PREVENTION IS BETTER THAN CURE

paloalto NETWORKS®




JAMIE BRUMMELL

Are our cyber adversaries winning?

Scottrade breach exposed 4.6M customer records

Over 600M Financial Records Stolen from 2013-2015

FSI is one of the top 3 industries for security incidents

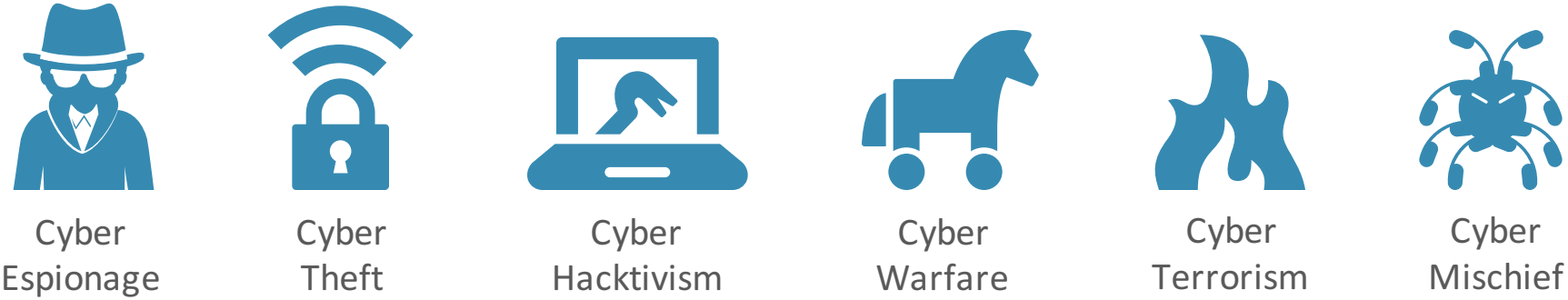
- **Trailing only Government and Media**
- **Accounted for ~35% of confirmed data breaches**

Verizon Data Breach Investigations Report

1.5M Accounts Exposed in Global Payments Breach

83M Records Stolen in JPMorgan Chase Breach

Motivations may vary…



but the fact is…

CYBERCRIME IS NOW A

£700bn+

BOOMING INDUSTRY

why are our cyber adversaries winning?

anatomy of a **data breach**

But first…. Some Terminology

- **Vulnerability**
  - A weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product
- **Exploit**
  - A piece of software, a chunk of data, or a sequence of commands that causes unintended or unanticipated behaviour to occur on software or hardware
- **Malware**
  - An umbrella term used to refer to a variety of forms of hostile or intrusive software
- **Patch**
  - Software security patches (attempt to) fix vulnerabilities that might be exploited
- **Code Execution**
  - An ability that allows an attacker to execute their own code on the victim machine

*"An attacker uses an **exploit** against a **vulnerability,** on an un**patch**ed system, to obtain **code execution,** often resulting in the installation of **malware"***

Step 1: Reconnaissance

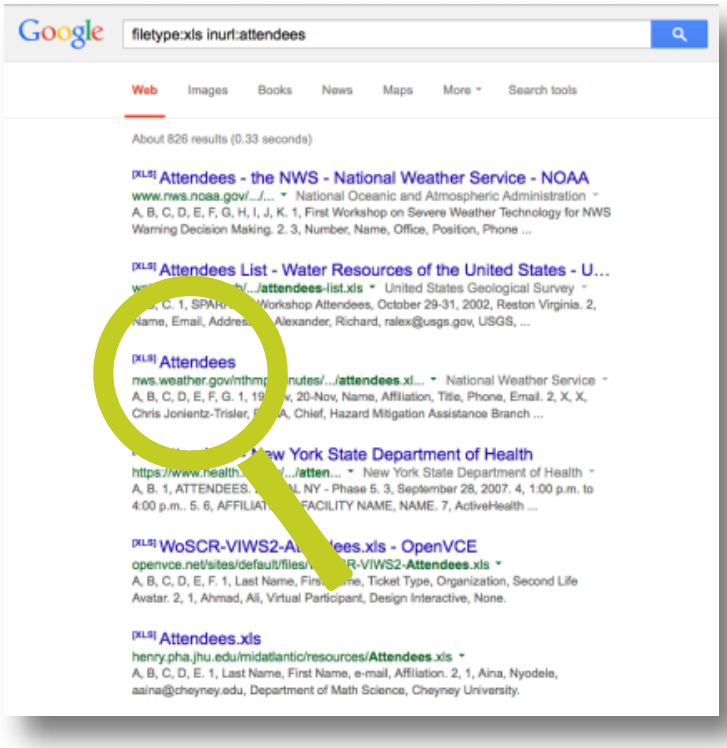
Identify a specific target within an organisation:

- Content from corporate websites
- Third-party sites to identify key targets
- Common search techniques

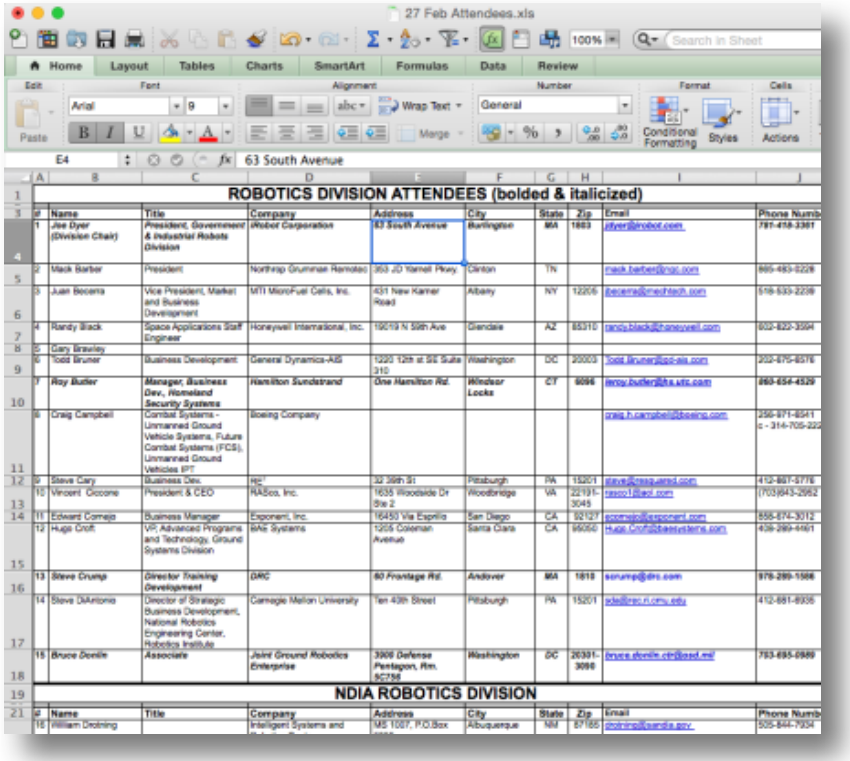
Step 1: Reconnaissance

Simple Google Search

`filetype:xls inurl:attendees`

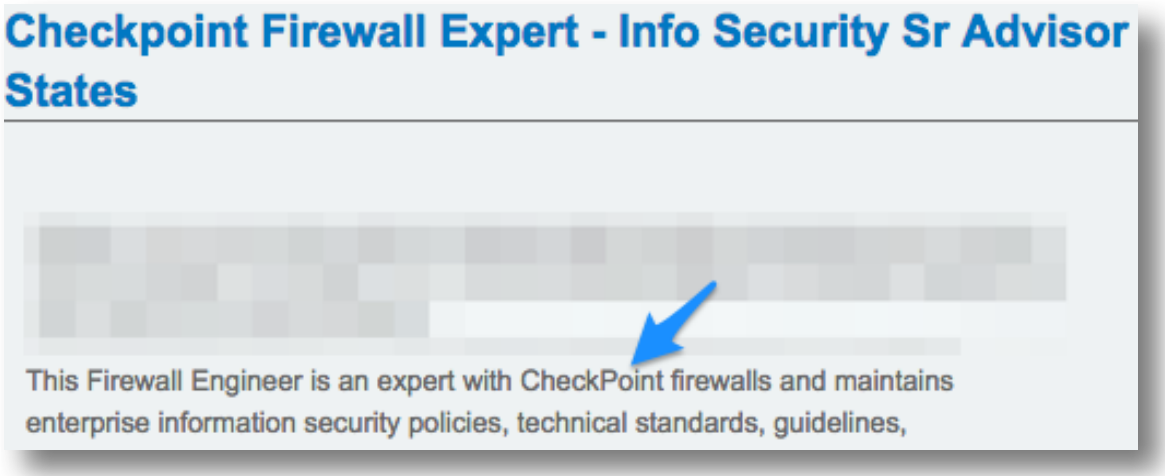


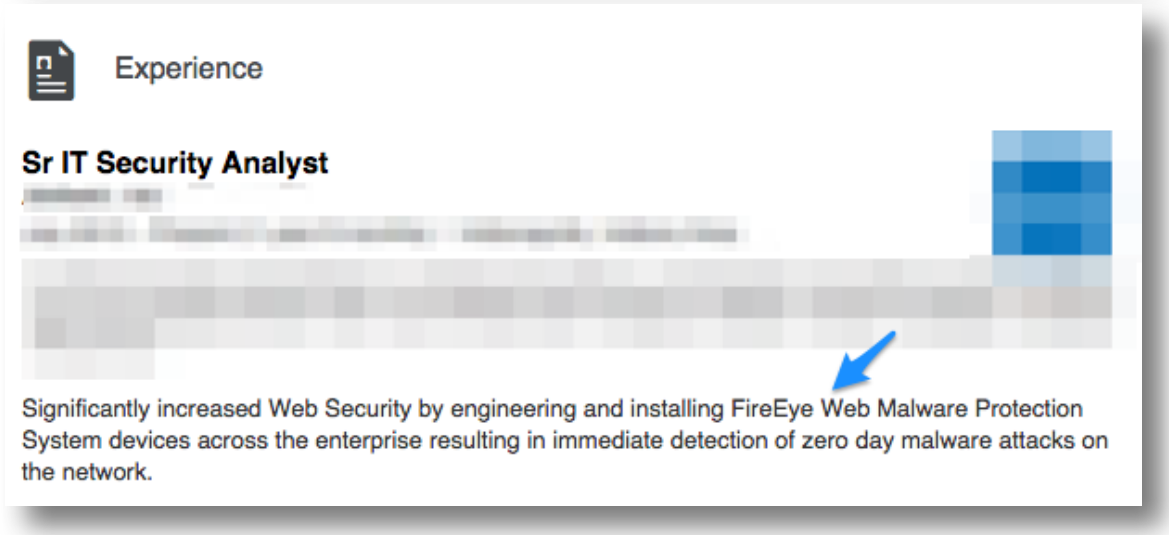
Event attendee contact details



Step 1: Reconnaissance

Identify the tools used to protect an organisation





Step 2: Weaponisation & Delivery

Spear Phishing

Attack a with a specific target

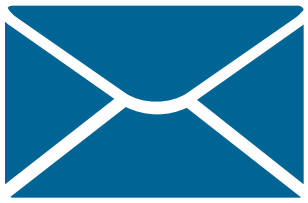
Watering Hole

Attack a group with specific interests

Everything Else

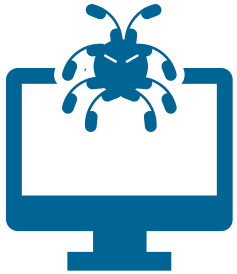
USB stick, direct network attack etc

Step 2: Weaponisation & Delivery: Spear Phishing + Drive-by Download



1 Targeted malicious email sent to user

2 User clicks on link to a malicious website



3 Malicious website silently uses exploit kit against a client-side vulnerability

4 'Drive-by download' of malicious payload

5 System infected, attacker has full access

Step 2: Weaponisation & Delivery: Watering hole + Drive-by Download

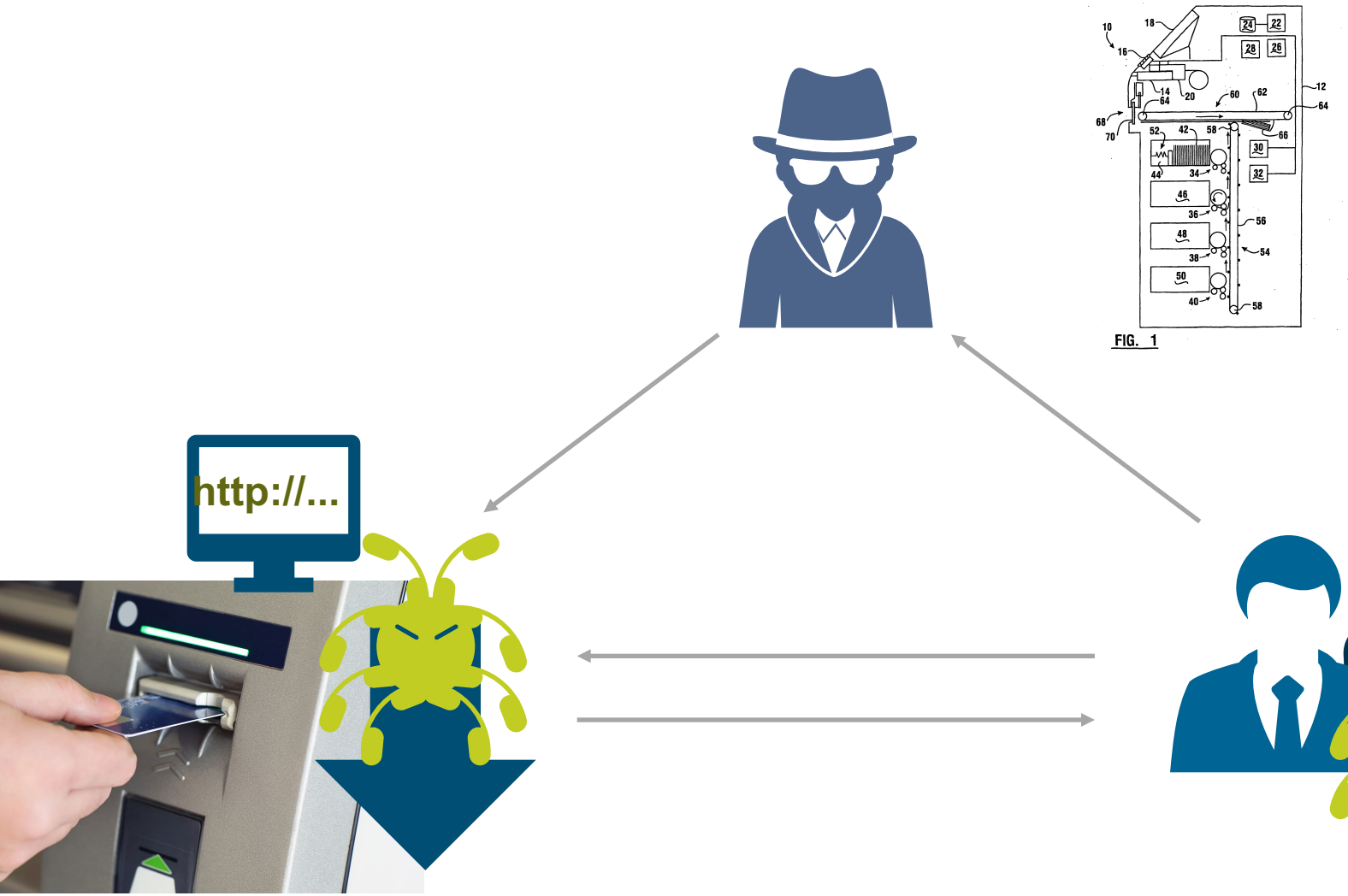


FIG. 1

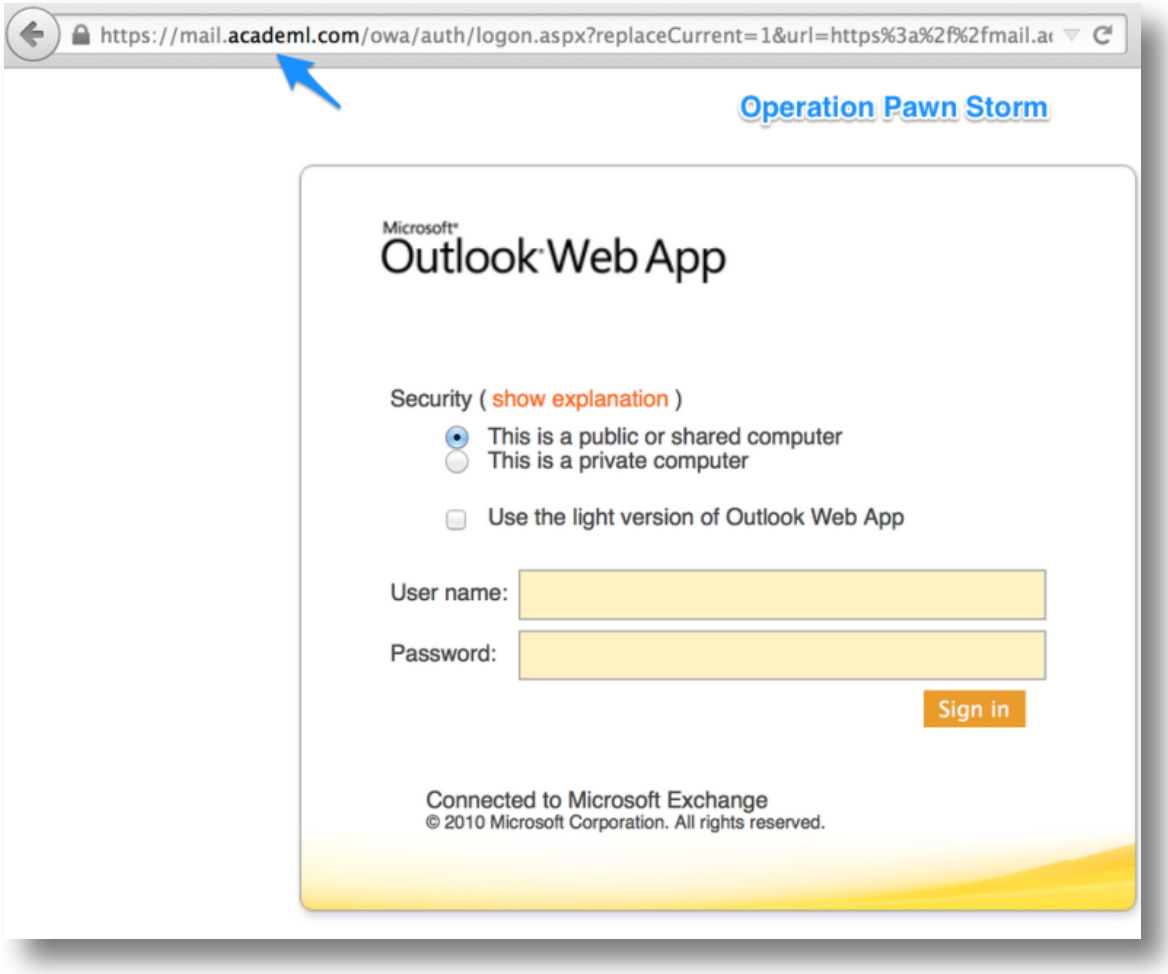
Step 2: Weaponisation & Delivery

Step 3: Exploitation

Exploiting the user

Why use malware when you have legitimate credentials?

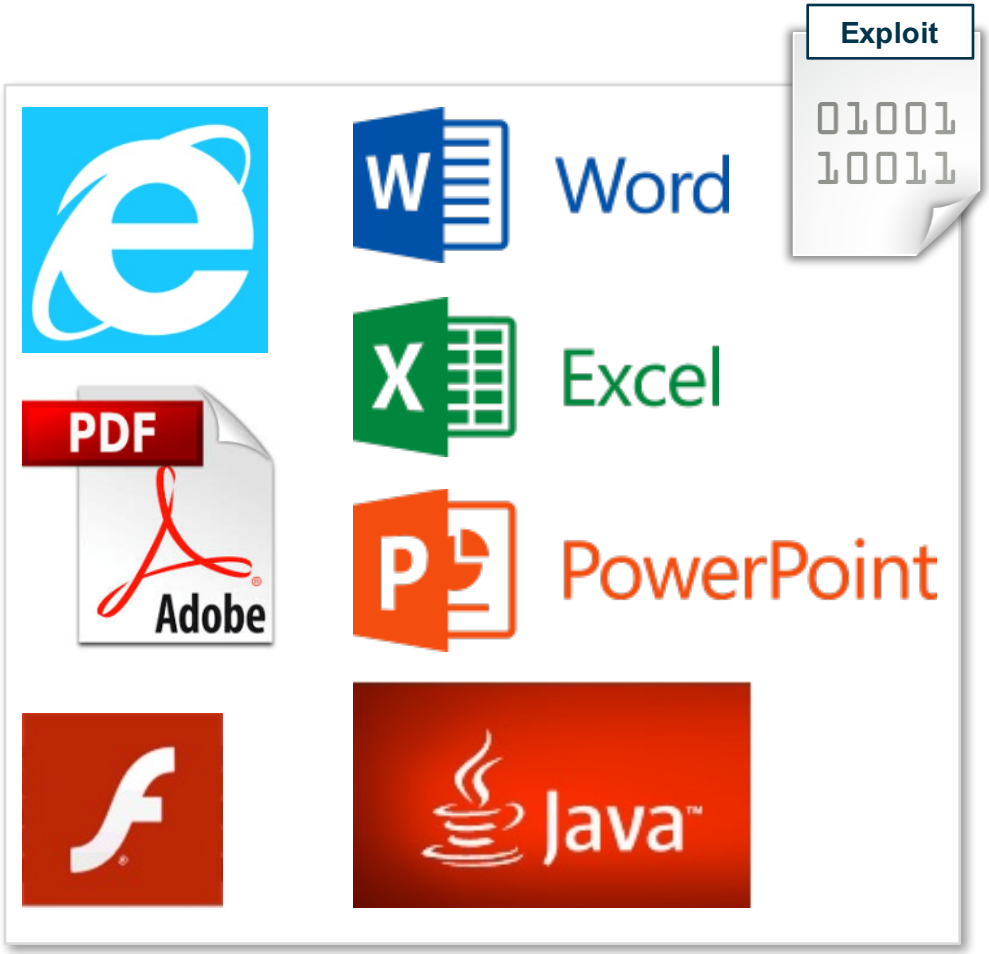
Users are typically the path of least resistance



Step 3: Exploitation

Exploiting software

Why use a valuable, previously unknown exploit (aka ‘0-day’) when old vulnerabilities may not be patched?



Step 4: Installation

Myth

Highly customised and unique tools are used for most attacks

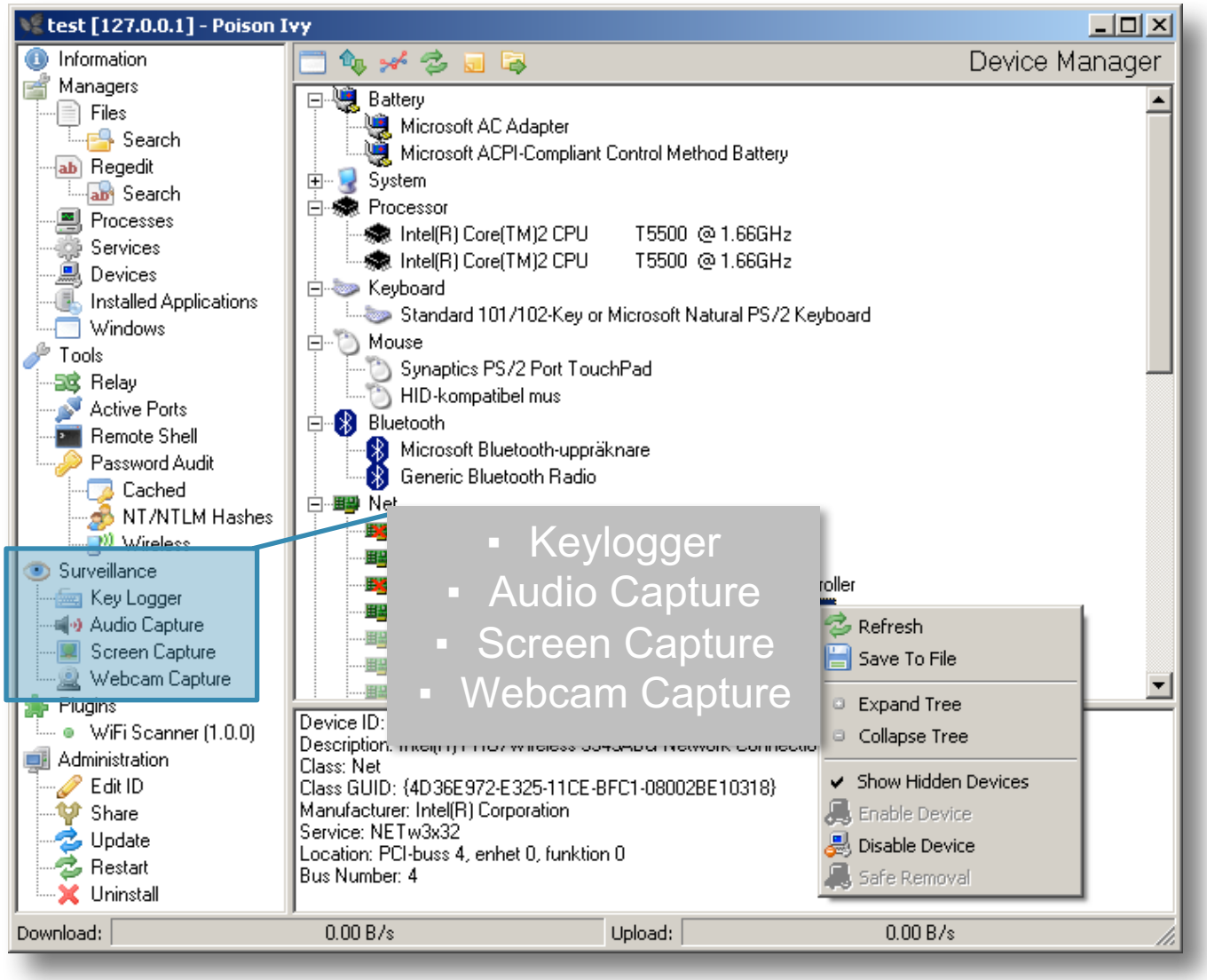
OR

Reality

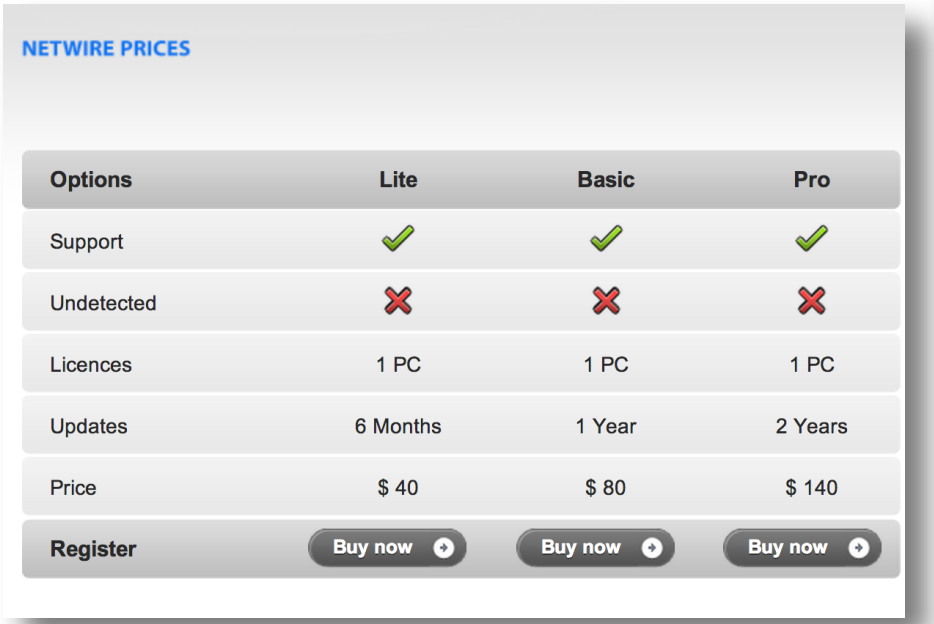
'Off-the-shelf' tools are most commonly used in an attack

?

Step 4: Installation

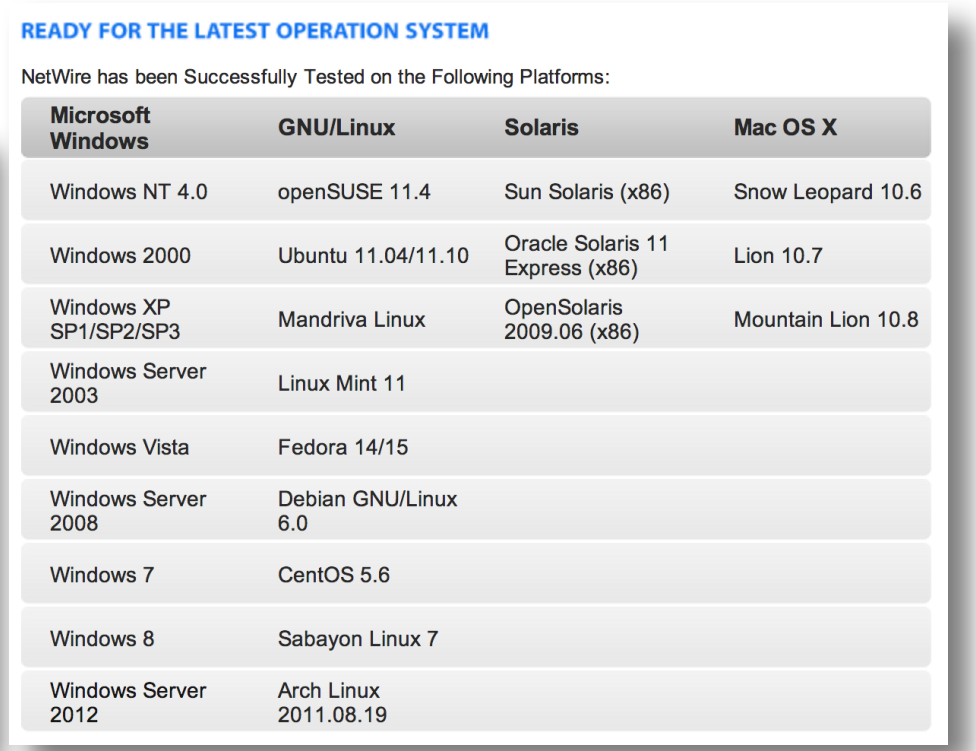


Step 4: Installation



NETWIRE PRICES

Options	Lite	Basic	Pro
Support	✓	✓	✓
Undetected	✗	✗	✗
Licences	1 PC	1 PC	1 PC
Updates	6 Months	1 Year	2 Years
Price	$ 40	$ 80	$ 140
Register	Buy now	Buy now	Buy now



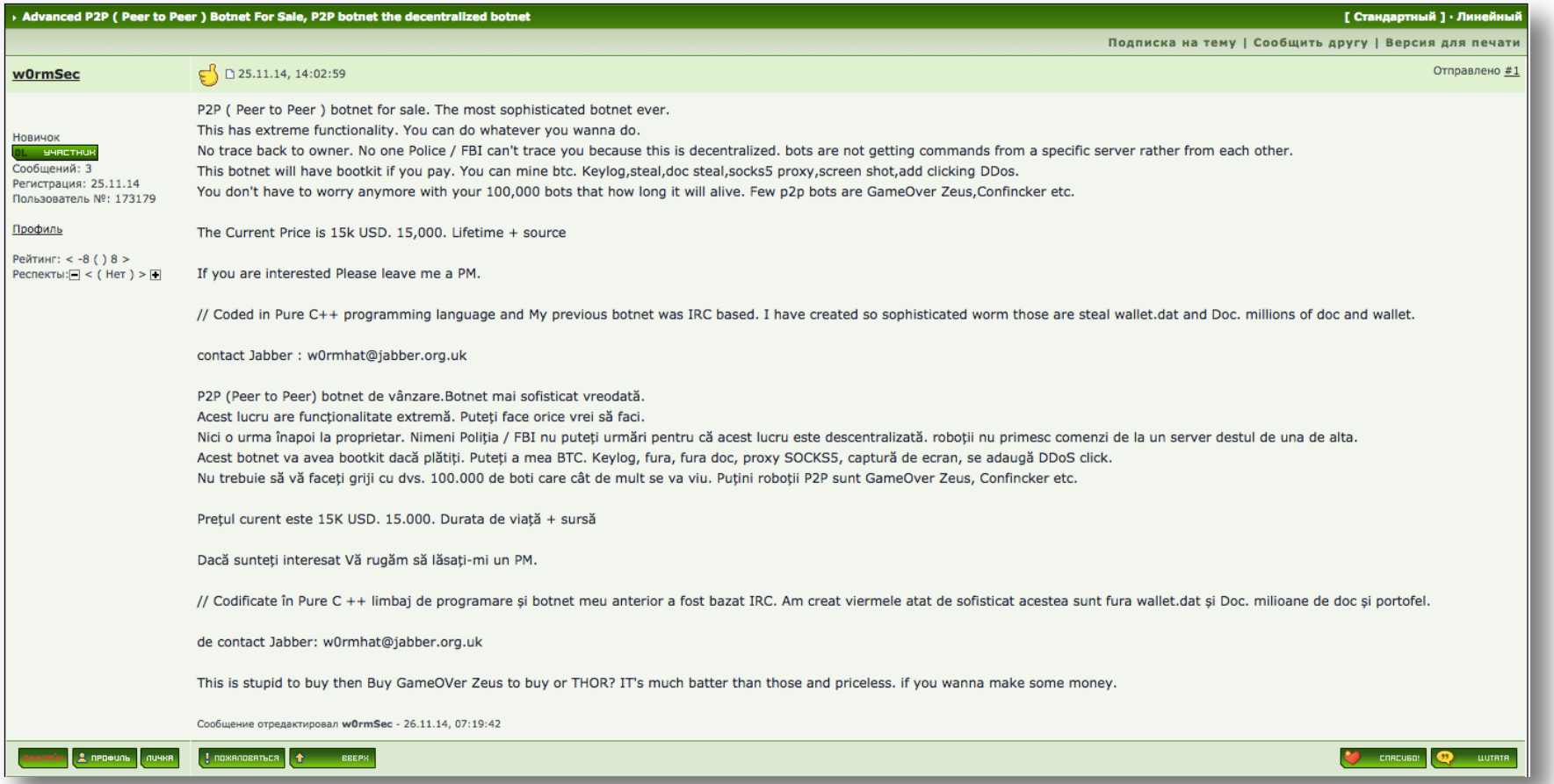
READY FOR THE LATEST OPERATION SYSTEM

NetWire has been Successfully Tested on the Following Platforms:

Microsoft Windows	GNU/Linux	Solaris	Mac OS X
Windows NT 4.0	openSUSE 11.4	Sun Solaris (x86)	Snow Leopard 10.6
Windows 2000	Ubuntu 11.04/11.10	Oracle Solaris 11 Express (x86)	Lion 10.7
Windows XP SP1/SP2/SP3	Mandriva Linux	OpenSolaris 2009.06 (x86)	Mountain Lion 10.8
Windows Server 2003	Linux Mint 11		
Windows Vista	Fedora 14/15		
Windows Server 2008	Debian GNU/Linux 6.0		
Windows 7	CentOS 5.6		
Windows 8	Sabayon Linux 7		
Windows Server 2012	Arch Linux 2011.08.19		

Buy ready-made, malicious software with 2 years support for only $140!

Step 4: Installation



› Advanced P2P (Peer to Peer) Botnet For Sale, P2P botnet the decentralized botnet [Стандартный] · Линейный

Подписка на тему | Сообщить другу | Версия для печати

w0rmSec 25.11.14, 14:02:59 Отправлено #1

Новичок
01 УЧАСТНИК
Сообщений: 3
Регистрация: 25.11.14
Пользователь №: 173179

Профиль

Рейтинг: < -8 ( ) 8 >
Респекты: < (Нет) >

P2P (Peer to Peer) botnet for sale. The most sophisticated botnet ever.
This has extreme functionality. You can do whatever you wanna do.
No trace back to owner. No one Police / FBI can't trace you because this is decentralized. bots are not getting commands from a specific server rather from each other.
This botnet will have bootkit if you pay. You can mine btc. Keylog,steal,doc steal,socks5 proxy,screen shot,add clicking DDos.
You don't have to worry anymore with your 100,000 bots that how long it will alive. Few p2p bots are GameOver Zeus,Confincker etc.

The Current Price is 15k USD. 15,000. Lifetime + source

If you are interested Please leave me a PM.

// Coded in Pure C++ programming language and My previous botnet was IRC based. I have created so sophisticated worm those are steal wallet.dat and Doc. millions of doc and wallet.

contact Jabber : w0rmhat@jabber.org.uk

P2P (Peer to Peer) botnet de vânzare.Botnet mai sofisticat vreodată.
Acest lucru are funcționalitate extremă. Puteți face orice vrei să faci.
Nici o urma înapoi la proprietar. Nimeni Poliția / FBI nu puteți urmări pentru că acest lucru este descentralizată. roboții nu primesc comenzi de la un server destul de una de alta.
Acest botnet va avea bootkit dacă plătiți. Puteți a mea BTC. Keylog, fura, fura doc, proxy SOCKS5, captură de ecran, se adaugă DDoS click.
Nu trebuie să vă faceți griji cu dvs. 100.000 de boti care cât de mult se va viu. Puțini roboții P2P sunt GameOver Zeus, Confincker etc.

Prețul curent este 15K USD. 15.000. Durata de viață + sursă

Dacă sunteți interesat Vă rugăm să lăsați-mi un PM.

// Codificate în Pure C ++ limbaj de programare și botnet meu anterior a fost bazat IRC. Am creat viermele atat de sofisticat acestea sunt fura wallet.dat și Doc. milioane de doc și portofel.

de contact Jabber: w0rmhat@jabber.org.uk

This is stupid to buy then Buy GameOVer Zeus to buy or THOR? IT's much batter than those and priceless. if you wanna make some money.

Сообщение отредактировал **w0rmSec** - 26.11.14, 07:19:42

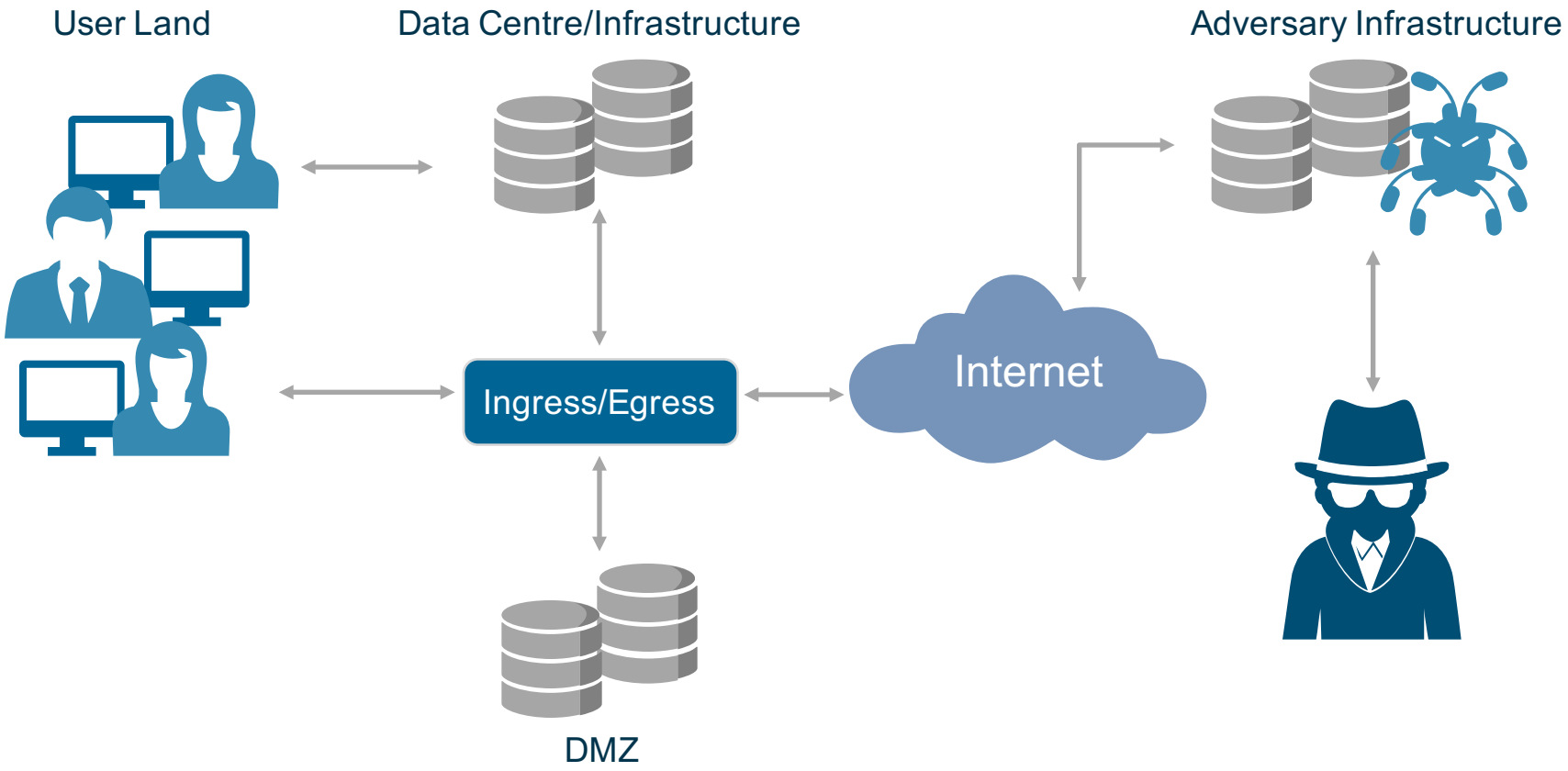
ПРОФИЛЬ ЛИЧКА ПОЖАЛОВАТЬСЯ ВВЕРХ СПАСИБО! ЦИТАТА

Or buy a massive, ready-made malware network for $15k!

paloalto NETWORKS

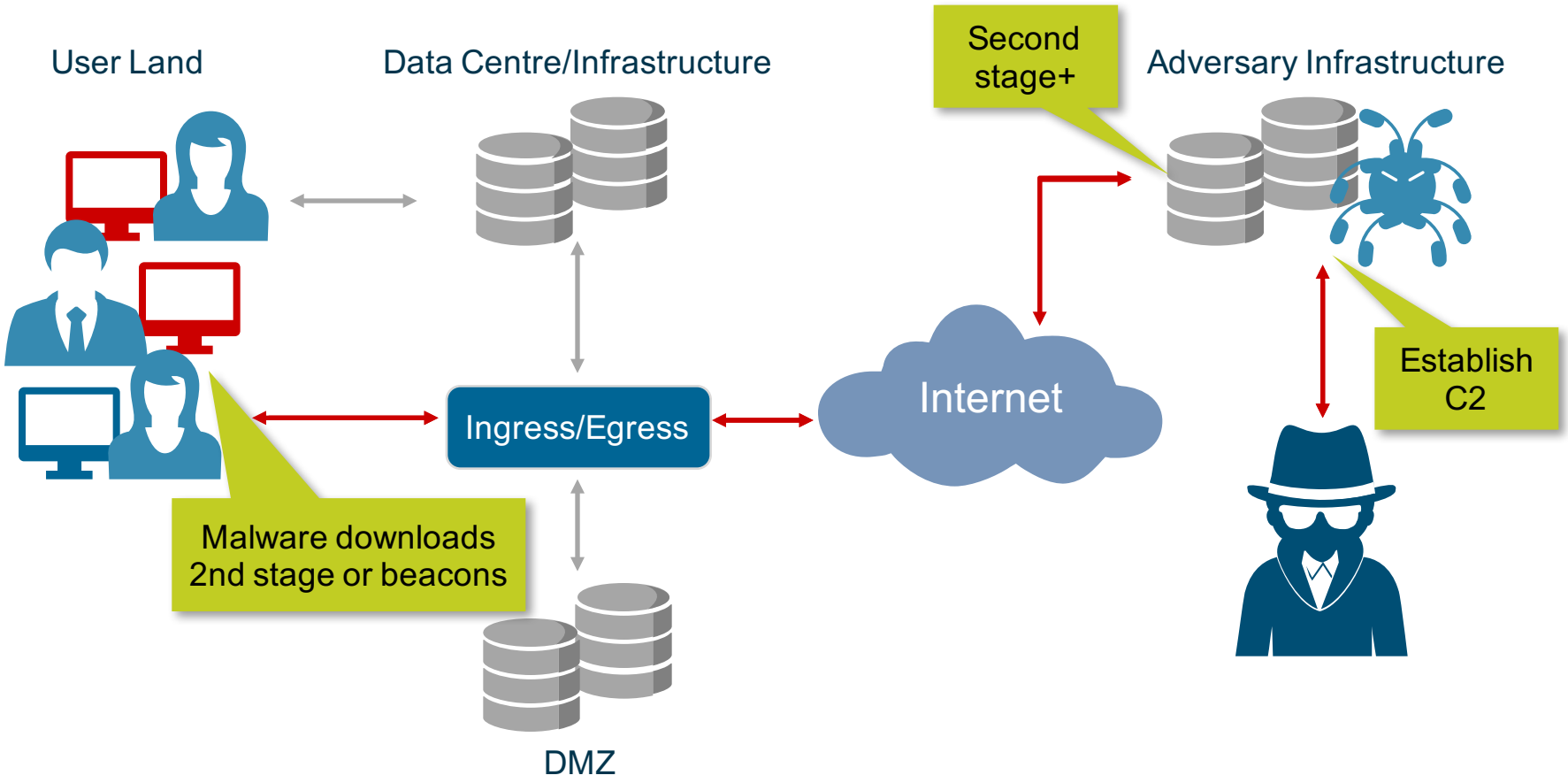
Step 5: Command and Control (aka ‘C2' or ‘CnC’)

Communicating with infected hosts and providing instructions



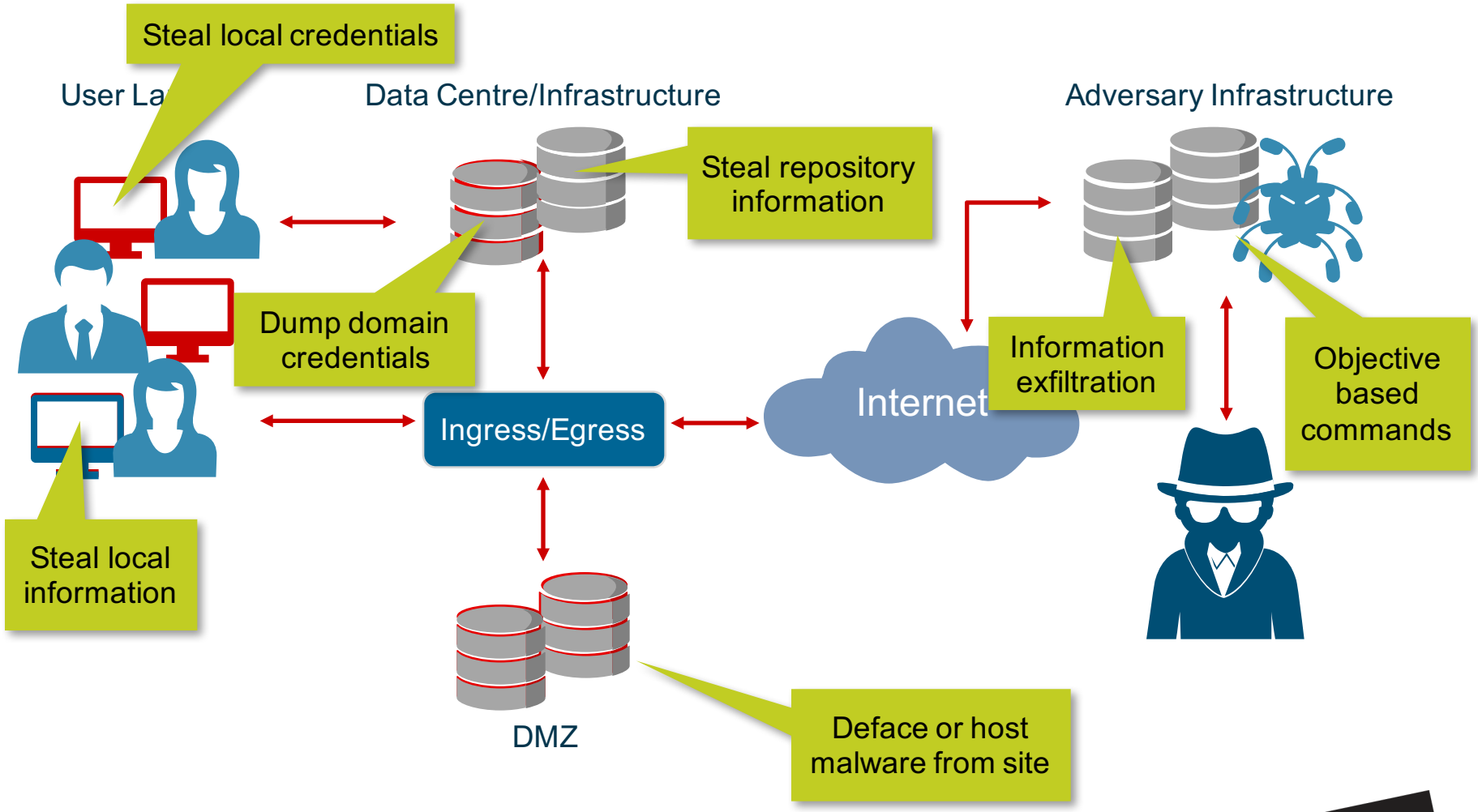
Step 5: Command and Control (aka ‘C2' or ‘CnC’)

2nd stage malware download and establish C2 channel

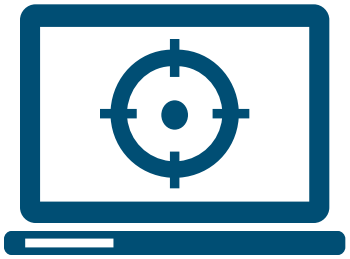


Step 6: Actions on Objectives

C2 ultimately enables the attacker's endgame: Actions on Objectives



Step 6: Actions on the Objective

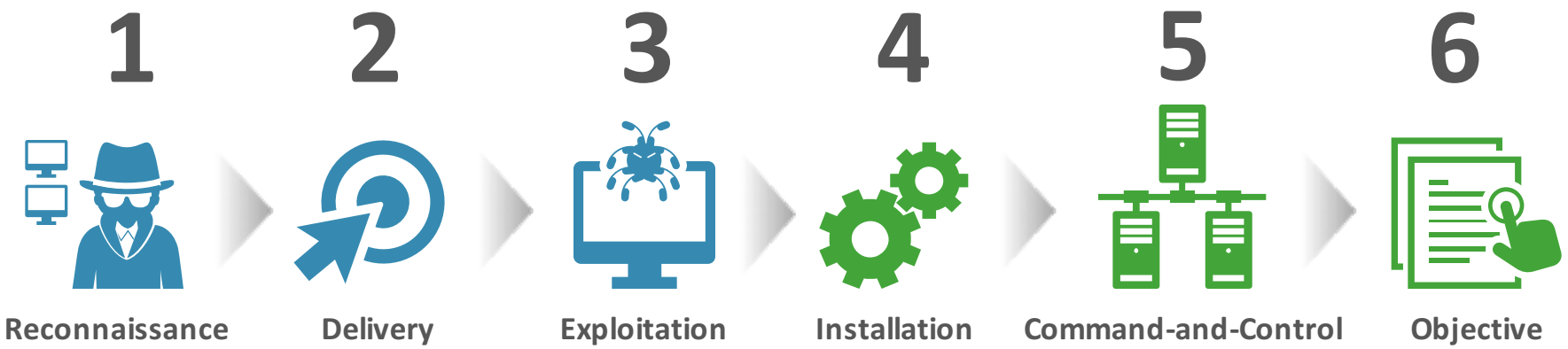


Goals Inside the Network

Completed by an Active Operator

Your data in their hands

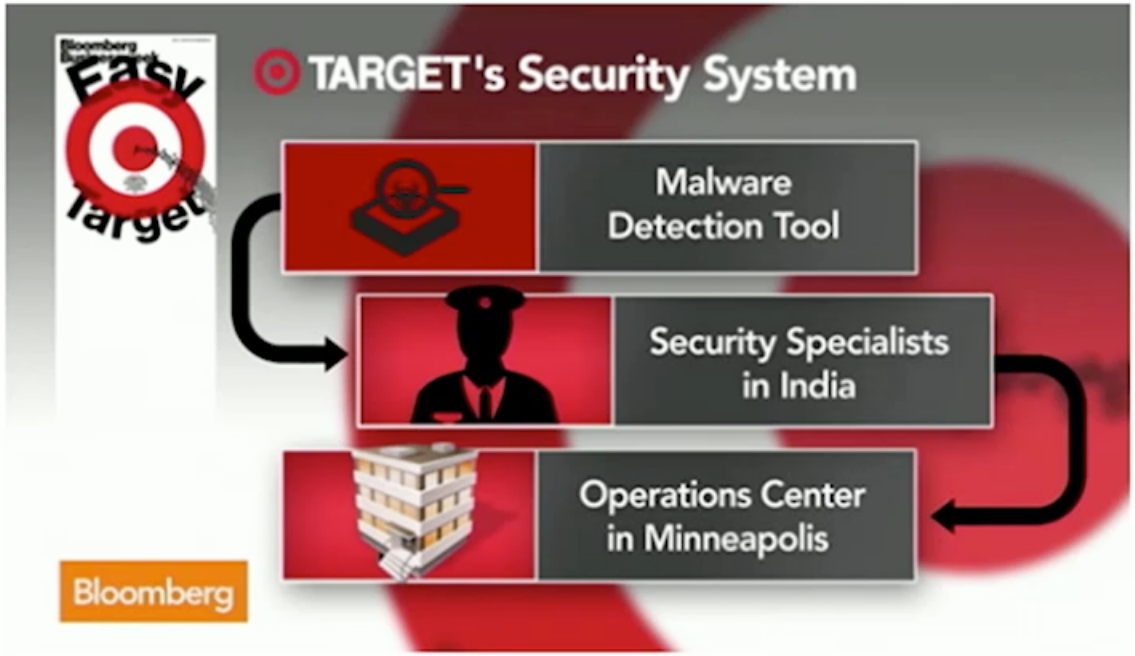
Prevention Opportunities in the Cyber Attack Lifecycle



…so what have we been doing wrong?

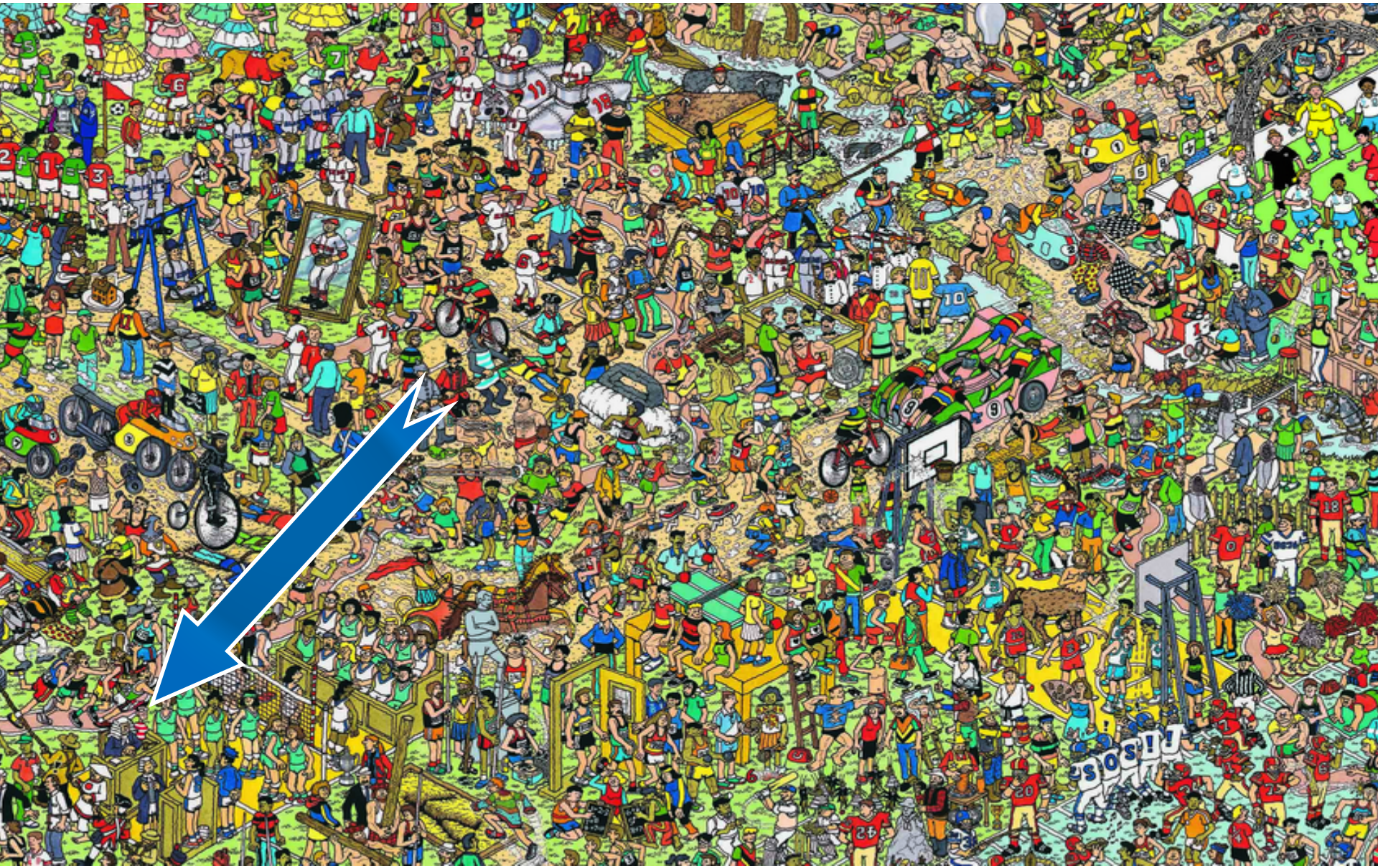
Legacy Whack-a-Mole Security

We mistakenly shift focus to detection and remediation



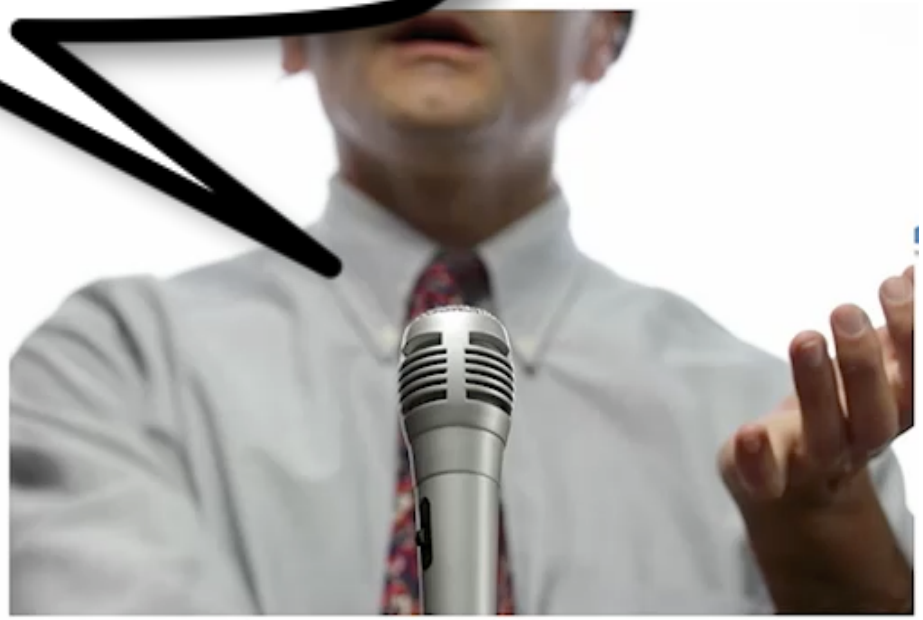
http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

paloalto NETWORKS



paloalto NETWORKS®

“The Home Office has determined that preventing attacks on our streets is futile and is therefore shifting investment to crime scene cleanup and timely restoration of normal life"



paloalto NETWORKS®

a new approach to prevention

1: Be Positioned to Prevent

On the Endpoint, anywhere it resides

At the Internet Edge and Partner Edge

Between our Employees Devices inside the network

At the Data Centre Edge and between servers

Within Private, Public, Hybrid Clouds and SaaS platforms

‘Zero Trust’ Approach

2: On the Endpoint: Prevent the Techniques - not the Attacks

Individual Attacks

1,000s

New Software Vulnerability Exploits p/a

1,000,000s

New Malware variants p/a

Core Techniques

2-4

New Exploitation Techniques p/a

~10s

New Malware Techniques p/a

Signature-based, AV technology is ineffective against unknown threats

3: We need Automation

4: We must share Threat Intelligence with our peers

FINANCIAL SERVICES Information Sharing and Analysis Center
AFFILIATE

- Global resource for cyber threat intelligence analysis and sharing for the Financial Services industry
- Distils threat information into actionable intelligence
- Palo Alto Networks is establishing automation to consume and share threat intelligence with the FS-ISAC and its members

CYBER THREAT ALLIANCE

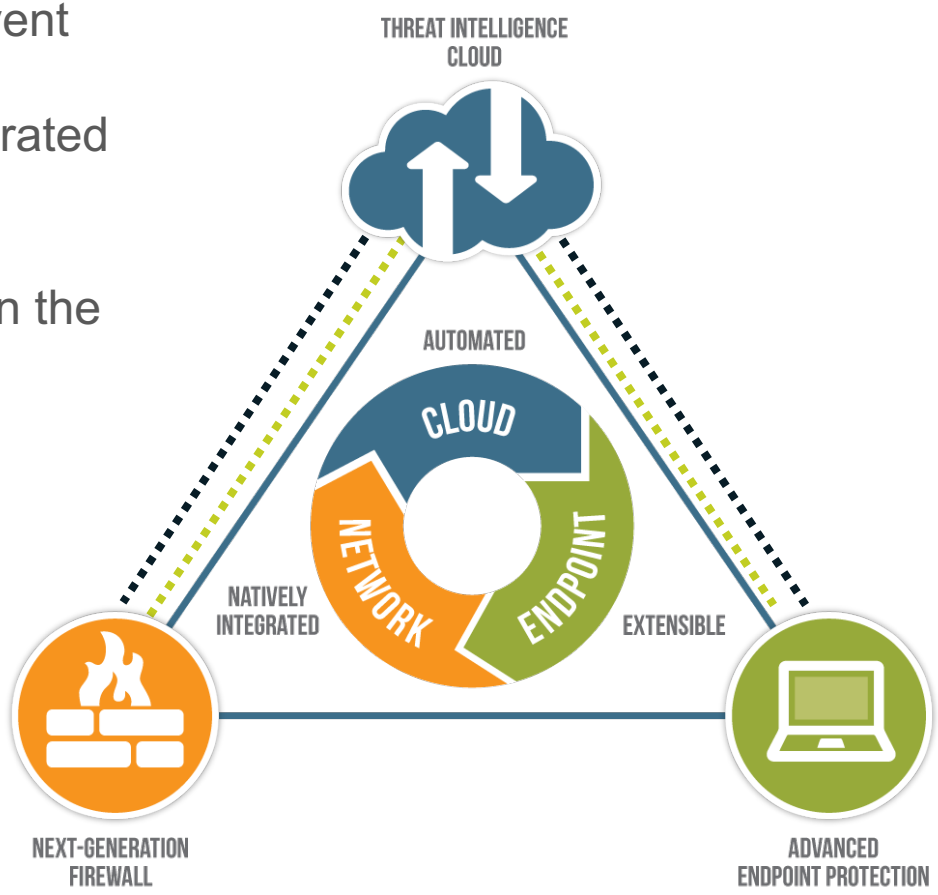
- Co-founded by Palo Alto Networks to share threat intelligence among cyber-security solutions providers
- Leverage the shared intelligence to improve collective defences offered to their customers

www.securityroundtable.org - The Security Roundtable is a community designed to share best practices, use cases, and expert advice to guide executives on managing cybersecurity risks.

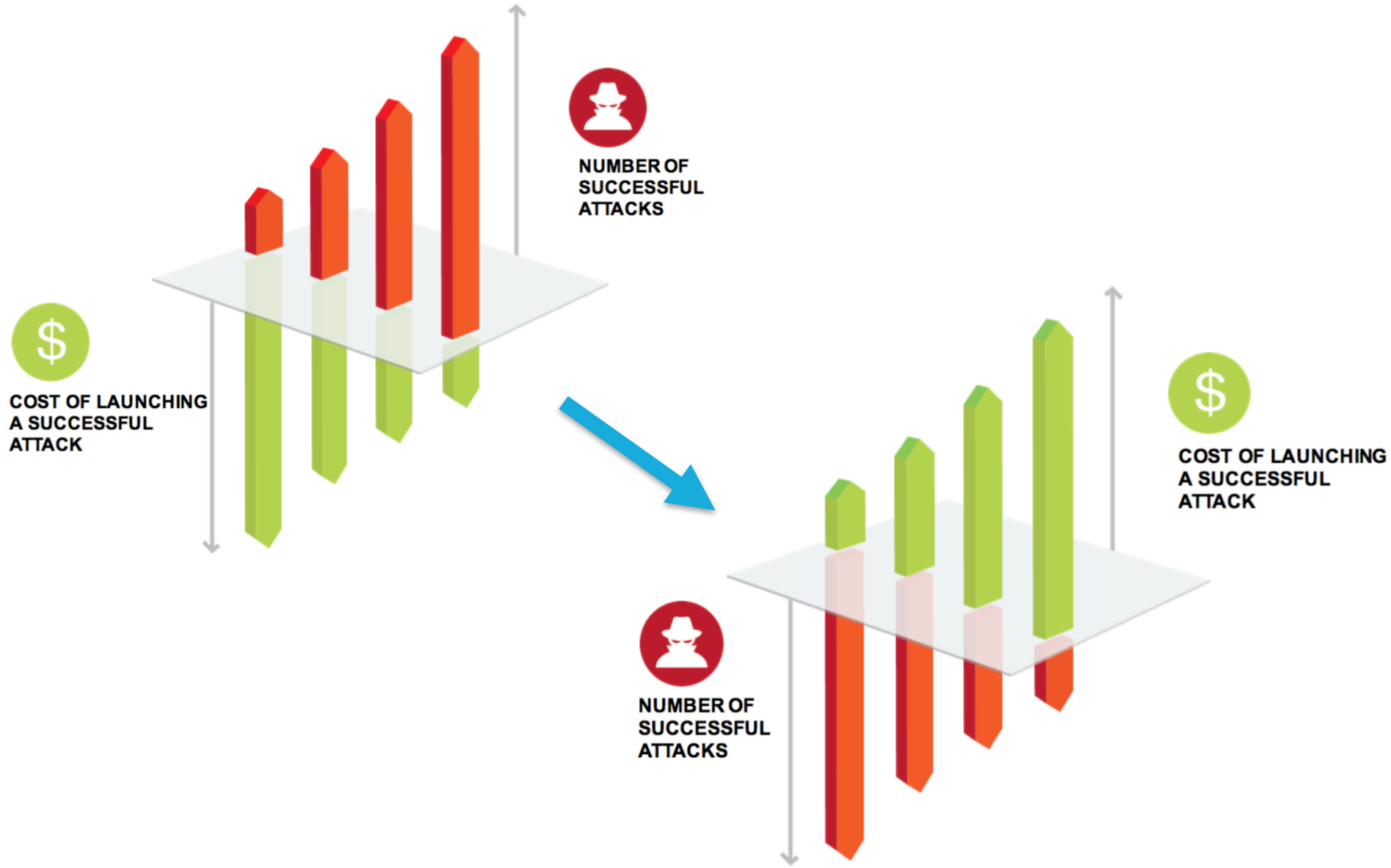
paloalto NETWORKS

Only an Integrated Platform can Prevent Cyber Attacks

- On the network and on the endpoints: Positioned to Prevent
- All components natively integrated and automated
- Driven by threat intelligence in the cloud



The End Result? We disrupt the attacker's business model

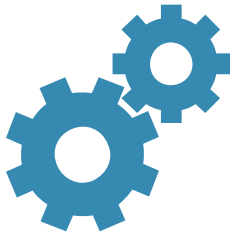



paloalto
NETWORKS®

the detail…

Preventing Delivery and Installation

Prevent malware and exploits at the network level



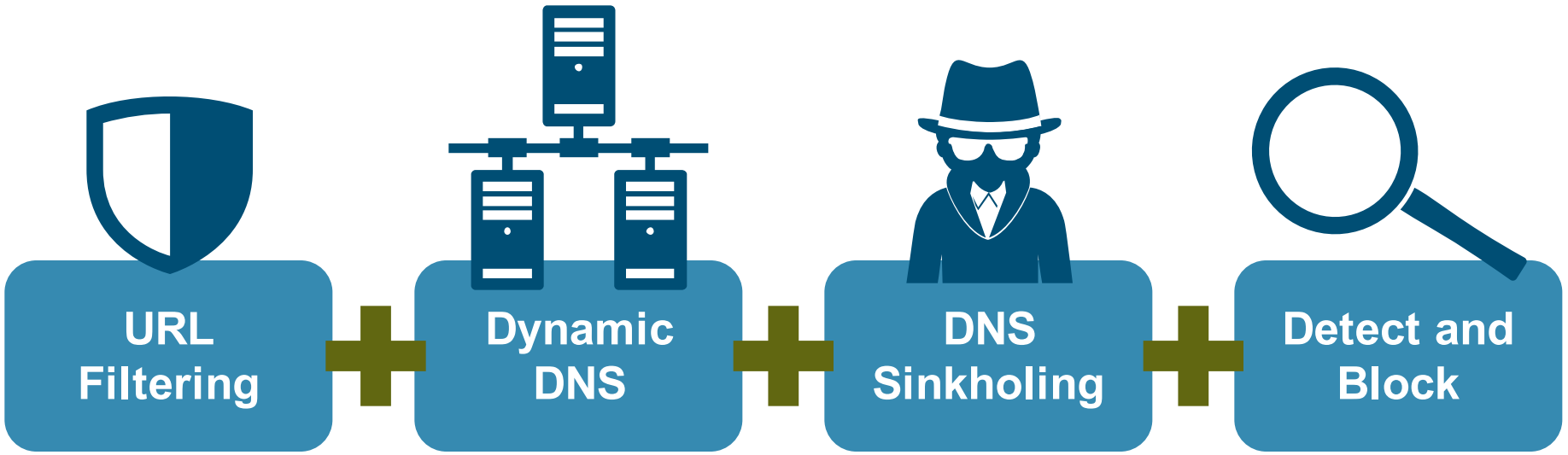
Deploy a solution that can detect new exploits and malware, dynamically updated your protections across AV, URL and DNS

Prevent exploits that have never been seen before on the endpoint

User-based policy such as limiting the download of executable files from the Internet

Block commonly exploited file-types on your network

Preventing Command-and-Control



Proactively Block Unknown and Undesirable websites

Block the Dynamic DNS URL category

Identify source of malicious DNS queries

Common RAT C2 signatures

paloalto NETWORKS

Preventing Attacks at Every Stage of the Attack Lifecycle

Breach the perimeter

Next-Generation Firewall / GlobalProtect

- Visibility into all traffic, including SSL
- Enable business-critical applications
- Block high-risk applications
- Block commonly exploited file types

Threat Prevention

- Block known exploits, malware and inbound command-and-control communications

URL Filtering

- Prevent use of social engineering
- Block known malicious URLs & IP addresses

Sandboxing (WildFire)

- Send specific incoming files and email links from the internet to public or private cloud for inspection
- Detect unknown threats
- Automatically deliver protections globally

Deliver the malware

Traps / Sandboxing (WildFire)

- Block known & unknown vulnerability exploits
- Block known and unknown malware
- Provide detailed forensics on attacks

Lateral movement

Next-Generation Firewall / GlobalProtect

- Establish secure zones with strictly enforced access control
- Provide ongoing monitoring and inspection of all traffic between zones

Sandboxing (WildFire)

- Detecting unknown threats pervasively throughout the network

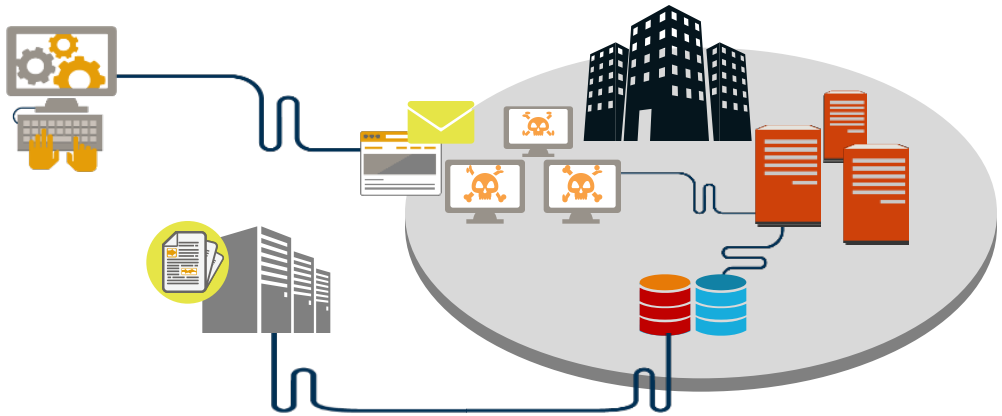
Exfiltrate data

Threat Prevention

- Block outbound command-and-control communications
- Block file and data pattern uploads
- DNS monitoring and sinkholing

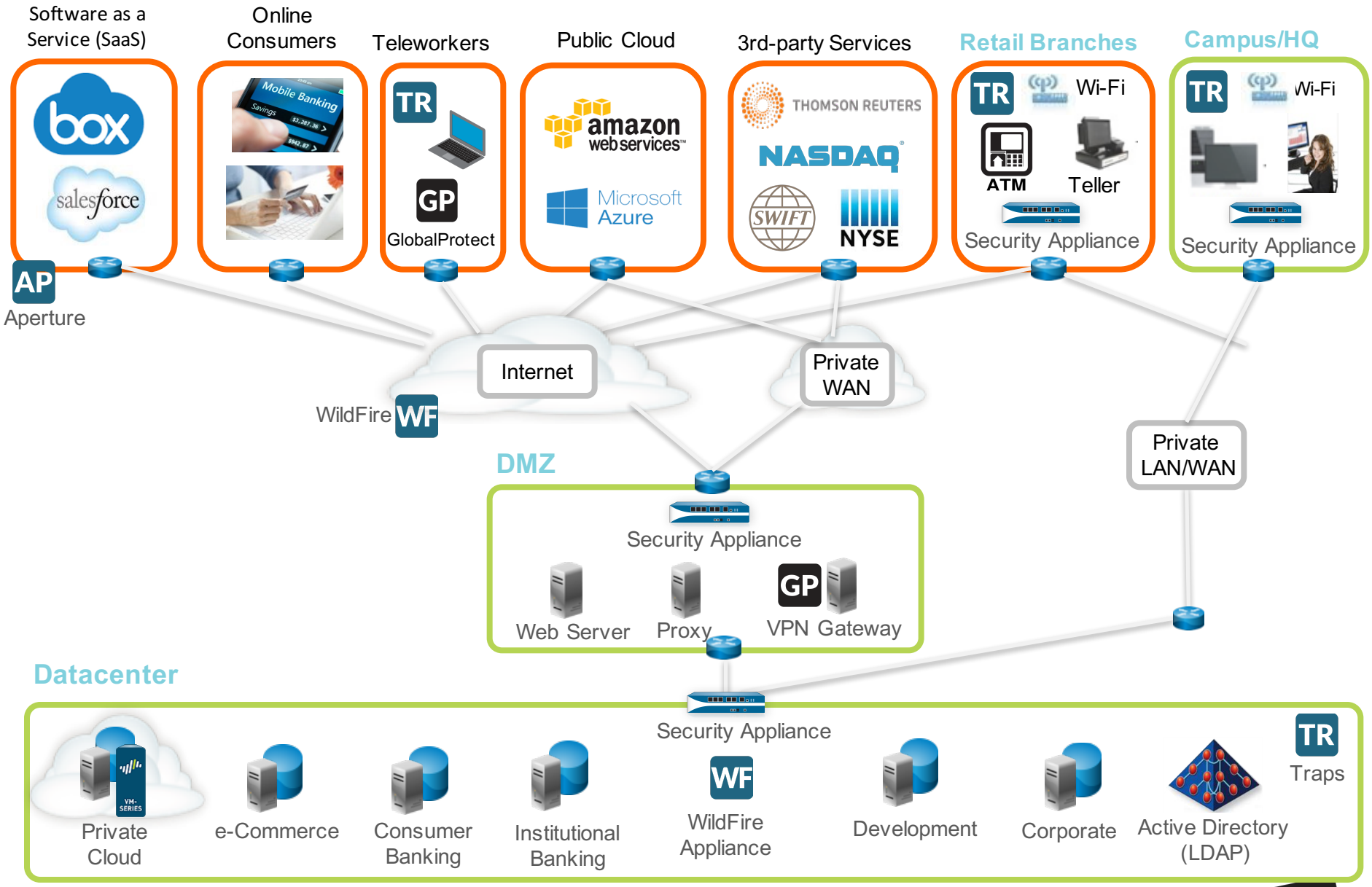
URL Filtering

- Block outbound communication to known malicious URLs and IP addresses



paloalto NETWORKS

FINANCIAL SERVICES REFERENCE BLUEPRINT



FINANCIAL SERVICES REFERENCE