Symantec

HACK IN BO
LAB EDITION

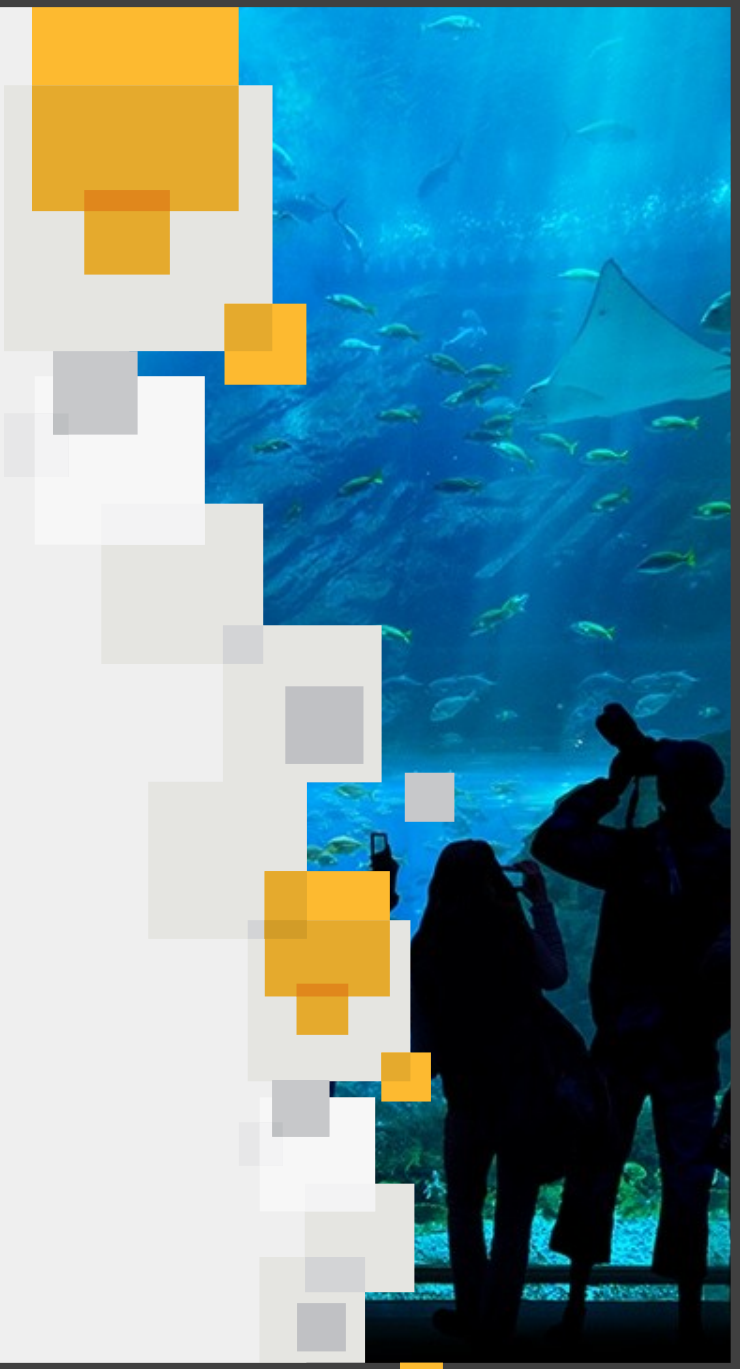
Attackers Vs Defenders:
change your strategy and stop losing

Antonio Forzieri

EMEA Cyber Security Practice Lead

Symantec

Attack Techniques



Attacker motivations

CYBERCRIME

- Financial Trojans
- Ransomware

ESPIONAGE

- Nation states
- Corporate

SUBVERSION

- DDoS
- Social media hacking

SABOTAGE

- Physical damage
- Data destruction

The three most common attack vectors

Spear Phishing

Email with an attachment or link to malic
1 in 247 email has a virus attached

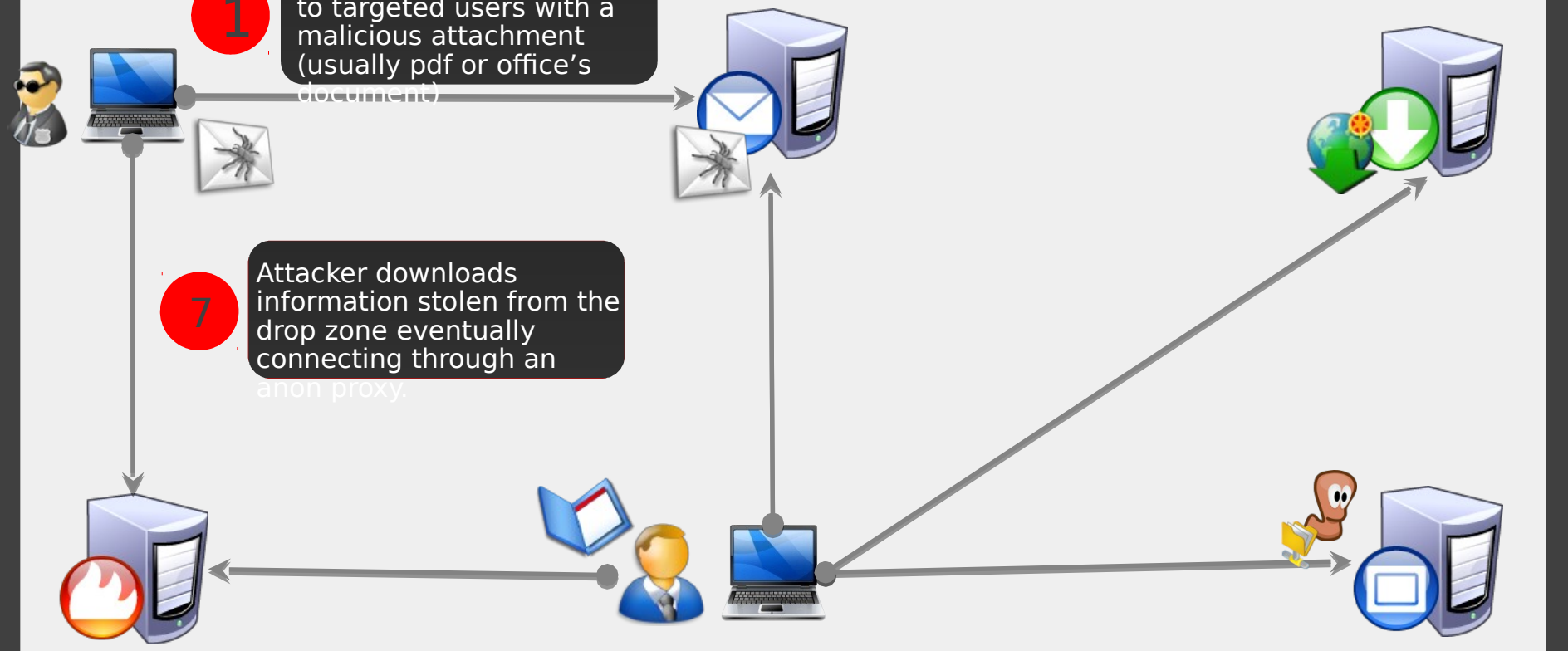
ve-by Download Attack

site uses exploit to install malware on
computer. Popular Exploit Toolkits

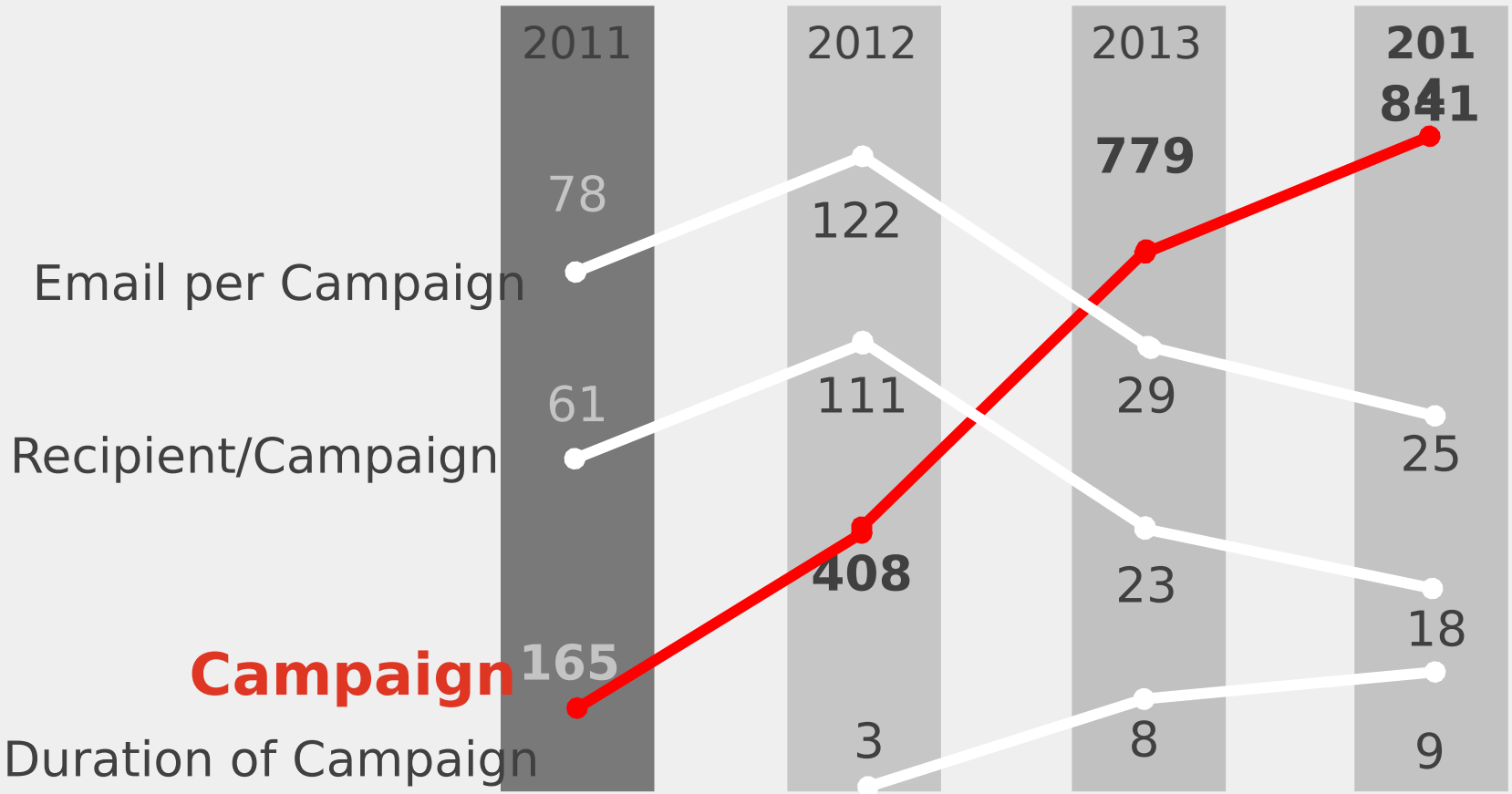
Supply-chain Hack

Software of a vendor gets compromis
and hijacked to infect its clients

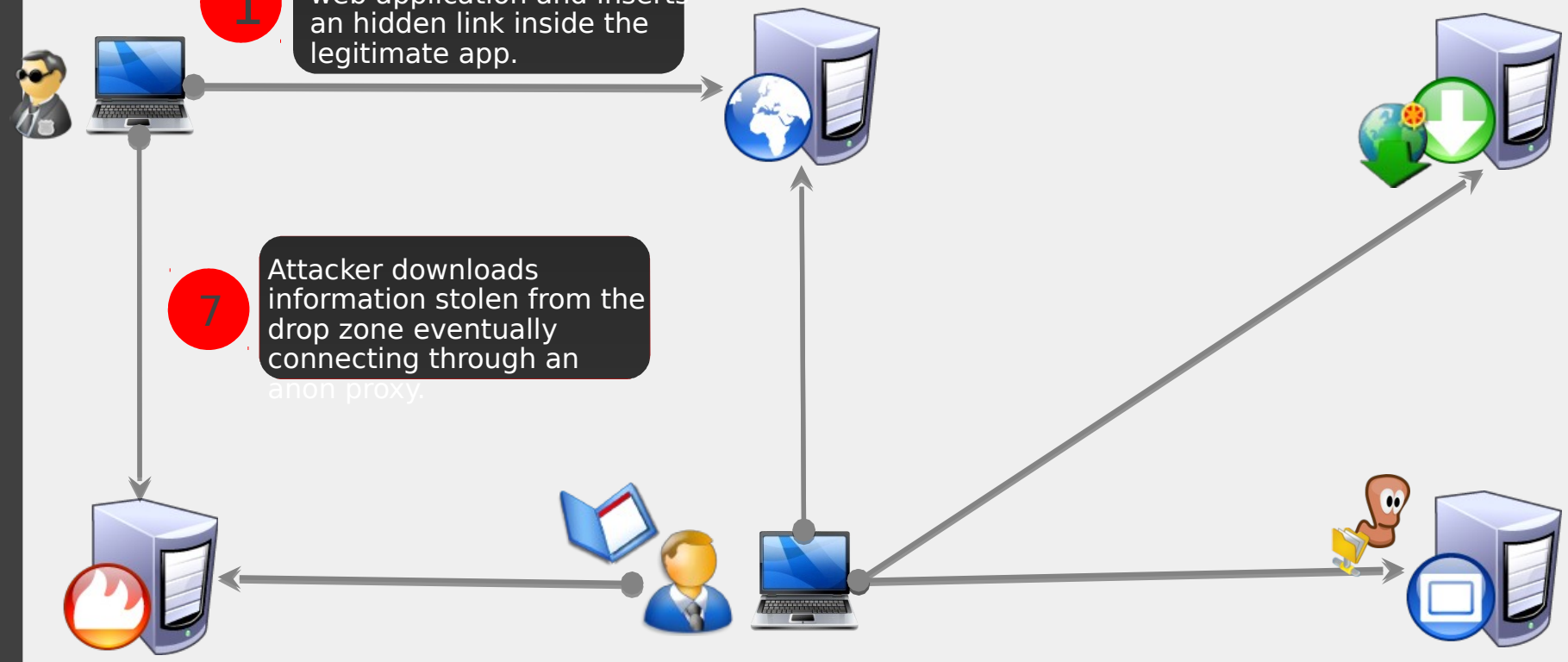
Spear phishing



Targeted attacks with spear phishing emails



Drive-by download (Watering hole)



Watering hole – let's have a look at it

Supply-chain Hack

- Hidden Lynx (Gov) 2012:
  - During SCADEF campaign, manufacturers and suppliers of military-grade computers were observed installing a Trojanized Intel driver application;
  - Attackers bundled an Intel driver application with variants of Backdoor.Moudoor
- DragonFly (Energy) 2013:
  - Three different ICS equipment providers were targeted and malware was inserted into the software bundles they had made available for download on their websites.

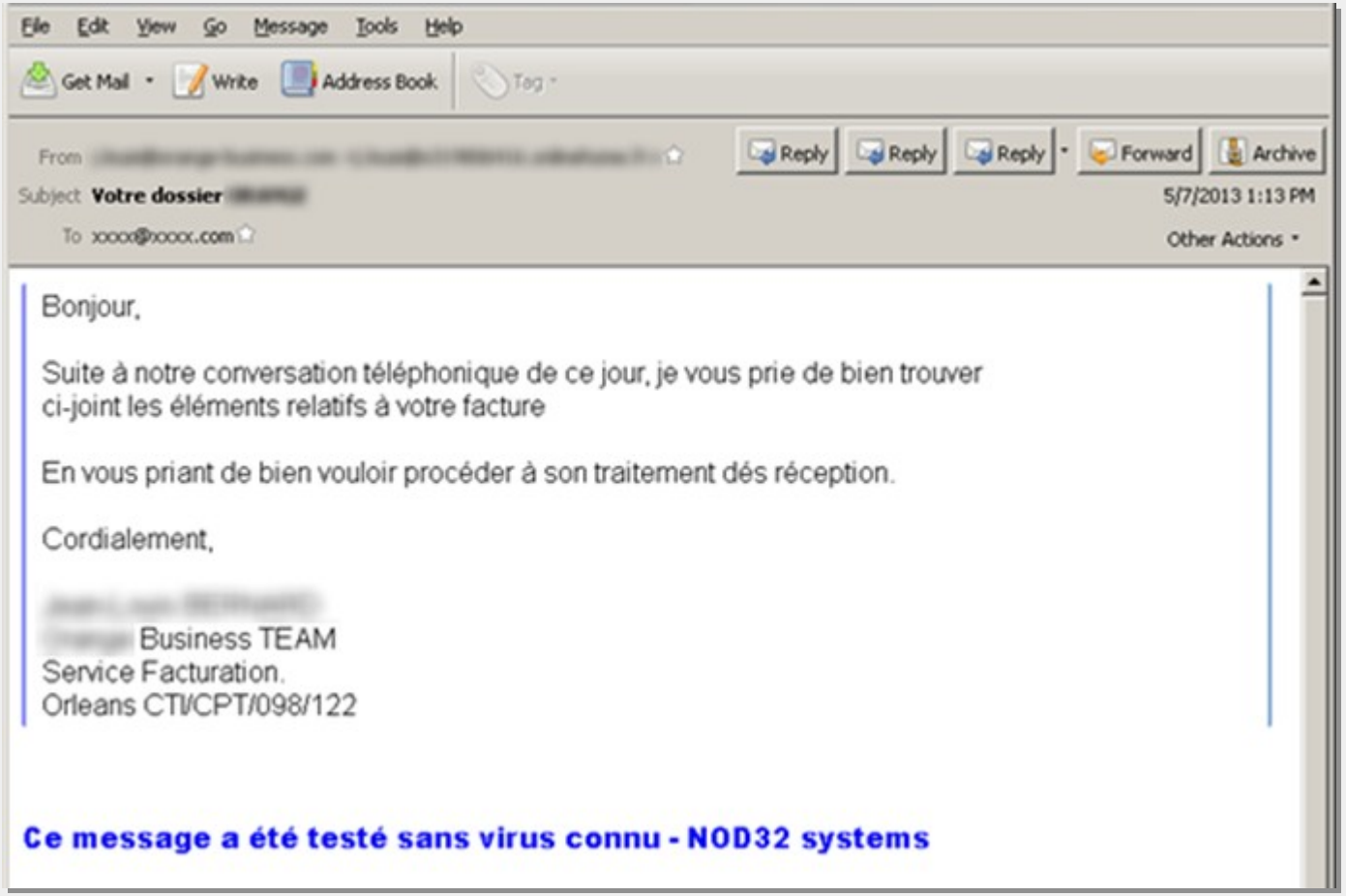
Nice techniques

What do they have in common?!?

- The old days where attackers were hitting servers are gone:
  - They still hit them, but there's a more juicy target
- Attackers are heavily using social engineering techniques:
  - Attacks are accurately planned gathering information my many means
  - E-mails are well built and realistic and relevant to real/realistic projects
  - Users targeted usually have access to sensitive information and have a low security awareness
  - Even badly written e-mails are effective:
    - Crypto/CTBlocker ANYONE?!?

Talking about social engineering...
Operation Francophoned

- Convinced by phone to open the attachment



Talking about social engineering...

Another spear phishing case

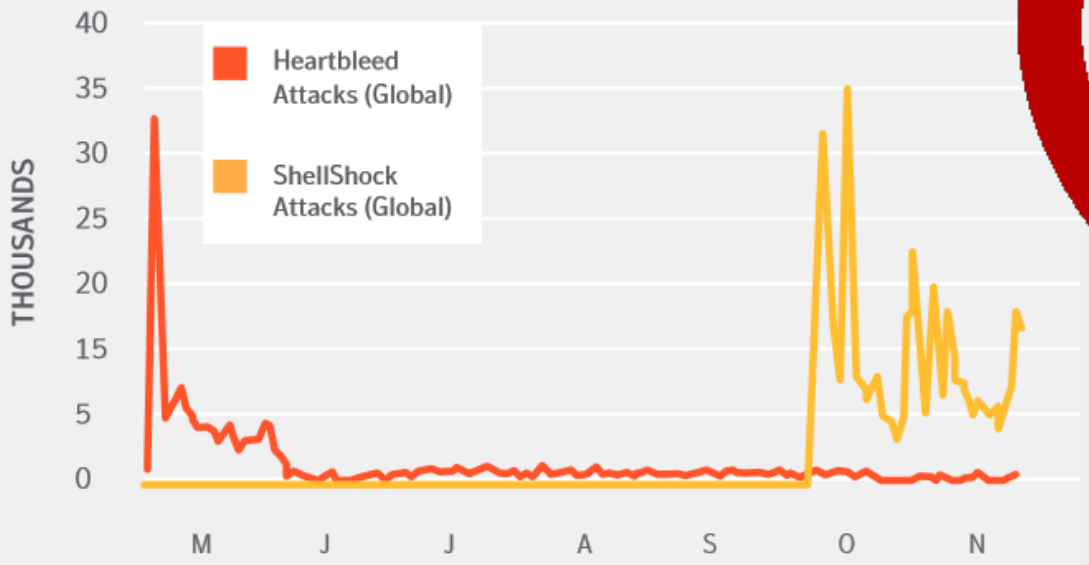
No you cannot patch them

- Awareness
- Awareness
- Awareness
- Awareness
- Awareness
- Awareness
- Awareness
- Awareness
- Awareness

What about server vulnerability?

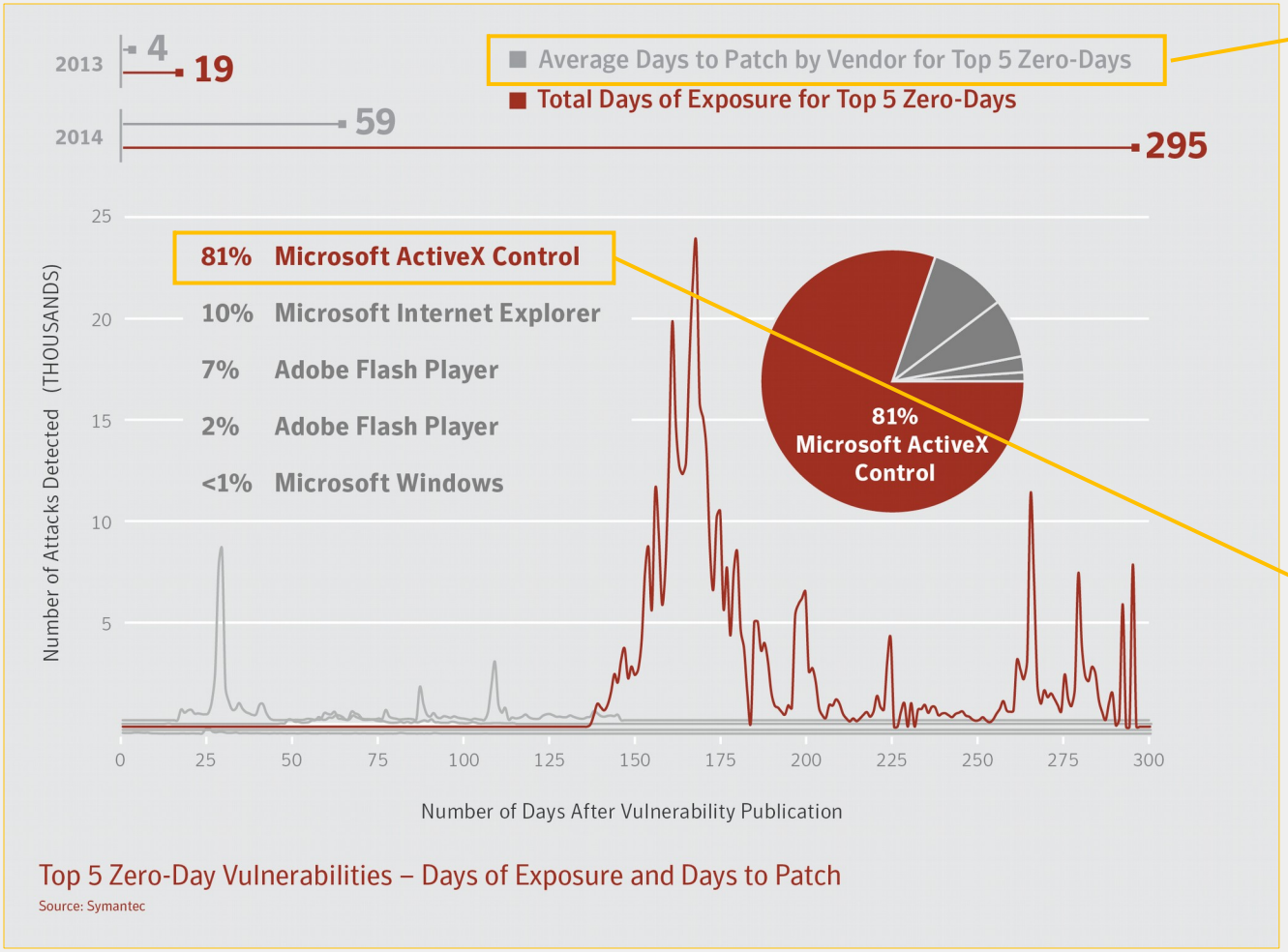
Heartbleed OpenSSL Vulnerability

- Affected > 500M trusted websites (~17% of all TLS servers)
- Heartbleed vulnerability used 4h after reporting
- Other issues: POODLE, FREAK, LogJam …
- 24 reported zero-day vulnerabilities in 2014



But we are good in patching right?

Well… I'd not say good.



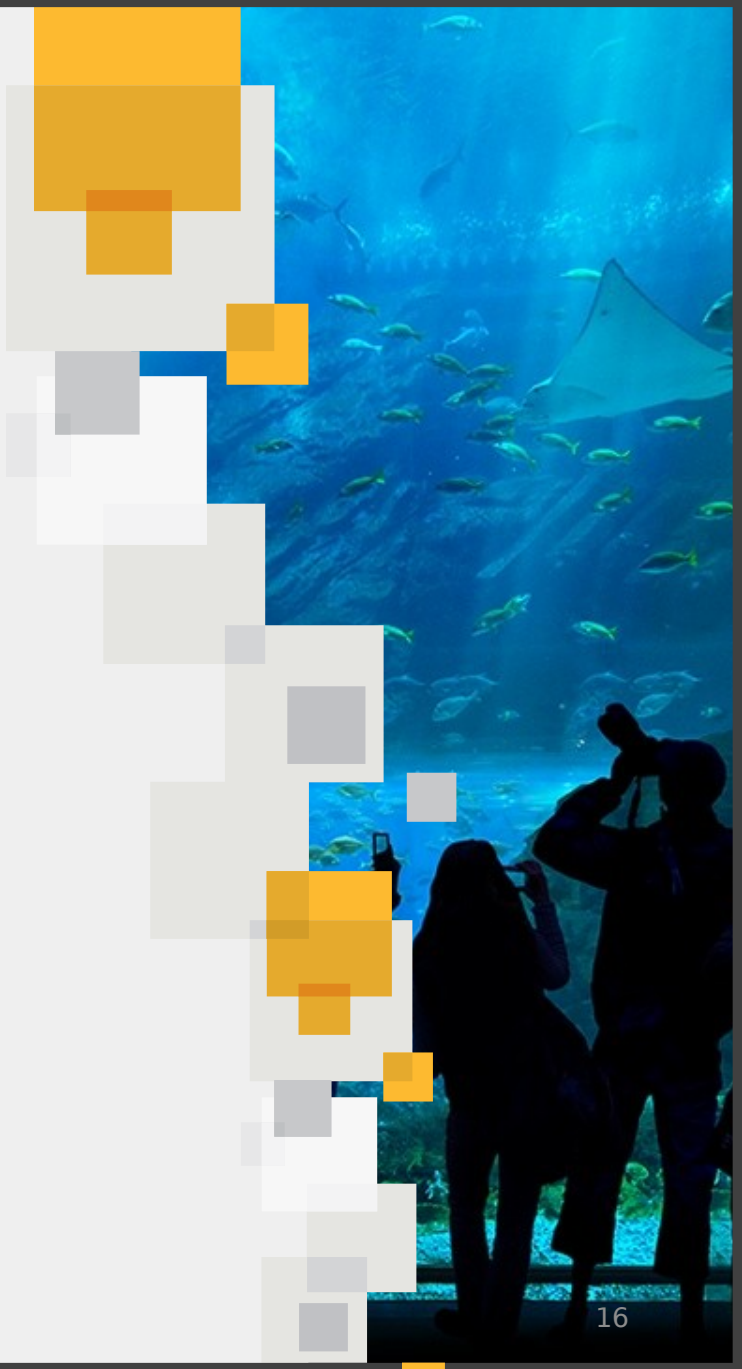
Top 5 Zero-Day Vulnerabilities – Days of Exposure and Days to Patch

Source: Symantec

- Time for vendor to supply a patch.
- *No tracking on how long companies take to patch was done.*

204 days to patch

Let’s see two attacks



Stages of an attack

INCURSION

Attacker breaks into the network by delivering targeted malware to vulnerable systems and employees

DISCOVERY

Attacker then maps organization's defenses from the inside

Create a battle plan

CAPTURE

Accesses data on unprotected system

Installs malware to secretly acquire data or disrupt operations

EXFILTRATION

Data sent to attacker for analysis

Information may be used for various purposes including fraud and planning further attacks

ECONNAISSANC INCURSION DISCOVERY CAPTURE EXFILTRATION

Regin at a glance

- COMPLEX TOOL-SUITE/PLATFORM FOR SPYING & SURVEILLANCE BY GOVERNMENTS
- SIMILAR TO STUXNET IN COMPLEXITY
- CUSTOMISED FOR EACH SPECIFIC MISSION
- USED AGAINST VARIETY OF ORGS IN MANY COUNTRIES
- INVESTIGATED BY SYMANTEC FOR OVER A YEAR
- **OPERATING SINCE AT LEAST 2008…**

SYMANTEC DETECTION NAME

BACKDOOR.REGIN

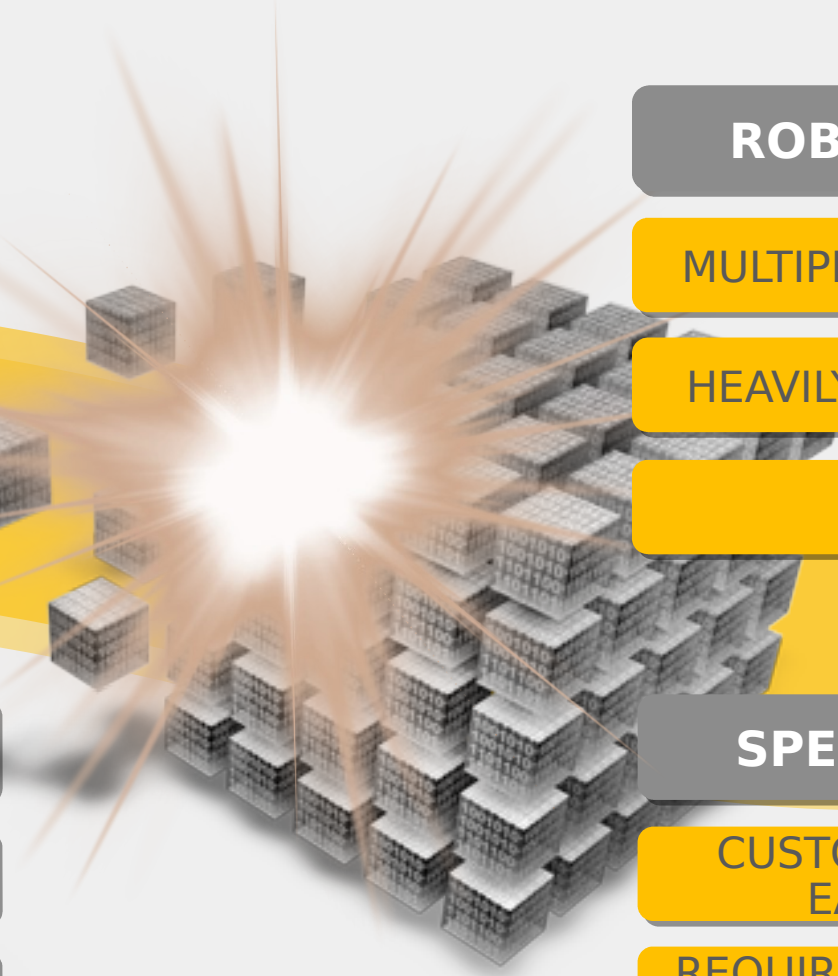
Regin features

MULTI-STAGED & MODULAR

- MANY COMPONENTS
- CUSTOMIZABLE
- DIFFICULT TO ANALYZE

ROBUST C&C

- MULTIPLE CHANNELS
- HEAVILY ENCRYPTED
- P2P



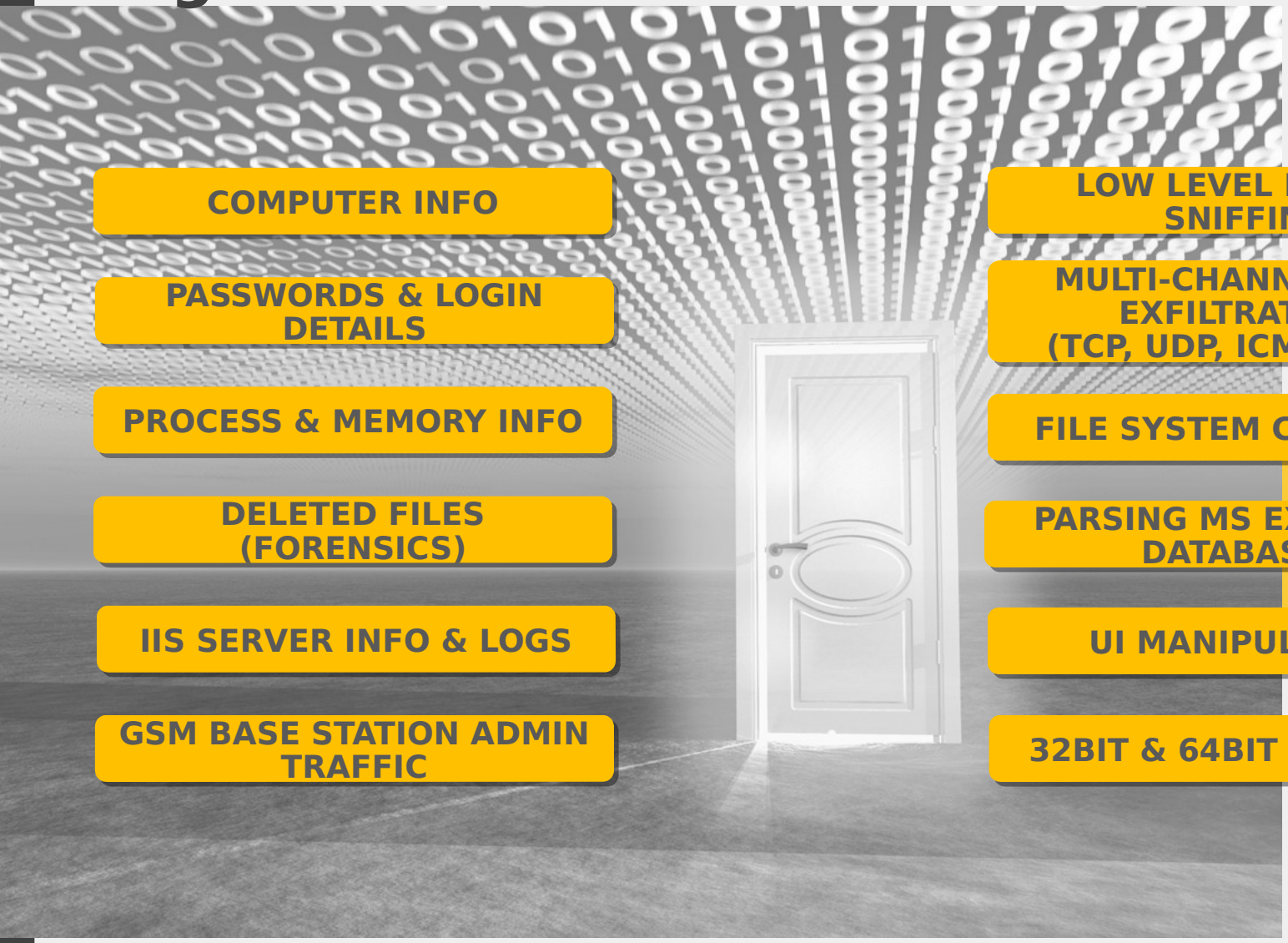
PERSISTANCE & STEALTH

- BULK OF CODE IS HIDDEN
- COMPLEX ENCRYPTION

SPECIALIZED

- CUSTOMIZED FOR EACH JOB
- REQUIRES SPECIALIST SKILLS

Regin: What can it do?

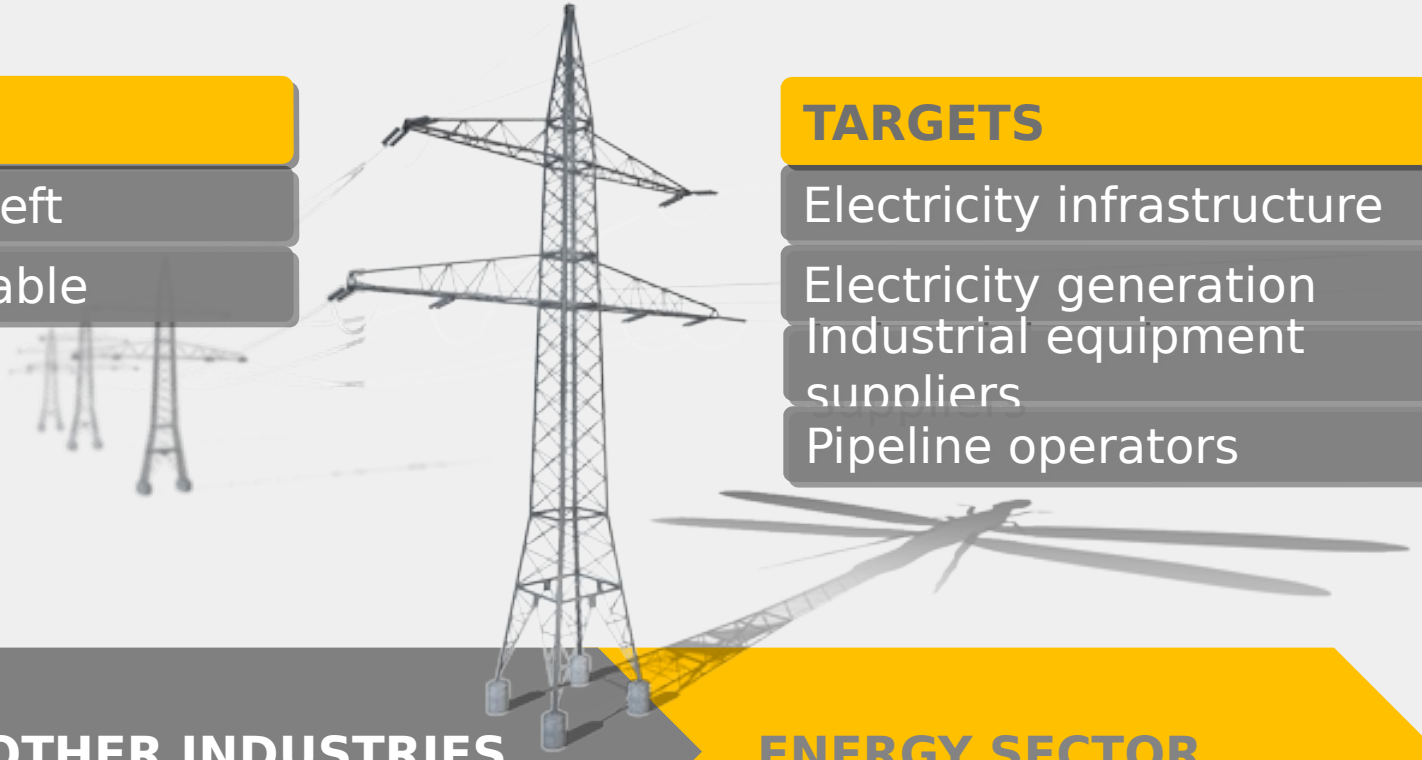


- COMPUTER INFO
- PASSWORDS & LOGIN DETAILS
- PROCESS & MEMORY INFO
- DELETED FILES (FORENSICS)
- IIS SERVER INFO & LOGS
- GSM BASE STATION ADMIN TRAFFIC
- LOW LEVEL PACKET SNIFFING
- MULTI-CHANNEL DATA EXFILTRATION (TCP, UDP, ICMP, HTTP)
- FILE SYSTEM CRAWLING
- PARSING MS EXCHANGE DATABASES
- UI MANIPULATION
- 32BIT & 64BIT VERSIONS

Yep… this was sophisticated and ADVANCED

Dragonfly: Attacks against the energy sector

Dragonfly attack group has been active since 2011, but shifted focus to the energy sector in early 2013…



ACTIVITIES

- Information theft
- Sabotage capable

TARGETS

- Electricity infrastructure
- Electricity generation
- Industrial equipment suppliers
- Pipeline operators

OTHER INDUSTRIES → **ENERGY SECTOR**

2011 2012 2013 2014

Dragonfly: The tools of the trade

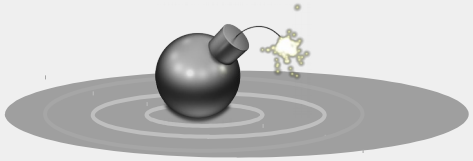
TROJAN.KARAGNY

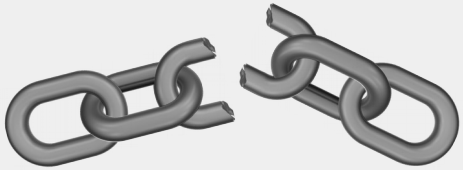
- Available in underground markets
- Adapted for use by Dragonfly group
- Download/upload/execute files
- Additional plugins available

BACKDOOR.OLDREA

- Custom made malware
- RAT – full back door access
- Used in 90% of cases

Dragonfly: Attack vectors





SPAM EMAIL

TARGETING:
Spam email sent to senior employees and engineers

HISTORY:
February 2013

EMAIL SUBJECTS:
- "The account"
- "Settlement of delivery problem"

EMAIL ATTACHMENT:
Malicious PDF file

WATERING HOLE

TARGETING:
Visitors to compromised websites related to energy sector

HISTORY:
May 2013

EXPLOITS:
Redirects visitors to other hacked sites hosting Lightsout exploit kit

Malware dropped onto victim's computer

SUPPLY CHAIN

TARGETING:
Compromise ICS equipment vendors & suppliers

HISTORY:
June/July 2013

POISONED SOFTWARE:
Malware added to software files/updates on vendor's websites

Victims unknowingly download and install "Trojanized" software updates

Yep… this was less (NOT) so advanced

How do we protect?

Forrest Gump MANTRA

it happens!!!

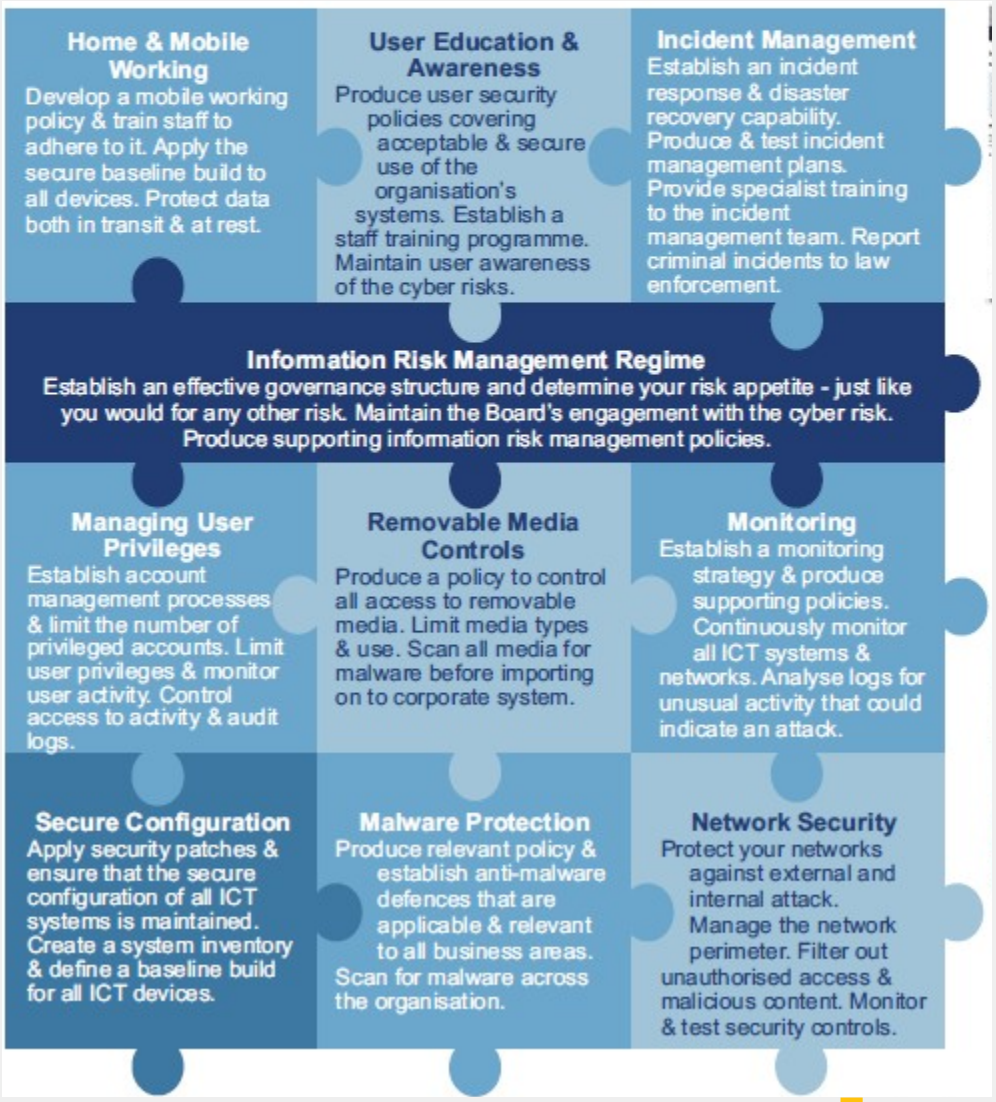
> **Bumper Sticker Guy:** [running after Forrest] Hey man! Hey listen, I was wondering if you might help me. 'Cause I'm in the bumper sticker business and I've been trying to think of a good slogan, and since you've been such a big inspiration to the people around here I thought you might be able to help me jump into - WOAH! Man, you just ran through a big pile of dog shit!
> **Forrest Gump:** It happens.
> **Bumper Sticker guy:** What, shit?
> **Forrest Gump:** Sometimes.

Before we start

Get the basics right!

CESG 10 Steps to Cyber Security

Cyber Security guidance from CESG (Communications-Electronics Security Group), the UK Government's National

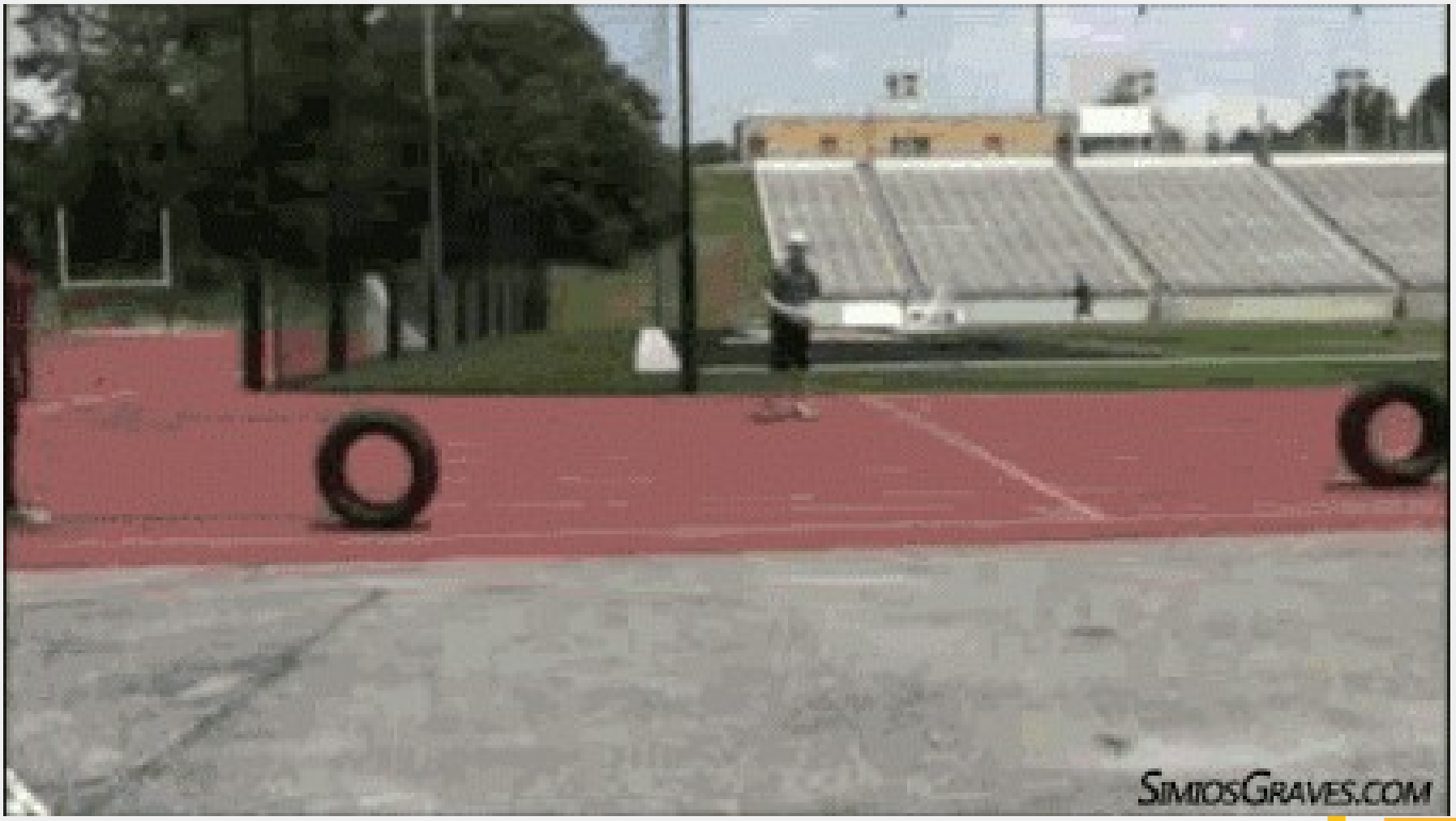


Back to basics…
few simple examples

- Endpoint Protection:
  - Is your technology configured to adopt all available engines?
  - Is the update mechanism scheduled every 2/4h?
- Patch Management:
  - Do you have a Patch Management Process (a real one I mean, not the one you have in your drawer)
- Vulnerability Management:
  - Do you have a Vulnerability Management Process (a real one I mean, not the one you have in your drawer)
- Perimeter Security:
  - Are you sure you should allow binary files (even zipped) attached to e-mail?
- Hardening:
  - I'm kidding… I know it's just a dream.

NO: IPS, Firewall and AV are not enough

Security… you are doing it wrong

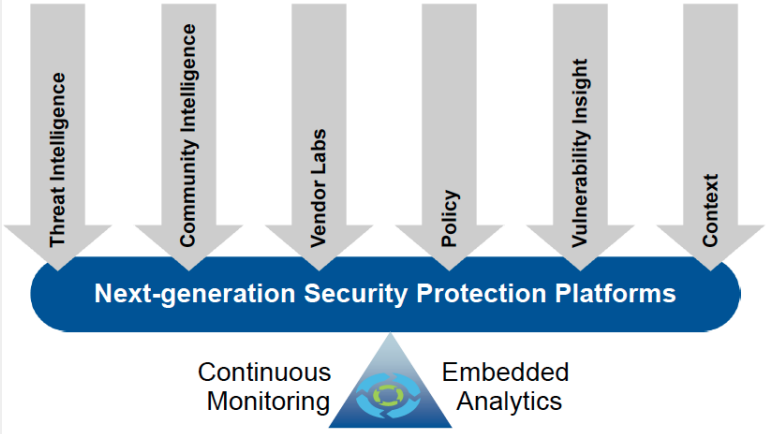


What else should we be doing?

Evaluating Vendor's Platforms: Ten Key Questions

- What specifically are you monitoring?
- How much data does this generate, what bandwidth and storage does it consume and where is it stored?
- What analytics do you use to detect potential incidents?
- How can the operator tune the algorithms to reduce noise?
- What context do you use to provide actionable intelligence?
- Do you prioritize incidents based on risk? Is this tunable?
- What third-party security intelligence feeds do you integrate?
- What are the capabilities of your own labs?
- Is there a community and ecosystem around the platform?
- What blocking/prevention capabilities does your product have or partners to achieve this?

Key Inputs Into Next-generation Security Platforms



Gartner

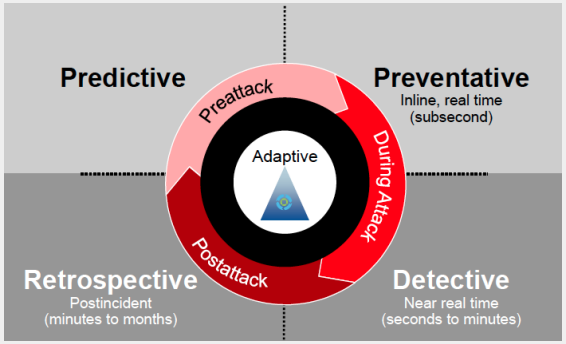
G00259490

Designing an Adaptive Security Architecture for Protection From Advanced Attacks

Published: 12 February 2014

Analyst(s): Neil MacDonald, Peter Firstbrook

Enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective and response capabilities.

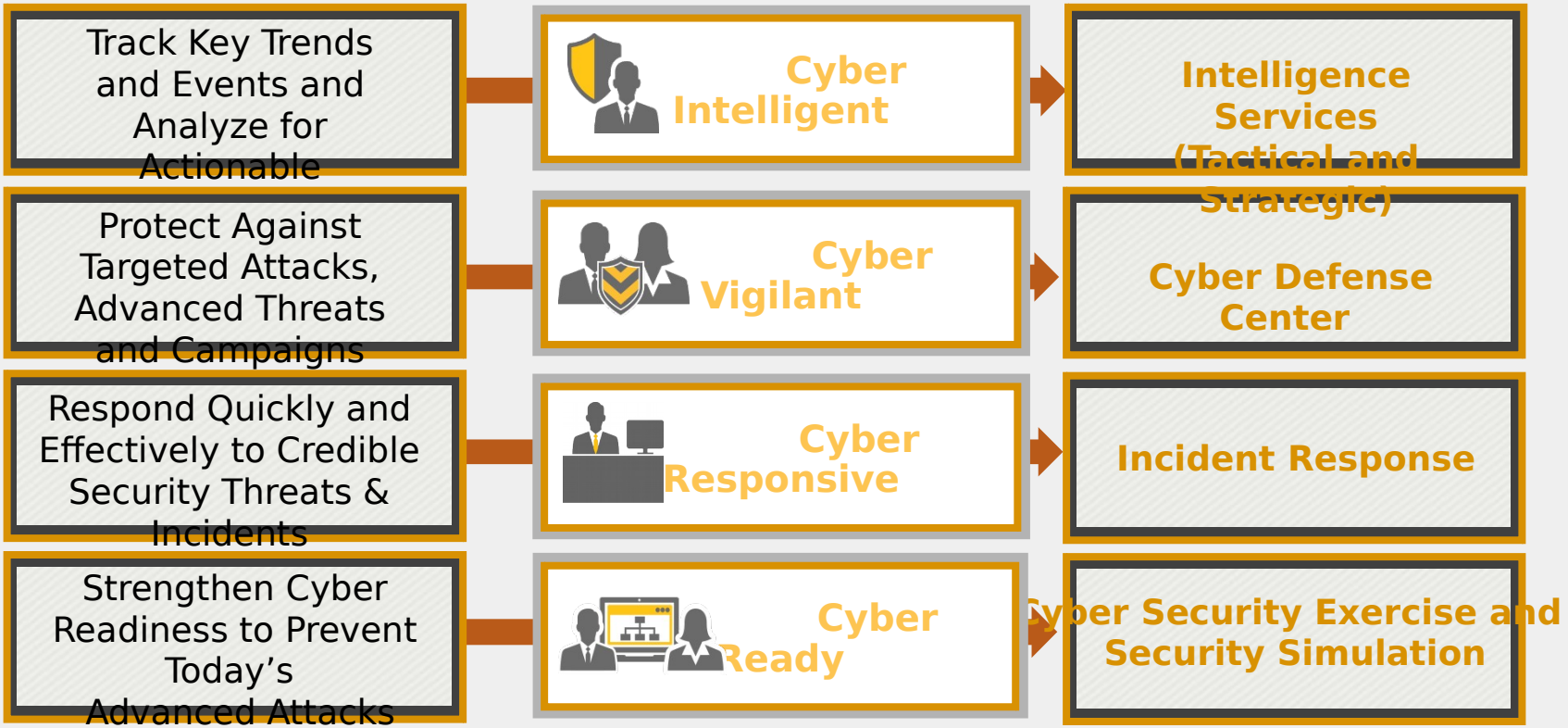


Recommendations

Information security architects:

- Shift your security mindset from "incident response" to "continuous response," wherein systems are assumed to be compromised and require continuous monitoring and remediation.
- Adopt an adaptive security architecture for protection from advanced threats using Gartner's 12 critical capabilities as the framework.
- Spend less on prevention; invest in detection, response and predictive capabilities.
- Favor context-aware network, endpoint and application security protection platforms from vendors that provide and integrate prediction, prevention, detection and response capabilities.

What else should we be investing on?

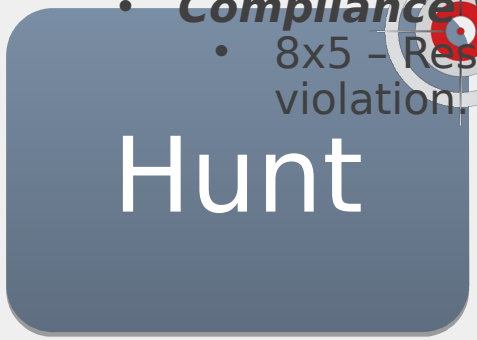


Cyber Defense Center

from monitoring to hunting (from reactive to proactive)

- ***Cyber Security Attack Monitoring***:
  - 24x7 - Real Time monitor of network devices and endpoints
  - 24x7 – intelligence monitoring
- ***Compliance Monitoring***:
  - 8x5 - Monitoring of system compliance to company/industry/national standards.

- ***Cyber Threat Intelligence:***
  - *Produce and consume threat intelligence*
- ***Incident Response:***
  - 8x5 - Monitoring of system compliance to company standards.
- ***Compliance Violation Response:***
  - 8x5 – Response to policy violation.



Use advanced technique to hunt for incidents:

- ***Trending***
- ***Hunting***
- ***Honeypotting***

Cyber Threat Analysis Cell
advanced services at the right time

- In order to benefit from such services:
  - Monitoring related services are required
  - Effective incident response procedures are required
  - A “stable” environment is required

Thank you!