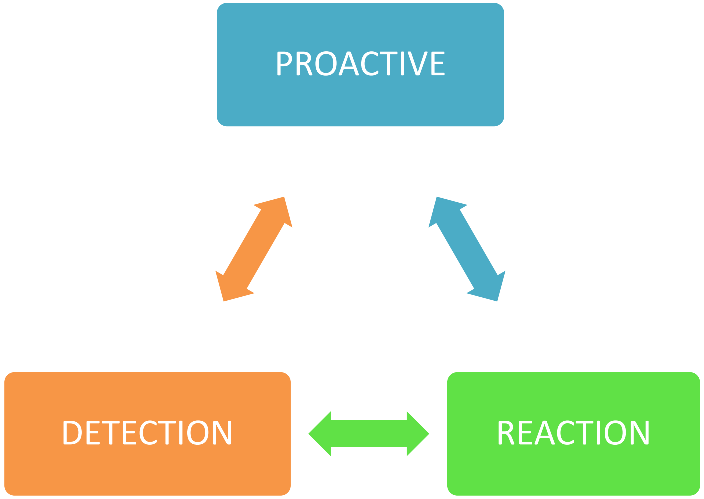
Cyber-Threats have shown that traditional mechanisms are not sufficient and that attackers are using advanced techniques, by even encrypting the payloads.

Most organizations lack the **knowledge** and/or resources to tackle these types of Cyber-Threats, as a result do not take adequate measures.

Combat: A Multidimensional Process

Predictive Approach

- Intelligence on the organization’s overall security postures & capabilities to sustain to a Cyber-Threat.
- Intelligence on new attacking techniques and trends.
- Ability to Resist & Respond.



Combat: A Multidimensional Process

Plan and deliver Proactive Measures to block malicious behavior

- Implement Security Controls (DDoS, IDS/IPS, Firewall, Web Filtering, Antivirus, Mail Relay).
- Harden the infrastructure to make it more difficult for attackers to get in.
- Educate your people to avoid social engineering.

ODYSSEY Cyber Security
Impossible Challenges, Possible Solutions!

Combat: A Multidimensional Process

Plan and deliver Proactive Measures to block malicious behavior

- Use of Managed Security where deemed necessary.
- Run Ethical Hacking Services.
- Run Security Effectiveness Assessment.
- Review DMZ Security Architecture.

Combat: A Multidimensional Process

Detect security threats

- Identify attacks that may have already occurred through event correlation and incident investigation.

- Provide incident analysis and briefings on threat dispositions (Research- Whitepapers).

Combat: A Multidimensional Process

Detect security threats

- Identify groups of malicious users and sources of threat.
- Identify persistent methods and procedures of criminals and other cyber adversaries.

Combat: A Multidimensional Process

React and Respond to threats

- Execute an efficient incident response plan.

- Provide countermeasure support and implementation guidance (ITHACA Labs® Security Advisories).

Combat: A Multidimensional Process

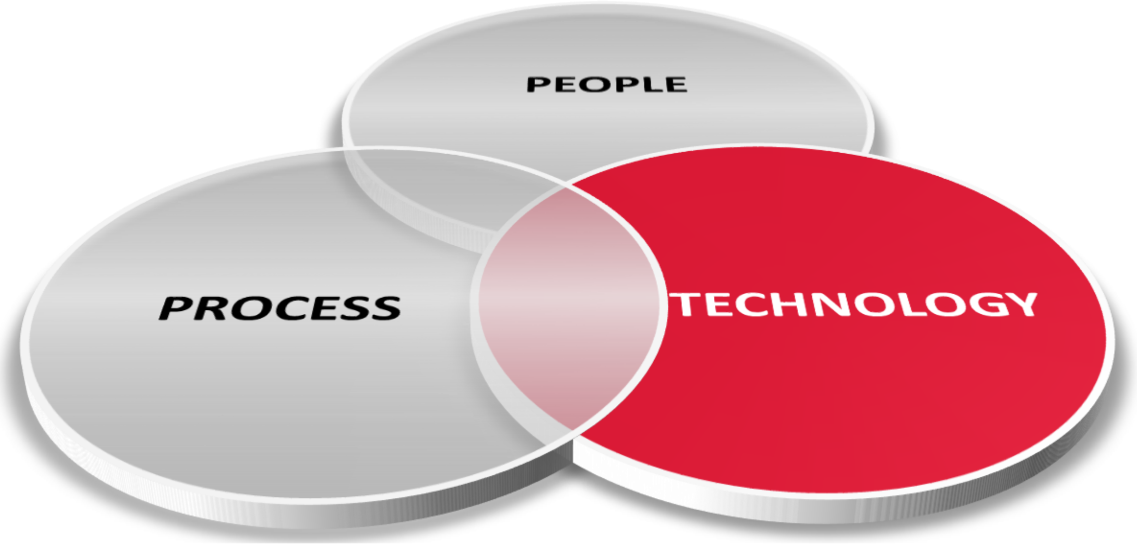
React and Respond to threats

- Provide a range of support options to help you decide the best course of action to defend against cyber attacks.

- Counter intellectual property theft through data leakage remediation.

Conclusion

Collaboration



Help/Support organizations in adopting a **Predictive Approach to Security.**

THANK YOU