ODYSSEY
Impossible Challenges, Possible Solutions

What got us here, won’t get us there

Angelos Printezis | Manager, IthacaLabs™

February 2017

Agenda

1. Company Overview
2. Common Cyber-Security Challenges
3. The state of mitigation practices
4. Re-define your strategy

Company Overview

About Odyssey

Founded in 2002

With the main objective to provide “**High-Quality, Cutting-Edge, Cyber-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 manage Cyber-Risk

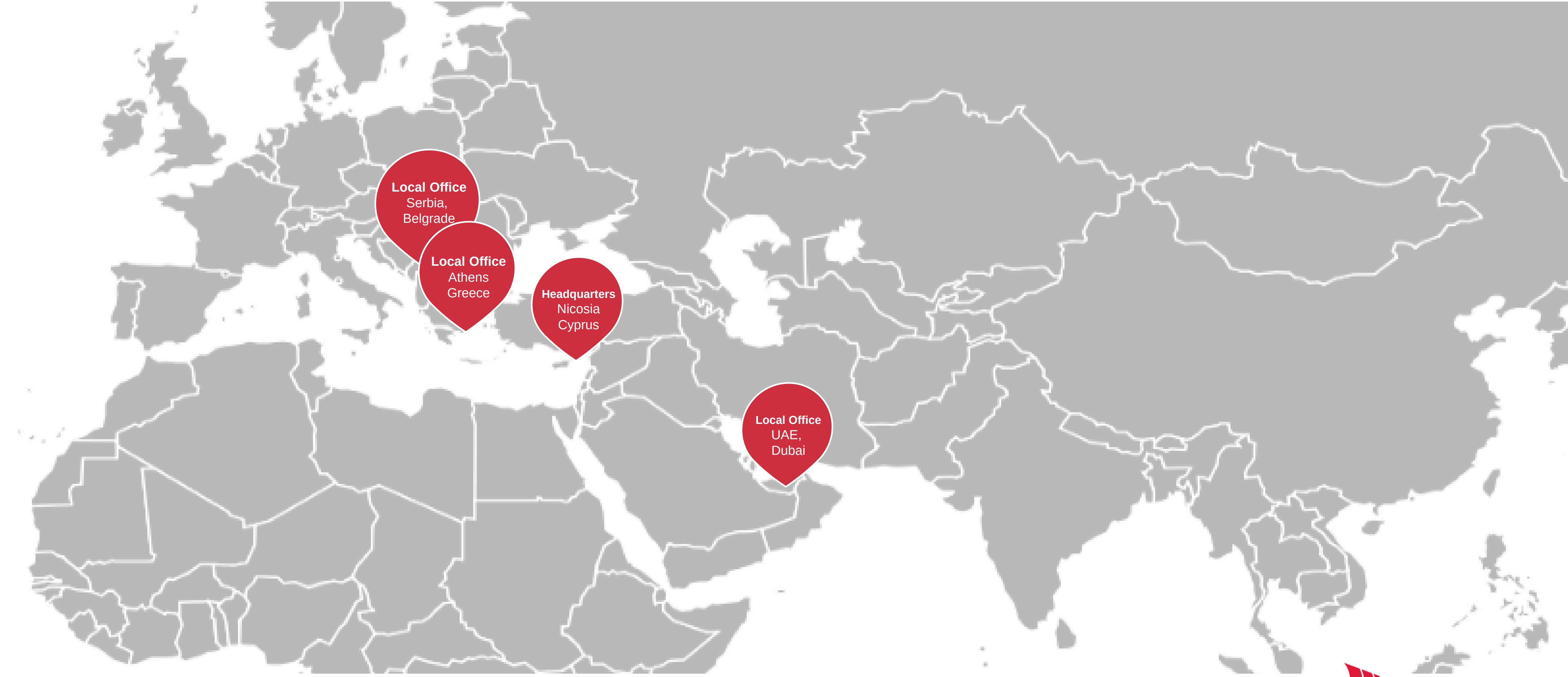
Offices in 4 countries

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

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)**

Odyssey Locations



Odyssey Team

Employees make up a team of 88 highly skilled professionals across all offices

They possess:

- Credentials
- Knowledge
- Hands-on Experience

To provide comprehensive solutions, spanning the whole spectrum of People-Process-Technology

Values

INNOVATION

Transforming innovative ideas into progressive products and solutions that proactively address cybersecurity trends and challenges

PASSION FOR PERFECTION

Striving for perfection by instilling into our people the sense of leadership, ownership and perseverance, which we support through a corporate culture of strong teamwork, mutual respect, and professionalism

CUSTOMER FOCUS

We place our customers in the center of our business equation. Our unconditional commitment is to be ahead of their needs and constantly exceed their expectations, by delivering high quality, adaptive and robust solutions. We develop and maintain long-term relationships with our customers who perceive us as a valuable business associate.

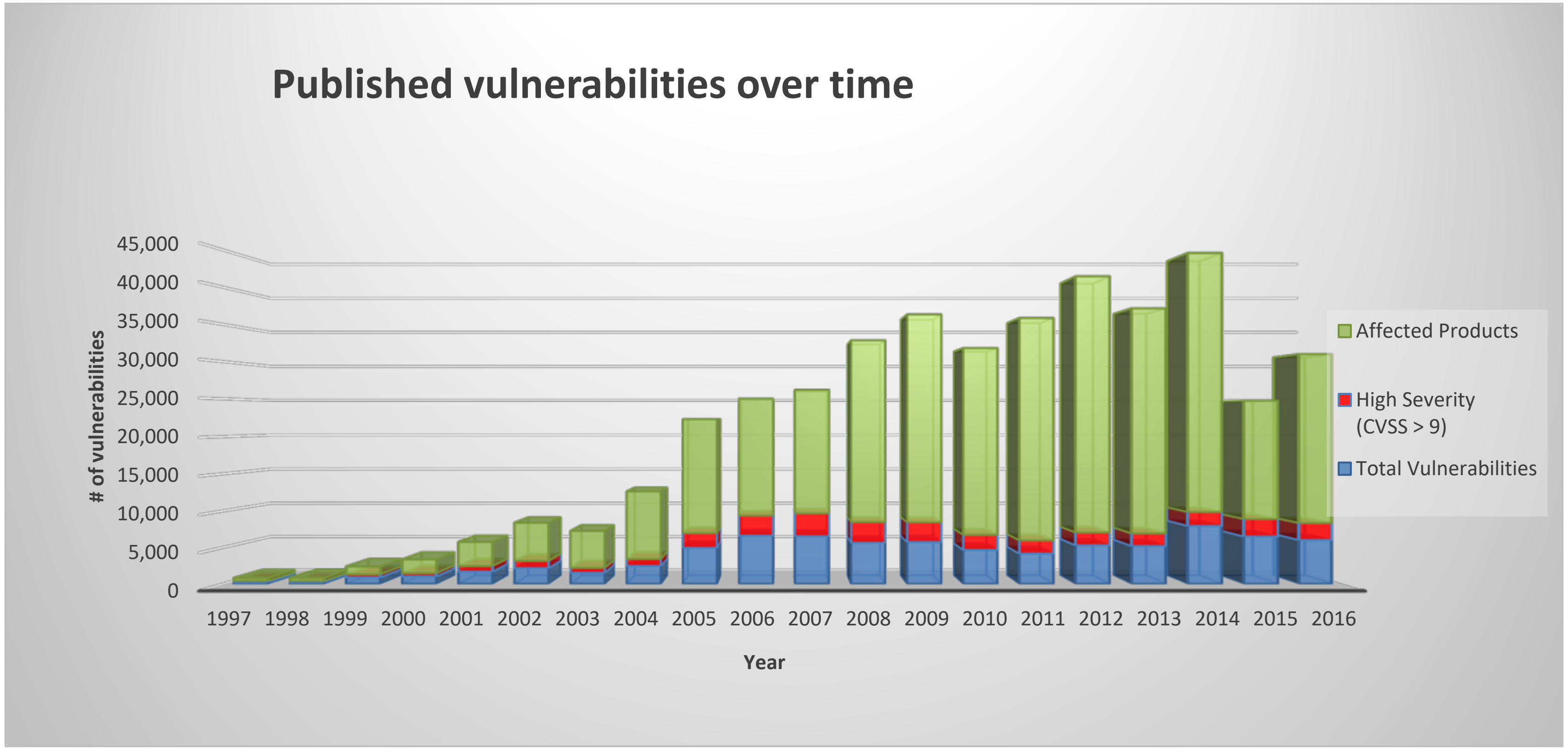
Common Cyber-Security Challenges

In a struggling economy organizations are faced with the following challenges:

- ✓ Constant change of their IT environment
- ✓ Increasing complexity
- ✓ Rapidly evolving threats
- ✓ The need to improve efficiency constantly

Cyber-Threats Landscape

Ever-increasing vulnerabilities

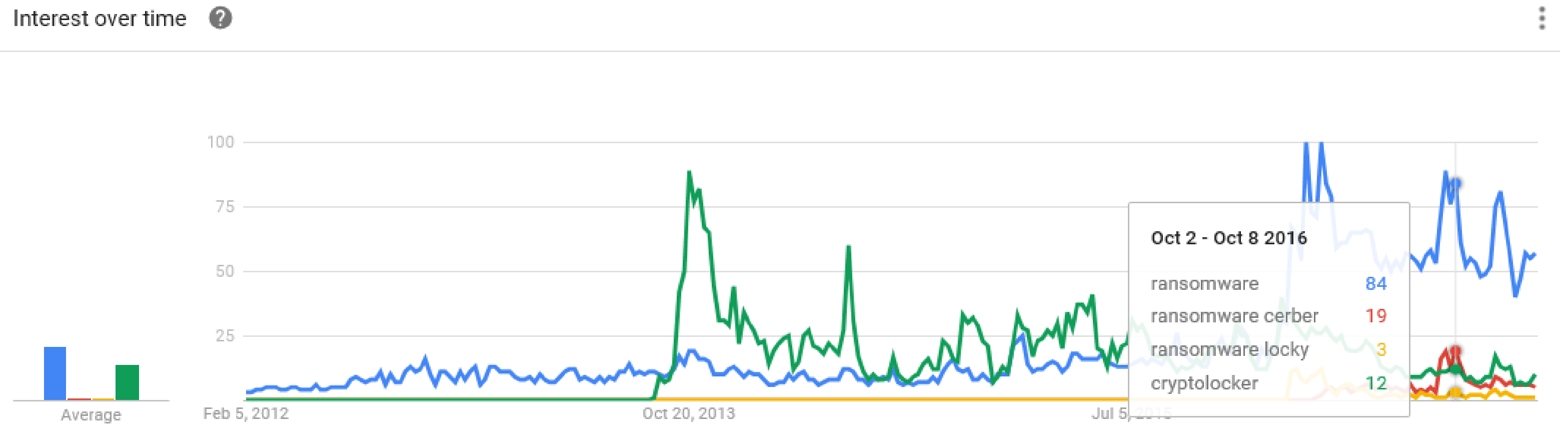


Statistics: IthacaLabs™ Vulnerability Intelligence

Cyber-Threats Landscape

Rise of Ransomware

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



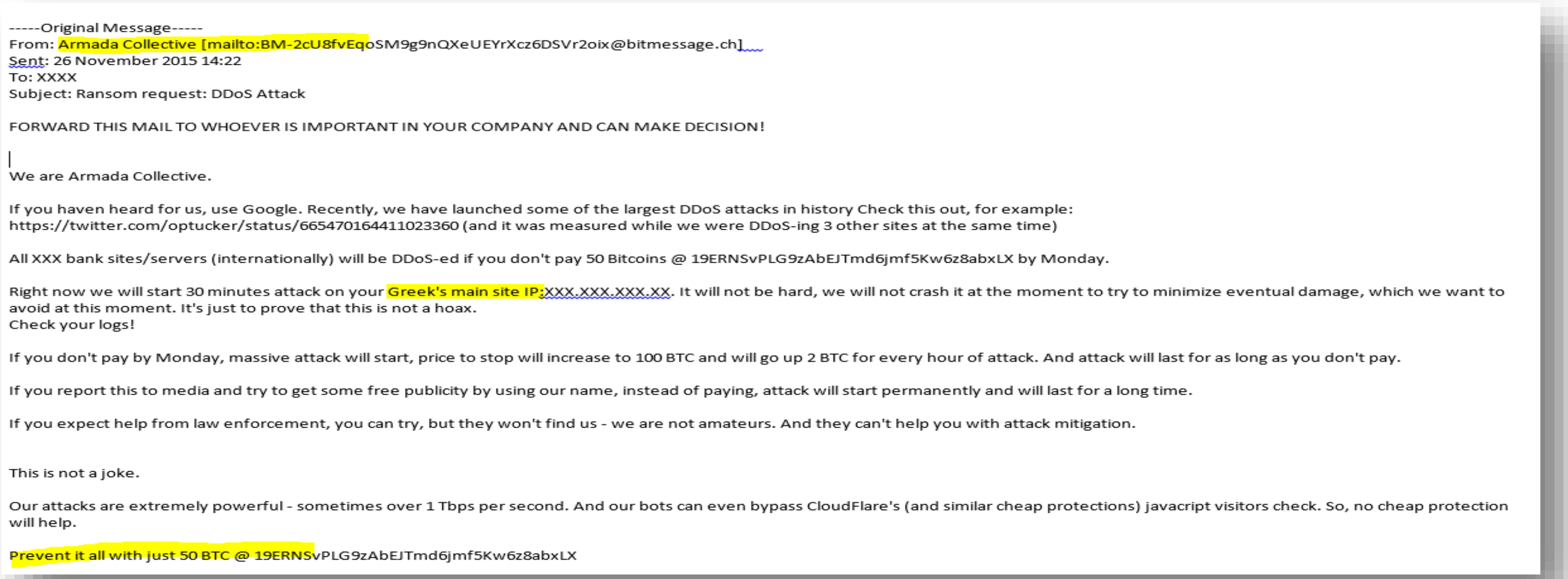
Oct 2 - Oct 8 2016

ransomware	84
ransomware cerber	19
ransomware locky	3
cryptolocker	12

Reference: Google Trends.

Cyber-Threats Landscape

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.

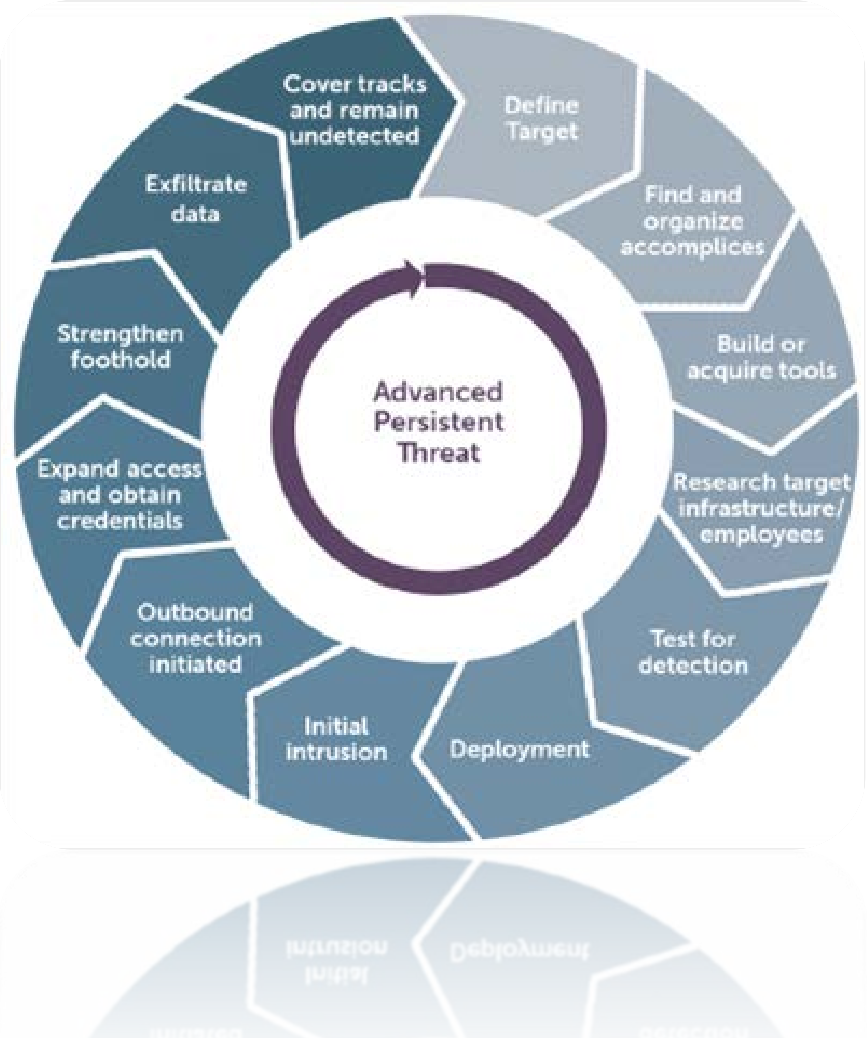
Our attacks are extremely powerful - sometimes over 1 Tbps per second. And our bots can even bypass CloudFlare's (and similar cheap protections) javacript visitors check. So, no cheap protection will help.

Prevent it all with just 50 BTC @ 19ERNSvPLG9zAbEJTmd6jmf5Kw6z8abxLX

Cyber-Threats Landscape

Advanced Persistent Threats (APTs)

The term APT is commonly used to refer to Cyber-Threats, in particular these 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.

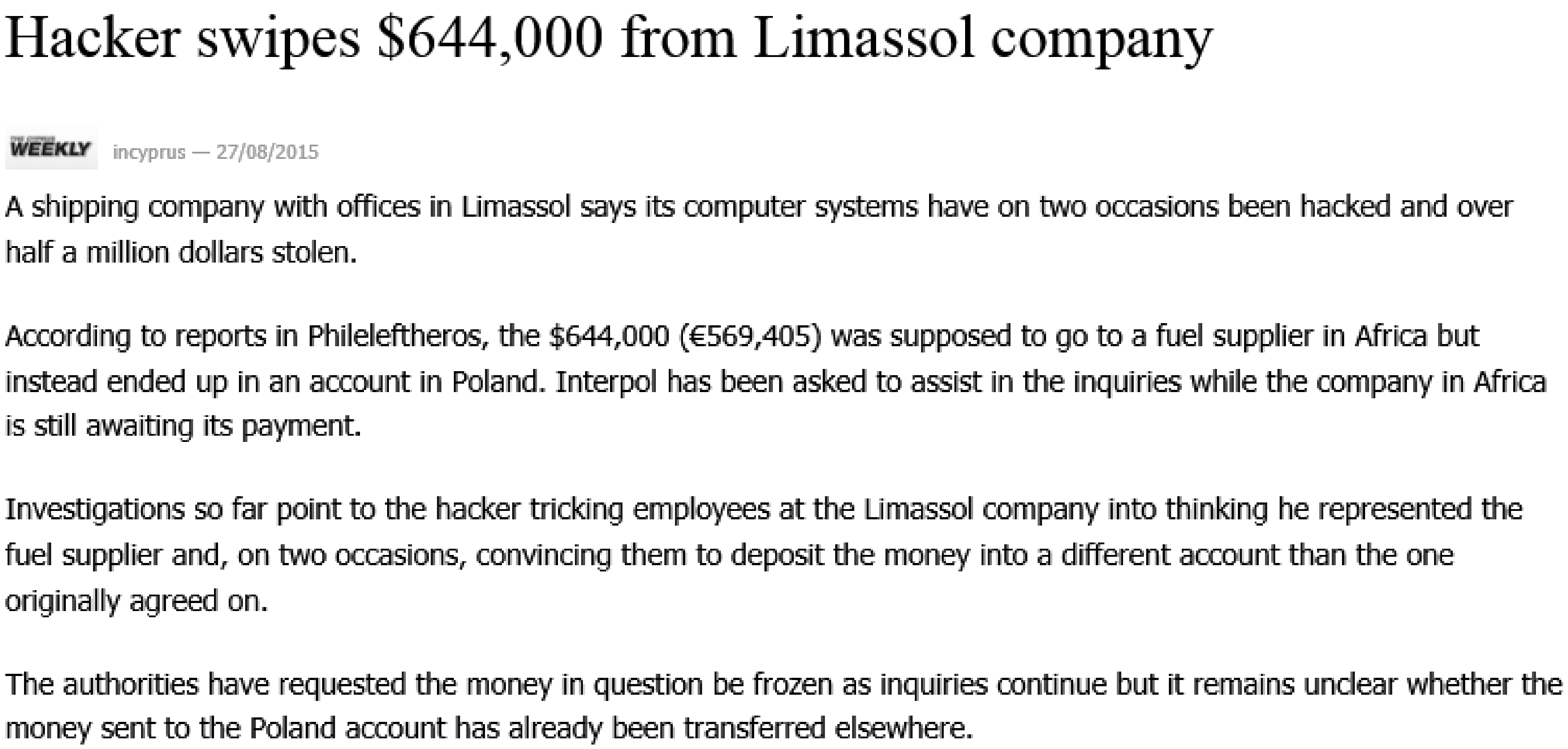

Advanced Persistent Threat
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and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

Examples of Cyber-Crime

Vodafone Germany confirms “insider” data theft

Vodafone Germany said back on 2013 that an internal IT System Administrator launched a criminal attack on one of the company’s servers and stole sensitive data of thousands customers (names, adresses, ID numbers, bank account numbers, credit card numbers and more).

Examples of Cyber-Crime



Hacker swipes $644,000 from Limassol company

WEEKLY incyprus — 27/08/2015

A shipping company with offices in Limassol says its computer systems have on two occasions been hacked and over half a million dollars stolen.

According to reports in Phileleftheros, the $644,000 (€569,405) was supposed to go to a fuel supplier in Africa but instead ended up in an account in Poland. Interpol has been asked to assist in the inquiries while the company in Africa is still awaiting its payment.

Investigations so far point to the hacker tricking employees at the Limassol company into thinking he represented the fuel supplier and, on two occasions, convincing them to deposit the money into a different account than the one originally agreed on.

The authorities have requested the money in question be frozen as inquiries continue but it remains unclear whether the money sent to the Poland account has already been transferred elsewhere.

Cyber-Threats are getting worse

There are many reasons why, though a number of them stand out:

- Emerging Cyber-Threats became successful and the “good news” were widely spread.
“Courage is contagious” (William Franklin Graham).

- Recent espionage and Cyber-Attacks like Wikileaks and Snowden have taught people the value of data.
Access to corporate resources such as e-mail, documents and databases now matters to people.

- Most organizations tend to overlook the basic security strategy.
If you build on sand, your castles will crumble.

Cyber-Security practices fall short

The organizations' boards are now increasingly aware of the cybersecurity problem.

Most organizations are investing in

- ✓ External trainings and certifications
- ✓ Vulnerability Assessment and Remediation
- ✓ Cryptography with Certificates
- ✓ Security patching
- ✓ URL Filtering and Anti-Spam
- ✓ Antivirus
- ✓ Network security controls (Firewalls, IDS/IPS e.t.c)

Still, organizations fall victims of successful Cyber-Attacks.

How can they mitigate risk in the future?

What should organizations do?

You should go back and revise:

- ✓ Understand your crown jewels

  WHAT is most important, WHO is using it, WHERE it is located and HOW can you protect it

- ✓ Revise your Risk Assessment Model - Use the business factor value
- ✓ Incorporate the right technologies
- ✓ Do not omit basic security controls such as network segmentation
- ✓ Do not neglect basic IT hardening
- ✓ Do not hesitate to seek out an expert to help
- ✓ Spend more time teaching your people what they should not do instead of what they should do

Source: https://premaseem.wordpress.com/2015/03/26/hard-work-vs-smart-work/

Keep in touch
Angelos Printezis
aprintezis@odysseycs.com

ODYSSEY
Impossible Challenges, Possible Solutions

HEADQUARTERS

CYPRUS
1 Lefkos Anastasiades str., 2012
Strovolos
Nicosia Tel.: +357 22463600
Fax: +357 22463563

OFFICES

GREECE
237 Mesogeion Av., 154 51
N. Psychiko,
Athens, Greece
Tel.: +30 210 6565200,
Fax: +30 210 6565219

SERBIA
38-40 Vladimira Popovica 1st
floor, 119 11000 Belgrade
Tel.:+381 117 156956
Fax: +381 117 156900

DUBAI
Ground Floor #07, Building 16,
Dubai Internet City, O Box 73030
Dubai, UAE
Tel.: +971 559357590,
Fax: +357 22463563