Crack the Code: Defeat the Advanced Adversary

Stefania Iannelli

System Engineer - Palo Alto Networks

Milano 24 Maggio Villa Necchi Campiglio

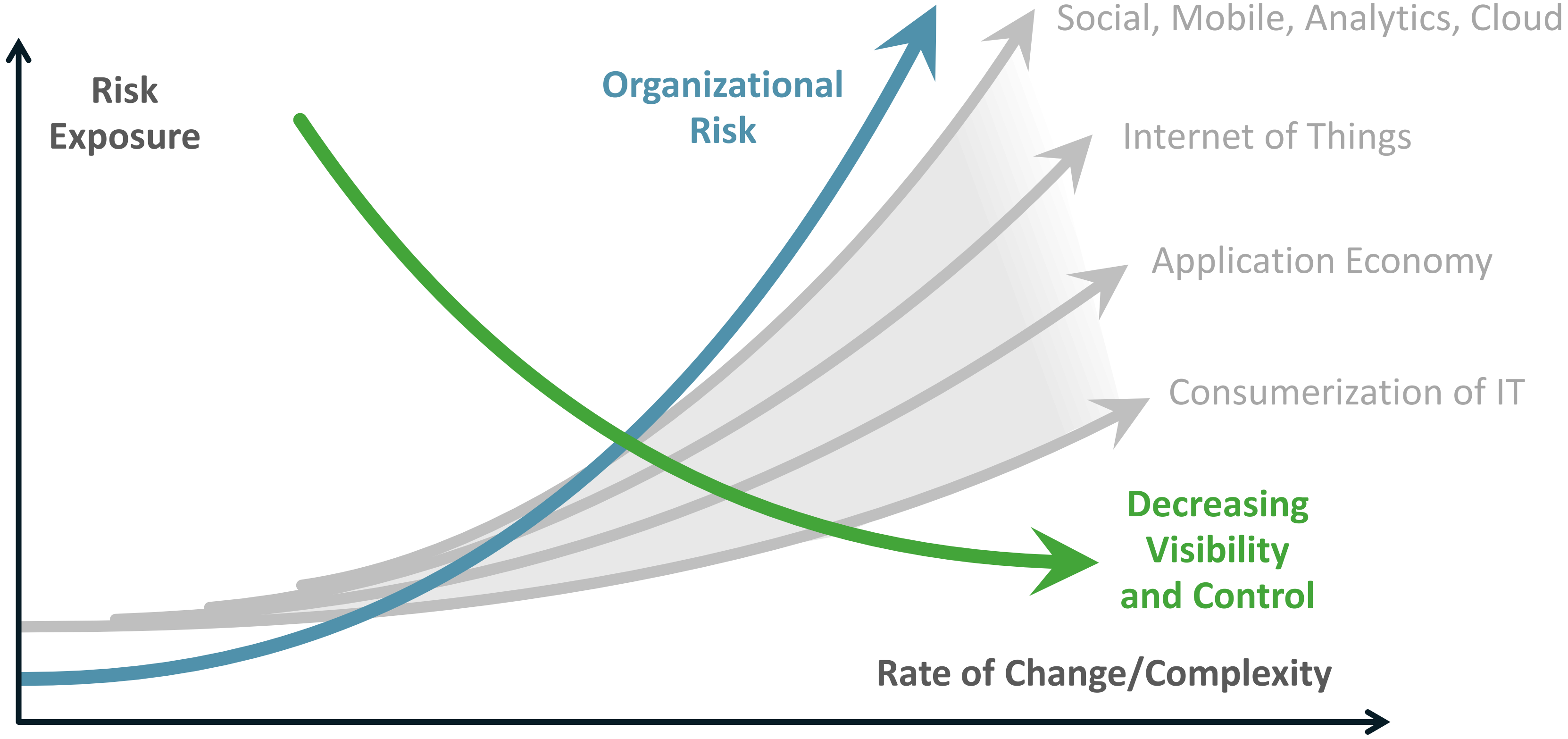
Key Perspectives

Who is the Adversary?

Understanding the Cyber Attack Lifecycle

How Attacks Happen

Challenges and Change Introduce Risks



Reliance on Multiple Layers of Service Providers

Exploring Actor Motivations

These are not mutually exclusive

Cyber Espionage

Cyber Crime

Cyber Hacktivism

Cyber Warfare

Cyber Terrorism

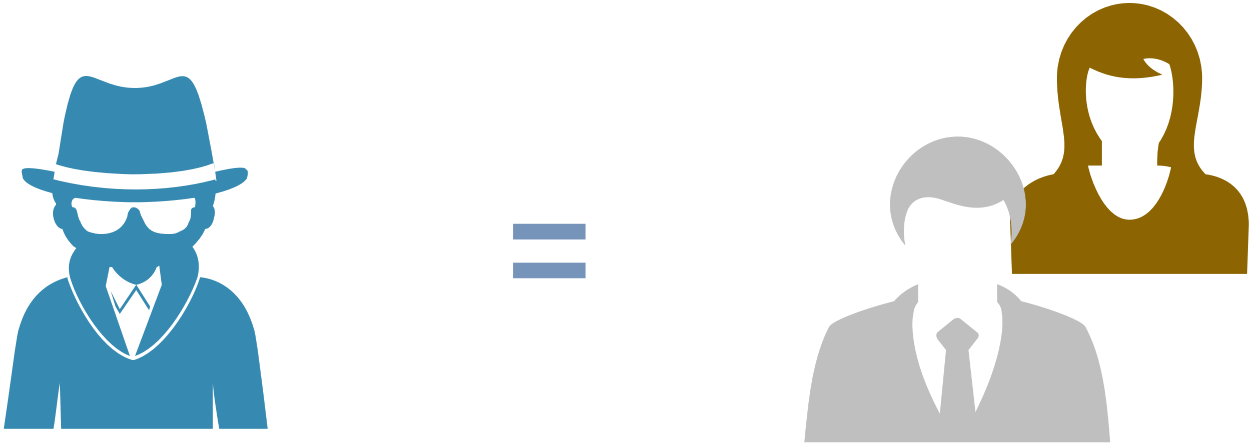
Cyber Mischief

$$$

The Advanced Adversary

Majority of adversaries are just doing their job:

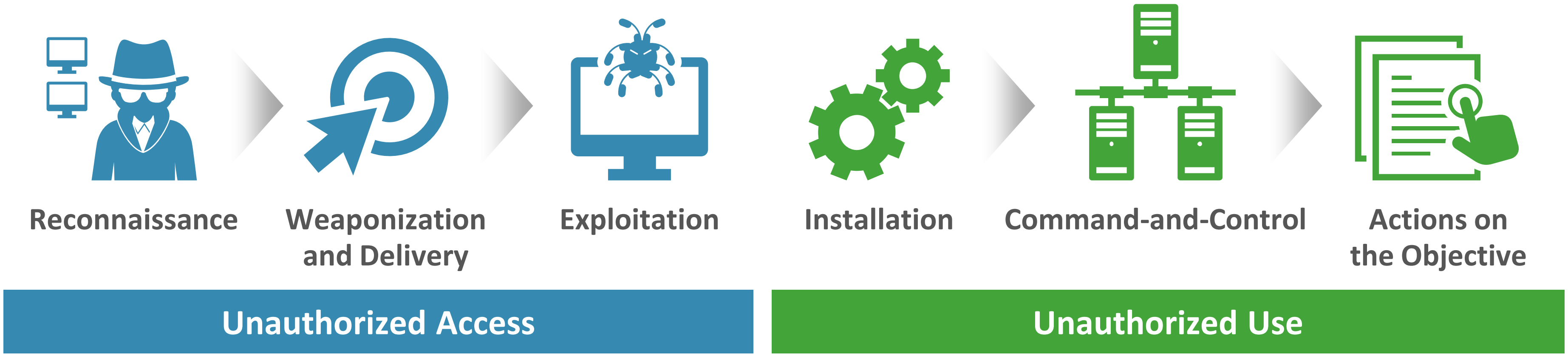
- Bosses, families, bills to pay.
- Want to get in, accomplish their task, and get out (un-detected).
- Goal isn’t making your life hard.



The Advanced Adversary

Increase the cost for adversaries.

Cyber Attack Lifecycle



Reconnaissance

Weaponization and Delivery

Exploitation

Installation

Command-and-Control

Actions on the Objective

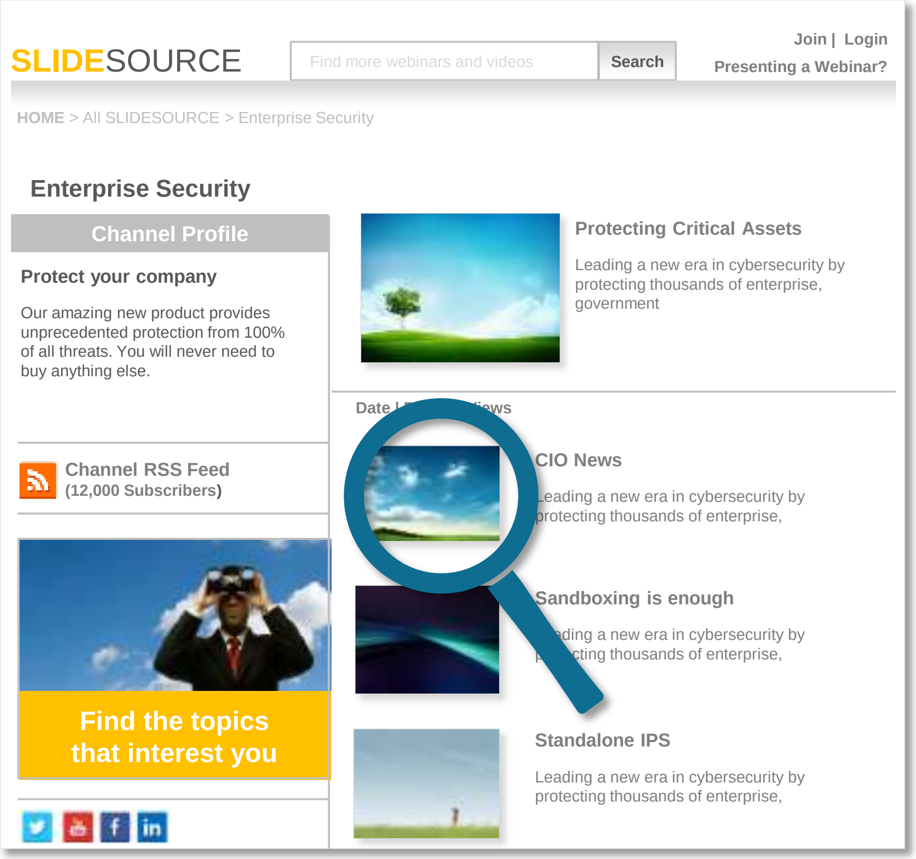
Unauthorized Access

Unauthorized Use

There is no predictable path for the advanced adversary.

Reconnaissance

Identify a specific target within an organization:



SLIDESOURCE

Find more webinars and videos | Search

Join | Login

Presenting a Webinar?

HOME > All SLIDESOURCE > Enterprise Security

Enterprise Security

Channel Profile

Protect your company

Our amazing new product provides unprecedented protection from 100% of all threats. You will never need to buy anything else.

Channel RSS Feed (12,000 Subscribers)

Find the topics that interest you

Protecting Critical Assets

Leading a new era in cybersecurity by protecting thousands of enterprise, government

Date | [illegible] Views

CIO News

Leading a new era in cybersecurity by protecting thousands of enterprise,

Sandboxing is enough

Leading a new era in cybersecurity by protecting thousands of enterprise,

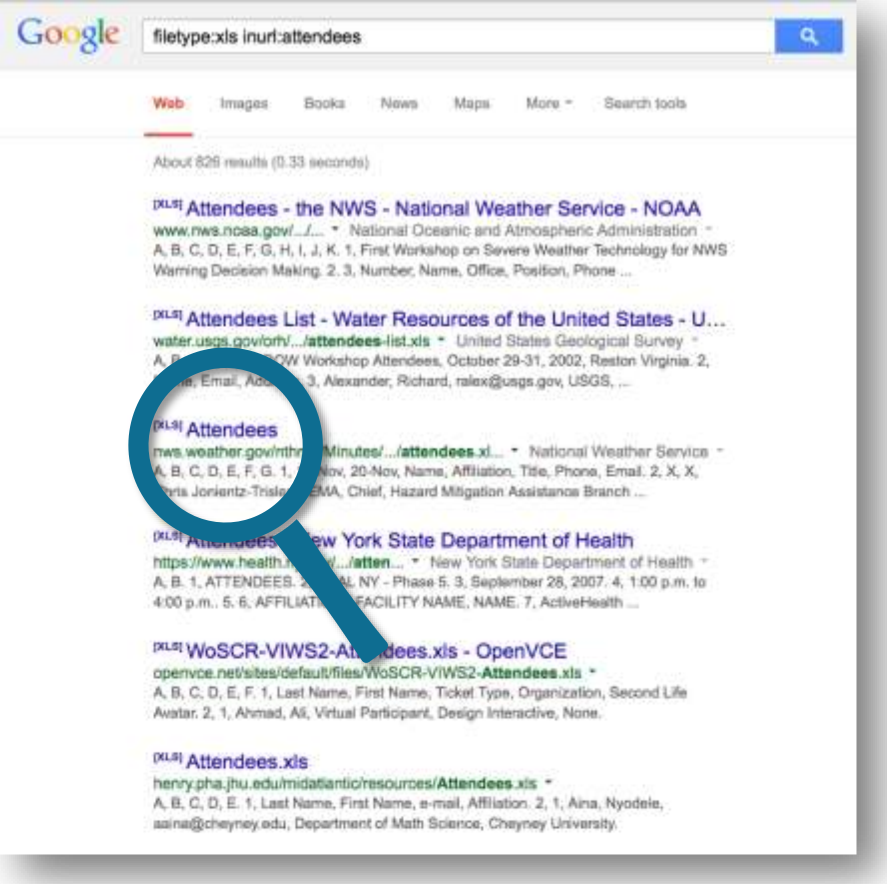
Standalone IPS

Leading a new era in cybersecurity by protecting thousands of enterprise,

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

Reconnaissance

Simple Google Search



filetype:xls inurl:attendees

About 826 results (0.33 seconds)

[XLS] Attendees - the NWS - National Weather Service - NOAA
www.nws.noaa.gov/.../... ▾ National Oceanic and Atmospheric Administration ▾
A, B, C, D, E, F, G, H, I, J, K. 1, First Workshop on Severe Weather Technology for NWS Warning Decision Making. 2. 3, Number, Name, Office, Position, Phone ...

[XLS] Attendees List - Water Resources of the United States - U...
water.usgs.gov/orh/.../attendees-list.xls ▾ United States Geological Survey ▾
A, B, ... OW Workshop Attendees, October 29-31, 2002, Reston Virginia. 2, ...e, Email, Add... 3, Alexander, Richard, ralex@usgs.gov, USGS, ...

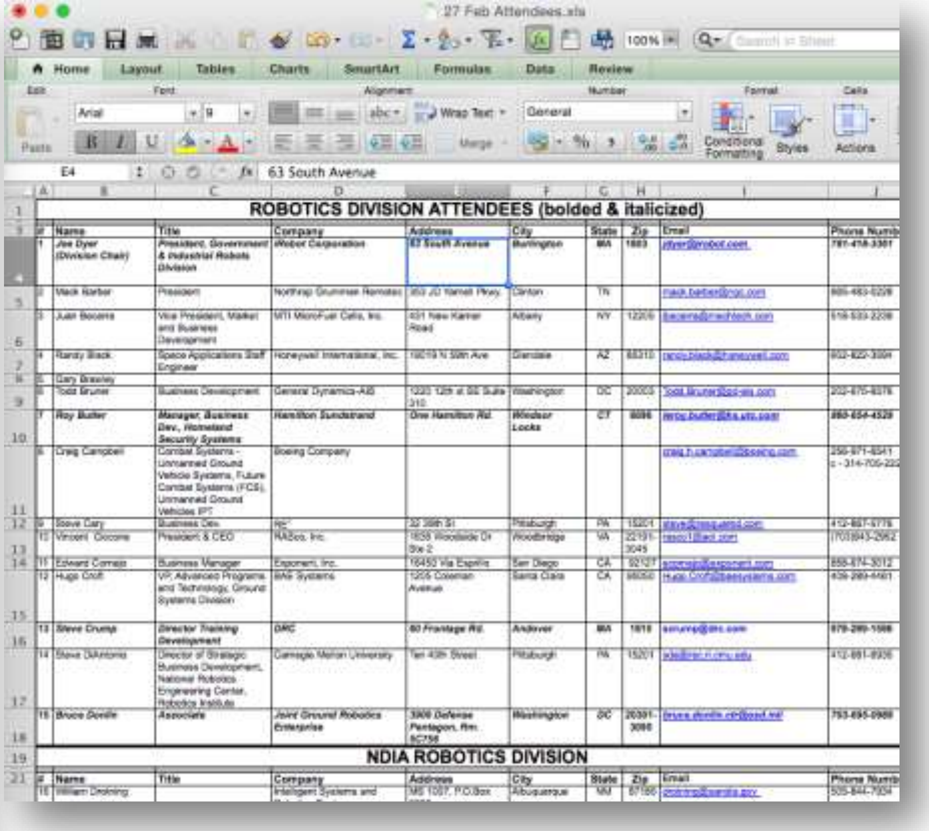
[XLS] Attendees
nws.weather.gov/nthr.../Minutes/.../attendees.xl... ▾ National Weather Service ▾
A, B, C, D, E, F, G. 1, ...Nov, 20-Nov, Name, Affiliation, Title, Phone, Email. 2, X, X, ...ris Jonientz-Trisler, ...EMA, Chief, Hazard Mitigation Assistance Branch ...

[XLS] Attendees - New York State Department of Health
https://www.health.n...v/.../atten... ▾ New York State Department of Health ▾
A, B. 1, ATTENDEES. 2, ...AL NY - Phase 5. 3, September 28, 2007. 4, 1:00 p.m. to 4:00 p.m.. 5. 6, AFFILIATI... FACILITY NAME, NAME. 7, ActiveHealth ...

[XLS] WoSCR-VIWS2-Attendees.xls - OpenVCE
openvce.net/sites/default/files/WoSCR-VIWS2-Attendees.xls ▾
A, B, C, D, E, F. 1, Last Name, First Name, Ticket Type, Organization, Second Life Avatar. 2, 1, Ahmad, Ali, Virtual Participant, Design Interactive, None.

[XLS] Attendees.xls
henry.pha.jhu.edu/midatlantic/resources/Attendees.xls ▾
A, B, C, D, E. 1, Last Name, First Name, e-mail, Affiliation. 2, 1, Aina, Nyodele, aaina@cheyney.edu, Department of Math Science, Cheyney University.

List of Attendees at a "National Defense Industrial Association"



63 South Avenue

ROBOTICS DIVISION ATTENDEES (bolded & italicized)

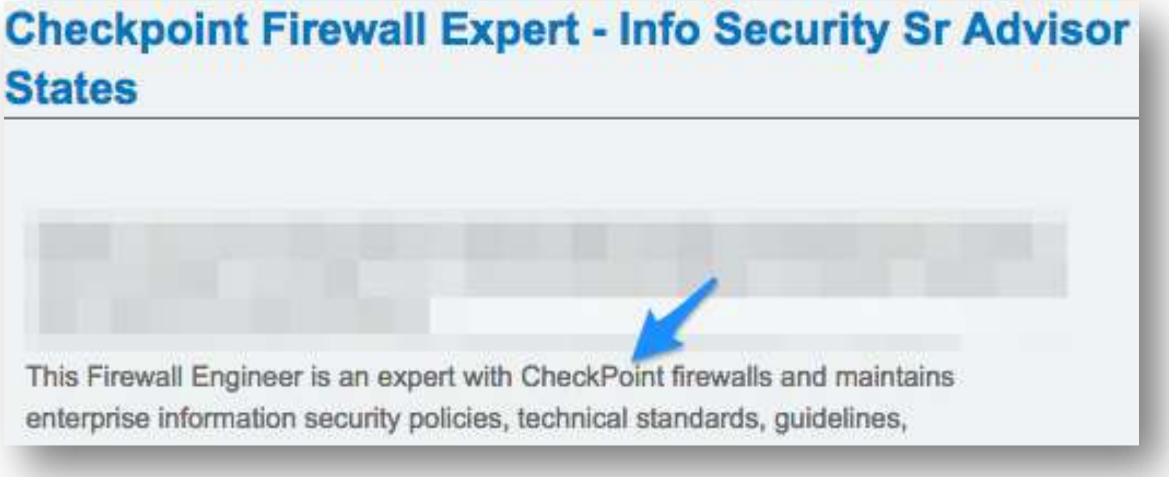
#	Name	Title	Company	Address	City	State	Zip	Email	Phone Numb
1	***Joe Dyer (Division Chair)***	***President, Government & Industrial Robots Division***	***iRobot Corporation***	***63 South Avenue***	***Burlington***	***MA***	***1803***	jdyer@irobot.com	***781-418-3381***
2	Mack Barber	President	Northrop Grumman Remotec	353 JD Yarnell Pkwy	Clinton	TN		mack.barber@ngc.com	865-483-0228
3	Juan Becerra	Vice President, Market and Business Development	MTI MicroFuel Cells, Inc.	431 New Karner Road	Albany	NY	12205	becerra@mechtech.com	518-533-2208
4	Randy Black	Space Applications Staff Engineer	Honeywell International, Inc.	19019 N 59th Ave	Glendale	AZ	85310	randy.black@honeywell.com	602-822-3384
5	Gary Brasley								
6	Todd Bruner	Business Development	General Dynamics-AIS	1220 12th st SE Suite 310	Washington	DC	20003	Todd.Bruner@gd-ais.com	202-675-8376
7	***Roy Butler***	***Manager, Business Dev., Homeland Security Systems***	***Hamilton Sundstrand***	***One Hamilton Rd***	***Windsor Locks***	***CT***	***6096***	leroy.butler@hs.utc.com	***860-654-4529***
8	Craig Campbell	Combat Systems - Unmanned Ground Vehicle Systems, Future Combat Systems (FCS), Unmanned Ground Vehicles IPT	Boeing Company					craig.h.campbell@boeing.com	256-971-6541 c - 314-705-222
9	Steve Cary	Business Dev.	RE²	32 39th St	Pittsburgh	PA	15201	steve@resquared.com	412-687-6775
10	Vincent Ciccone	President & CEO	RABco, Inc.	1656 Woodside Dr Ste 2	Woodbridge	VA	22191-3045	[illegible]	(703)943-2962
11	Edward Cornejo	Business Manager	Exponent, Inc.	16450 Via Esprillo	San Diego	CA	92127	ecornejo@exponent.com	858-674-3012
12	Hugo Croft	VP, Advanced Programs and Technology, Ground Systems Division	BAE Systems	1205 Coleman Avenue	Santa Clara	CA	95050	Hugo.Croft@baesystems.com	408-289-4461
13	***Steve Crump***	***Director Training Development***	***DRC***	***60 Frontage Rd.***	***Andover***	***MA***	***1810***	scrump@drc.com	***978-289-1568***
14	Steve DiAntonio	Director of Strategic Business Development, National Robotics Engineering Center, Robotics Institute	Carnegie Mellon University	Ten 40th Street	Pittsburgh	PA	15201	[illegible]	412-681-6936
15	***Bruce Doville***	***Associate***	***Joint Ground Robotics Enterprise***	***3090 Defense Pentagon, Rm. 5C756***	***Washington***	***DC***	***20301-3090***	bruce.doville.ctr@osd.mil	***703-695-0989***

NDIA ROBOTICS DIVISION

#	Name	Title	Company	Address	City	State	Zip	Email	Phone Numb
16	William Drotning		Intelligent Systems and [illegible]	MS 1007, P.O.Box [illegible]	Albuquerque	NM	87185	[illegible]@sandia.gov	505-844-7934

Reconnaissance

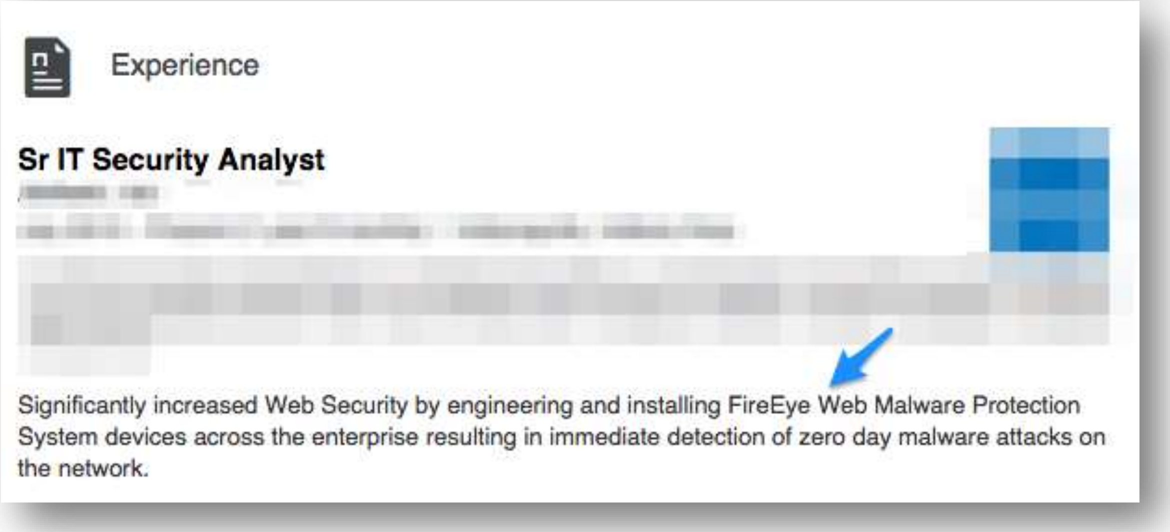
Identify the tools used to protect an organization



Checkpoint Firewall Expert - Info Security Sr Advisor States

[redacted]

This Firewall Engineer is an expert with CheckPoint firewalls and maintains enterprise information security policies, technical standards, guidelines,



Experience

Sr IT Security Analyst

[redacted]

Significantly increased Web Security by engineering and installing FireEye Web Malware Protection System devices across the enterprise resulting in immediate detection of zero day malware attacks on the network.

Preventing Recon

People

&

Process

Nothing the Adversary Did Could Have Been Prevented by Technology

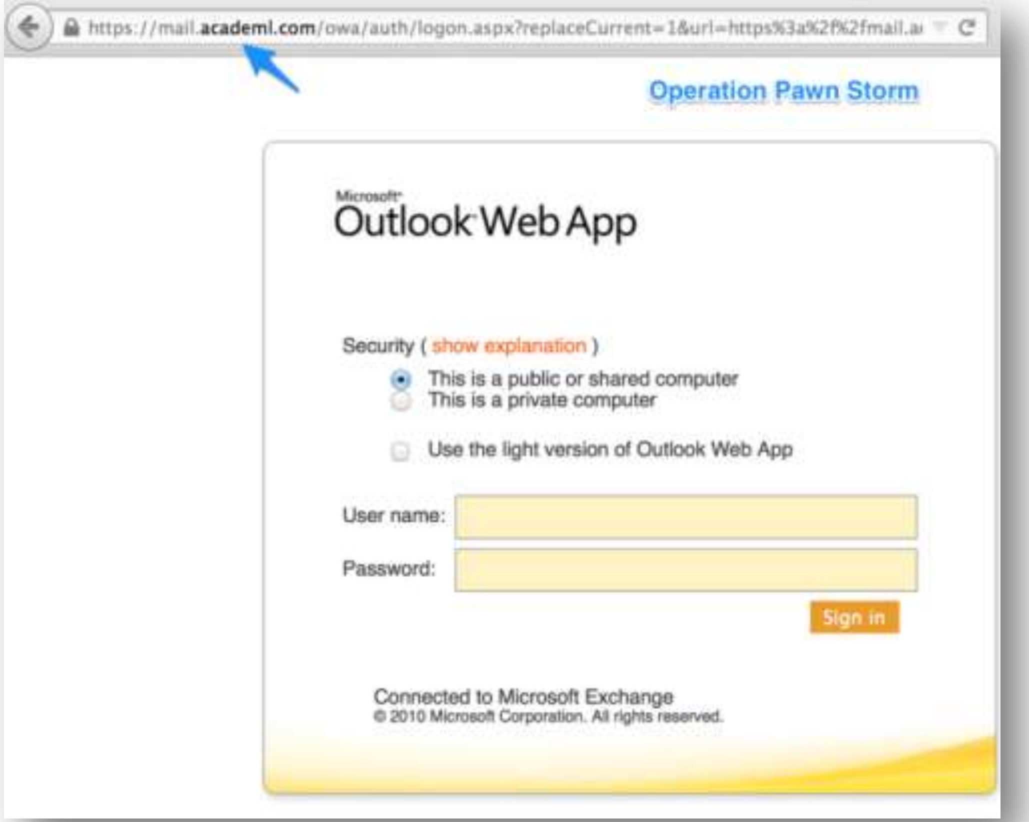
Exploitation

1

Exploiting the user

Why use malware when you have legitimate credentials?

Users are typically the path of least resistance.



https://mail.academl.com/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.a

Operation Pawn Storm

Microsoft Outlook Web App

Security (show explanation)

● This is a public or shared computer
○ This is a private computer

□ Use the light version of Outlook Web App

User name:

Password:

Sign in

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

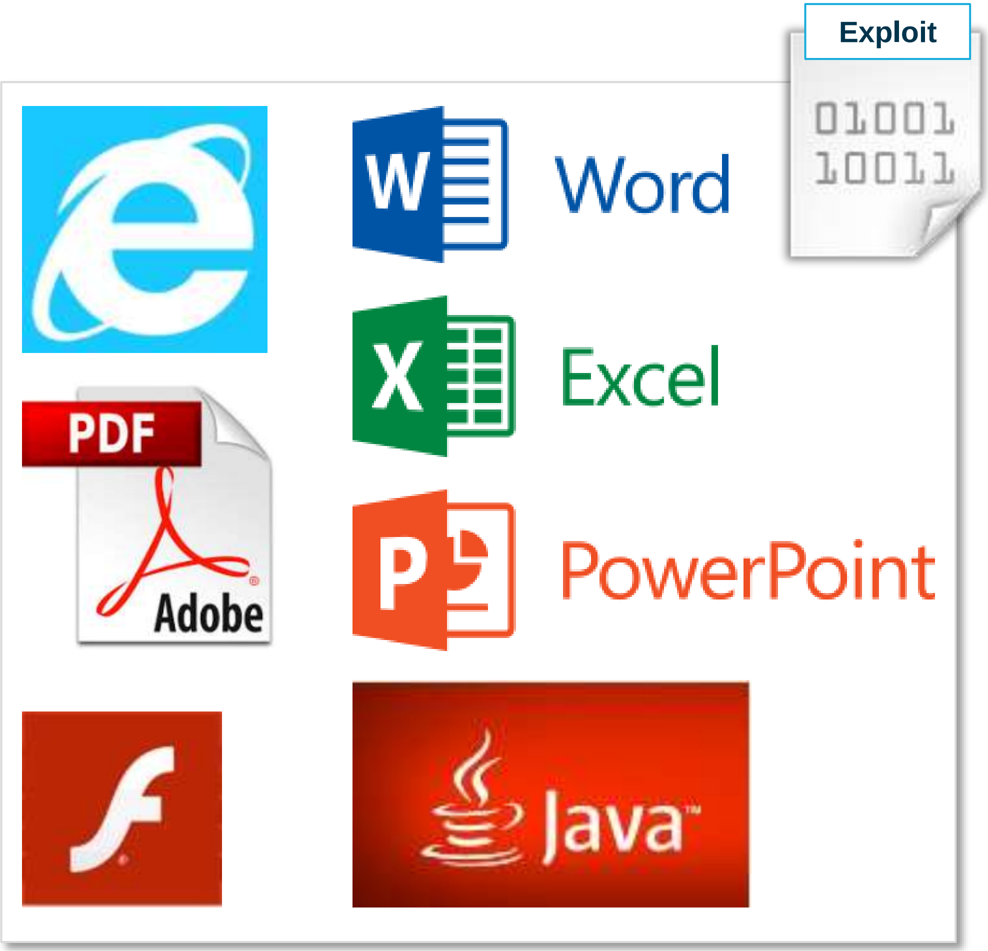
Exploitation

2

Exploiting the software

Why use a 0-day when 2012-0158/2010-3333 still open?

Old vulnerabilities may not be patched.



Exploitation

People:

- Training to recognize phishing attempts and be careful with credentials.

Process:

- Keep software patched to reduce the attack surface.

Technology:

- If you can’t patch systems, limit access via user-based policy.
- Deploy solutions that can prevent exploitation on the endpoint and network, even those that have not been seen before.
- Use systems that learn from new exploits and can stop them in real-time.

Delivery

Technology

Technology Becomes Critical to Preventing Advanced Attacks

Delivery

Delivering the Exploit

Spear Phishing

Attackers with a specific target

Watering Hole

AKA: Strategic Web Compromise for attackers targeting people with specific interests

Everything Else

Malicious USB Drives, Network Exploitation, etc.

Installation

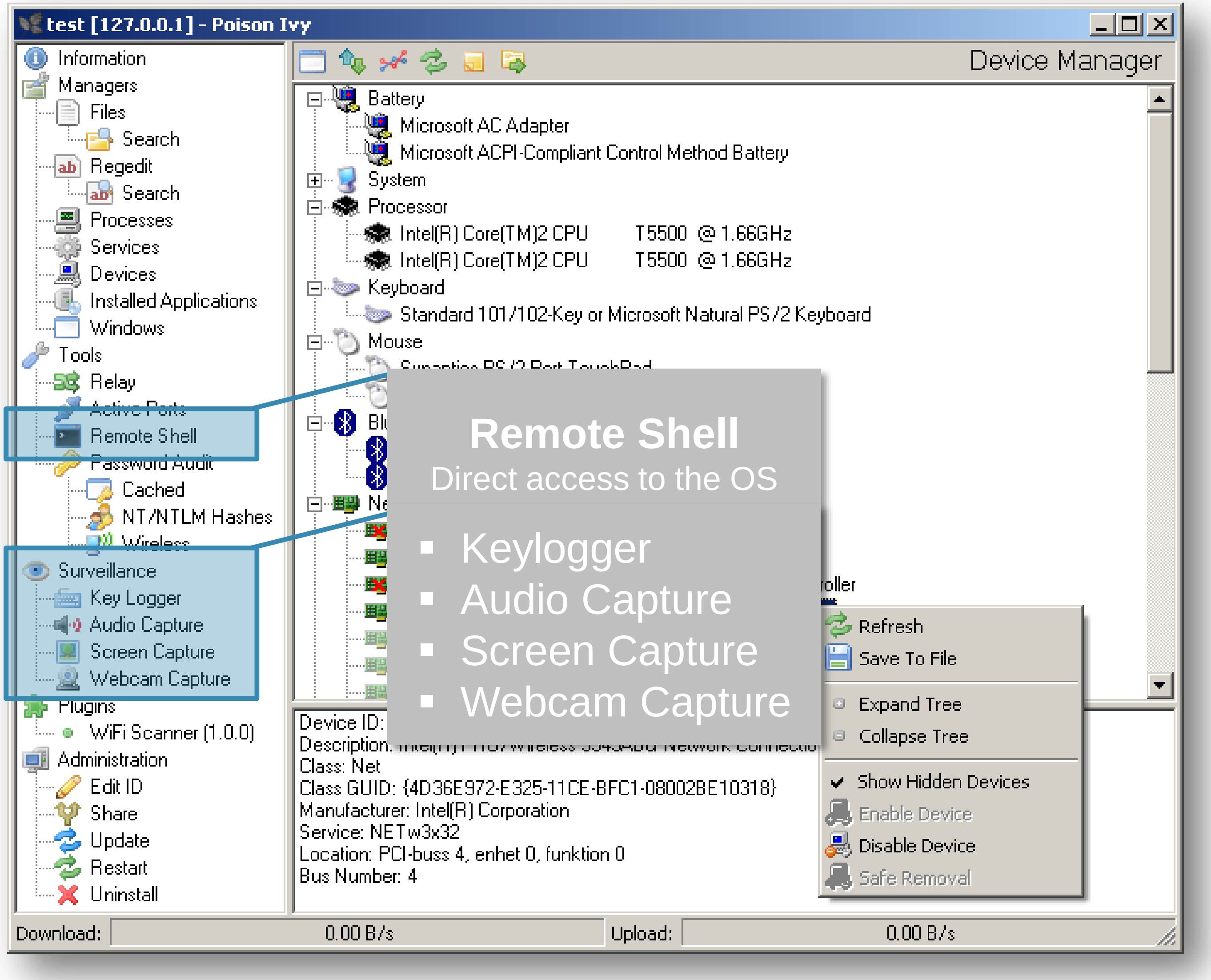
Myth

Highly customized and unique tools are used for every attack.

Reality

Off-the-shelf tools are the most common method of attack.

Common Tools



Device ID:
Description: Intel(R) PRO/Wireless 3945ABG Network Connectio
Class: Net
Class GUID: {4D36E972-E325-11CE-BFC1-08002BE10318}
Manufacturer: Intel(R) Corporation
Service: NETw3x32
Location: PCI-buss 4, enhet 0, funktion 0
Bus Number: 4

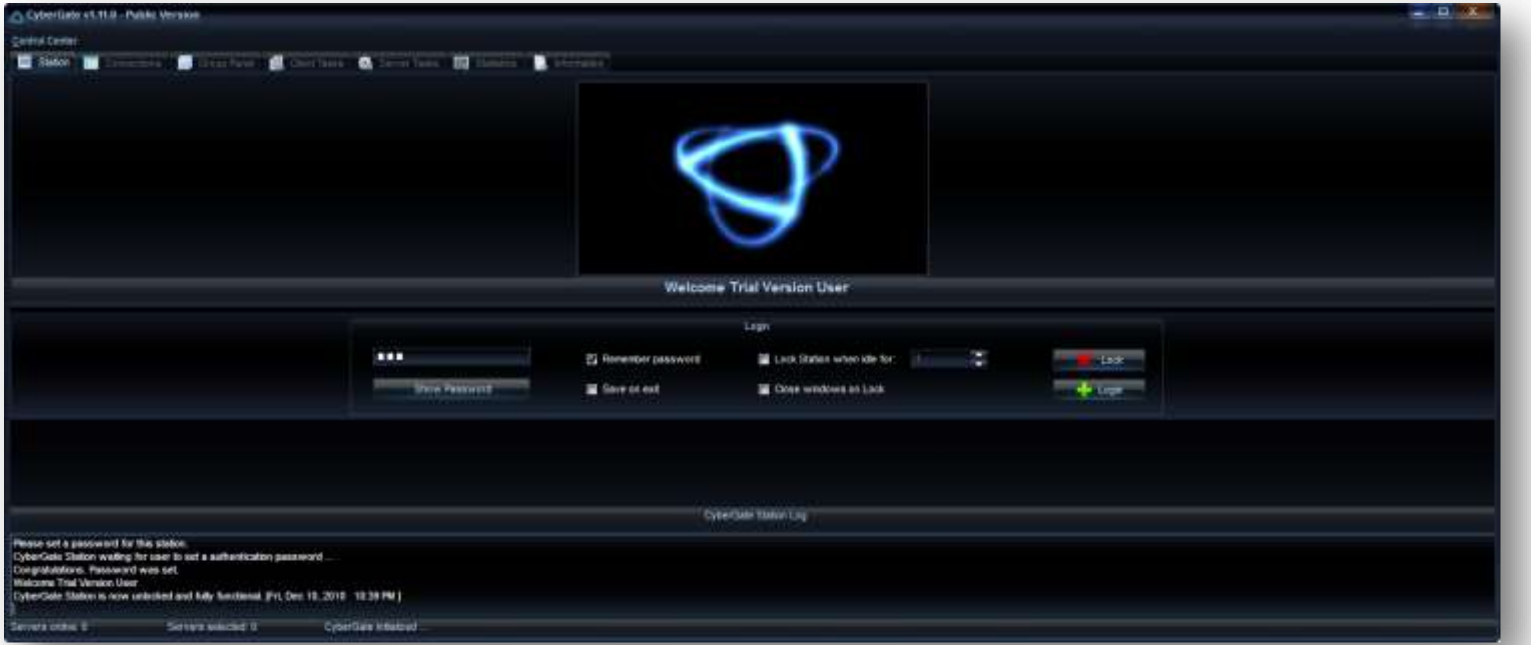
Download: 0.00 B/s
Upload: 0.00 B/s

Remote Shell

Direct access to the OS

- Keylogger
- Audio Capture
- Screen Capture
- Webcam Capture

Common Tools



Welcome Trial Version User

☑ Remember password

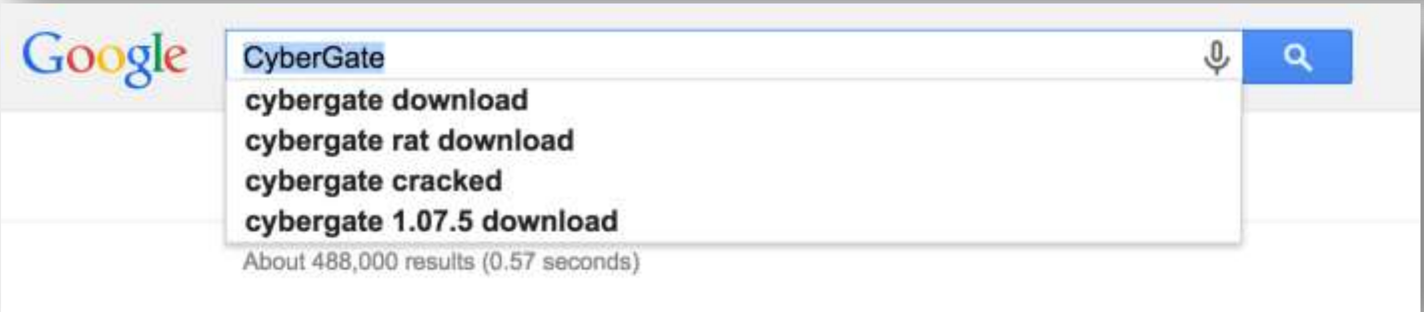
☐ Save on exit

☐ Lock Station when idle for:

☐ Close windows on Lock

```
Please set a password for this station.
CyberGate Station waiting for user to set a authentication password ...
Congratulations. Password was set.
Welcome Trial Version User
CyberGate Station is now unlocked and fully functional. [Fri, Dec 10, 2010   10:39 PM ]
```

Servers online: 0   Servers selected: 0   CyberGate initiated ...



CyberGate

cybergate download

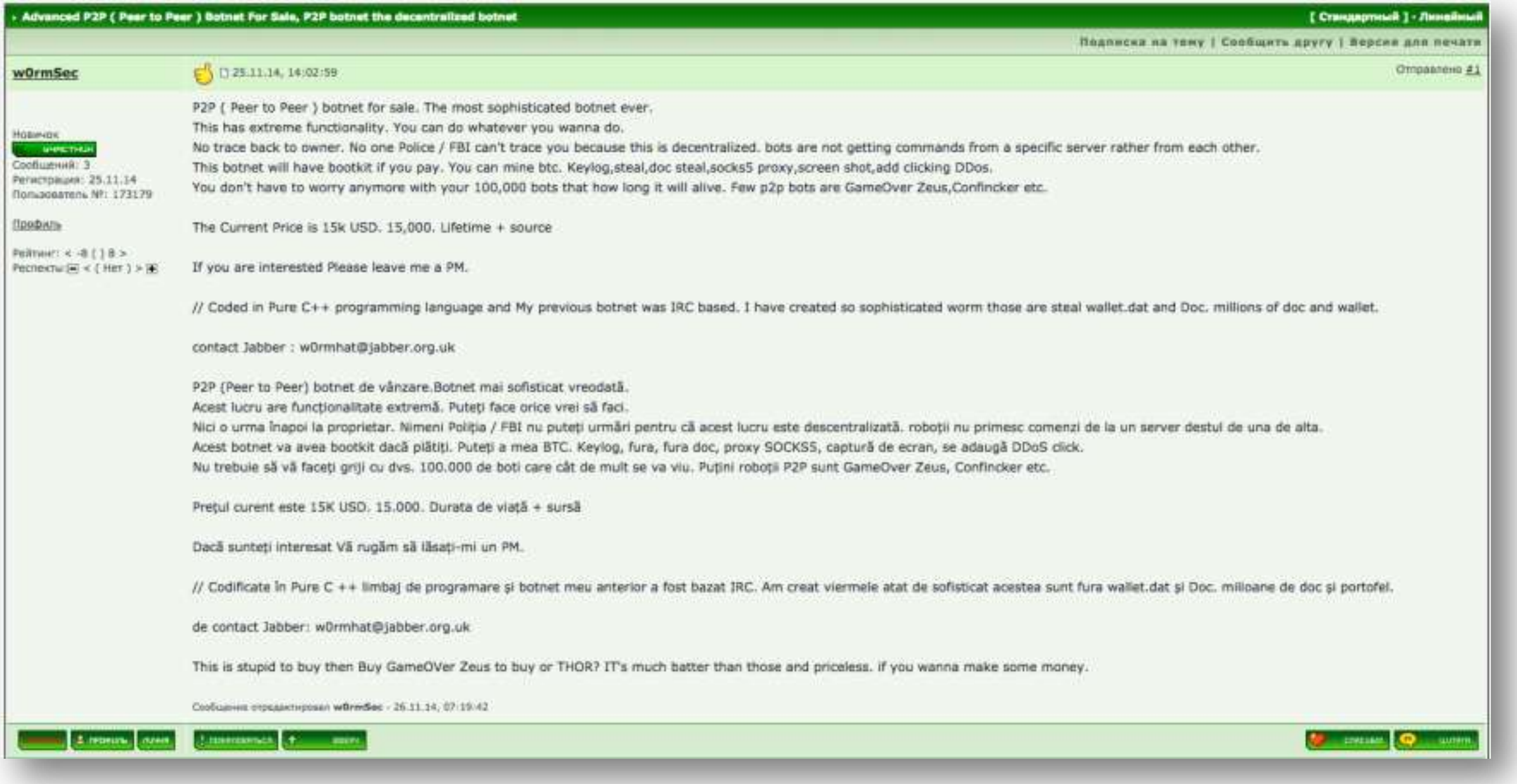
cybergate rat download

cybergate cracked

cybergate 1.07.5 download

About 488,000 results (0.57 seconds)

The Underground Economy


[Стандартный] · Линейный
Подписка на тему | Сообщить другу | Версия для печати
Отправлено #1
Профиль
профиль
лично
пожаловаться
вверх
спасибо
цитата

› Advanced P2P (Peer to Peer) Botnet For Sale, P2P botnet the decentralized botnet

w0rmSec

Новичок
участник
Сообщений: 3
Регистрация: 25.11.14
Пользователь №: 173179

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

25.11.14, 14:02:59

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

“Peer-to-peer Botnet […] $15,000”

Preventing Delivery and Installation

Technology:

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

Command and Control (C2)

Communicating with infected hosts and providing instructions

Myth

Customized protocols, with unique encryption types are used for CnC.

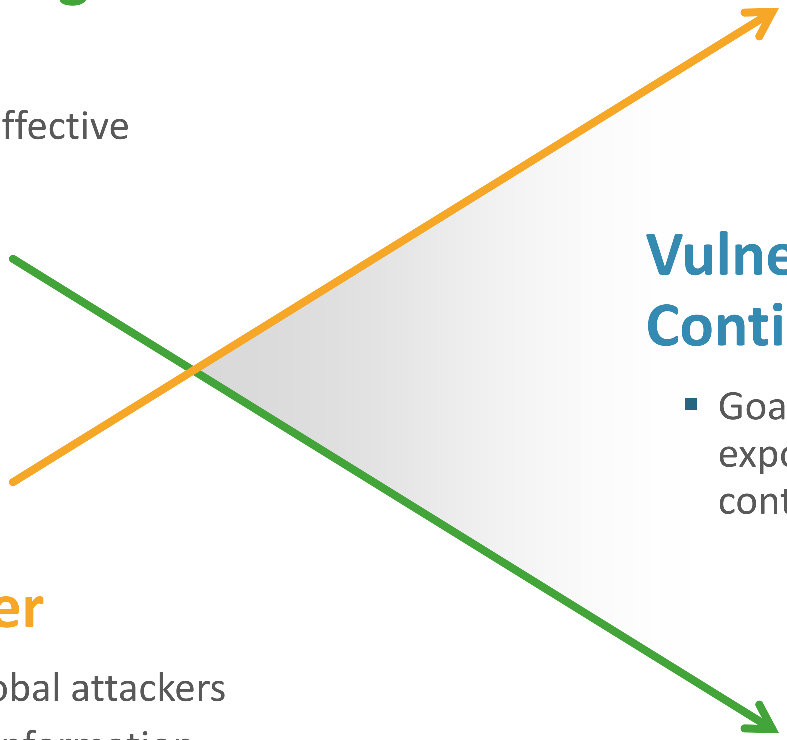
Reality

HTTP is most common for custom backdoors.

New Strategic Approaches to Security Are Needed

Security Organizations Are Not Innovating Fast Enough

- Existing controls ineffective against new threats
- Controls not evolving fast enough



Vulnerability Gap Continues to Widen

- Goal: reduce threat exposure by strengthening controls

Attackers Are Innovating Faster

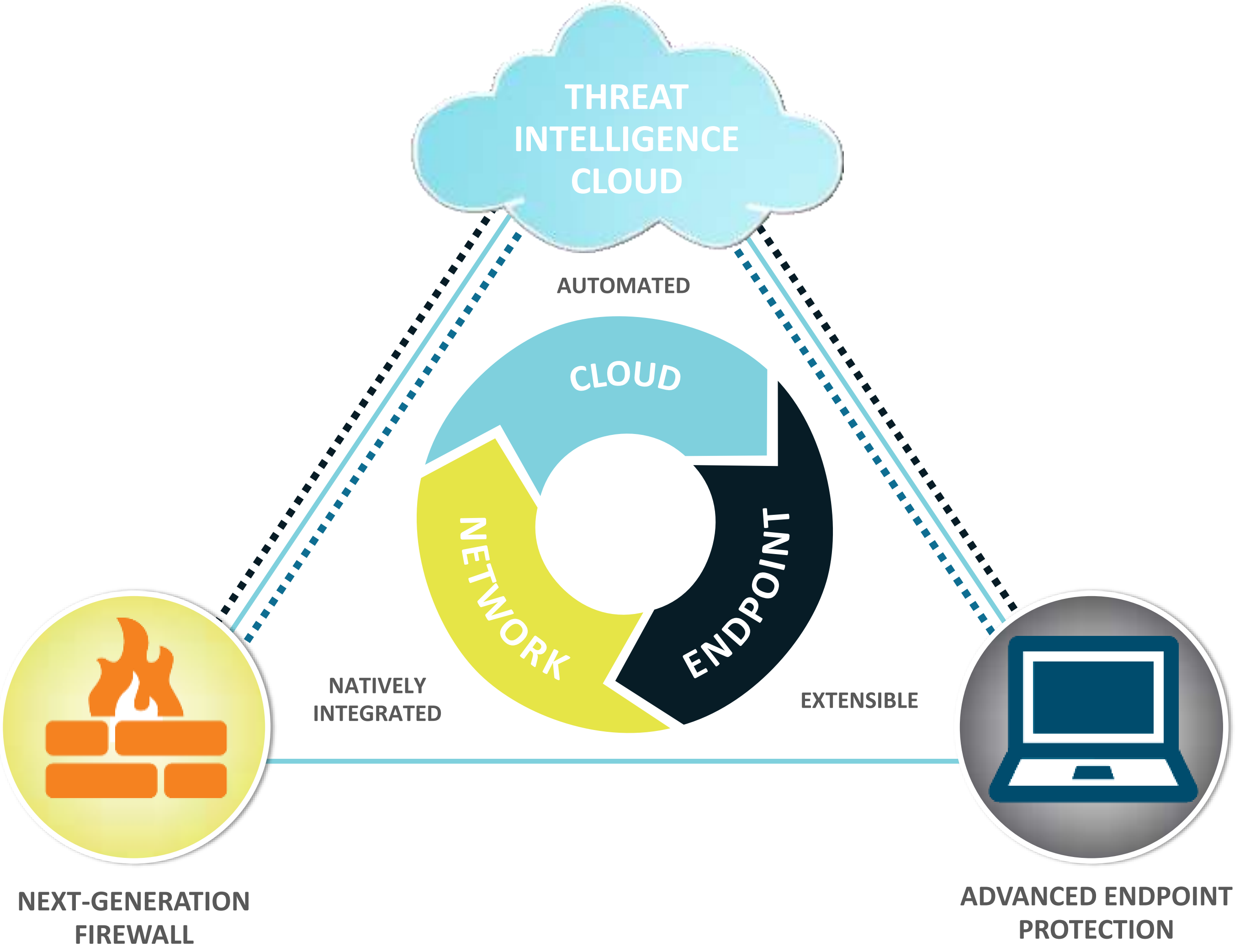
- Sophistication of global attackers
- Increasing value of information
- Easier targets

ZERO TRUST NETWORKING

THEN AND NOW

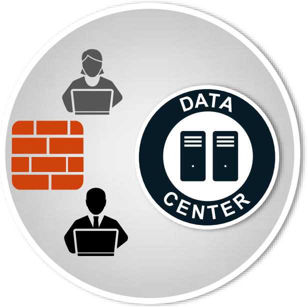
How the posture of security is changing

Next-Generation Security Platform



Detect & Prevent Threats at Every Point

At the
Mobile Device



At the
Internet Edge

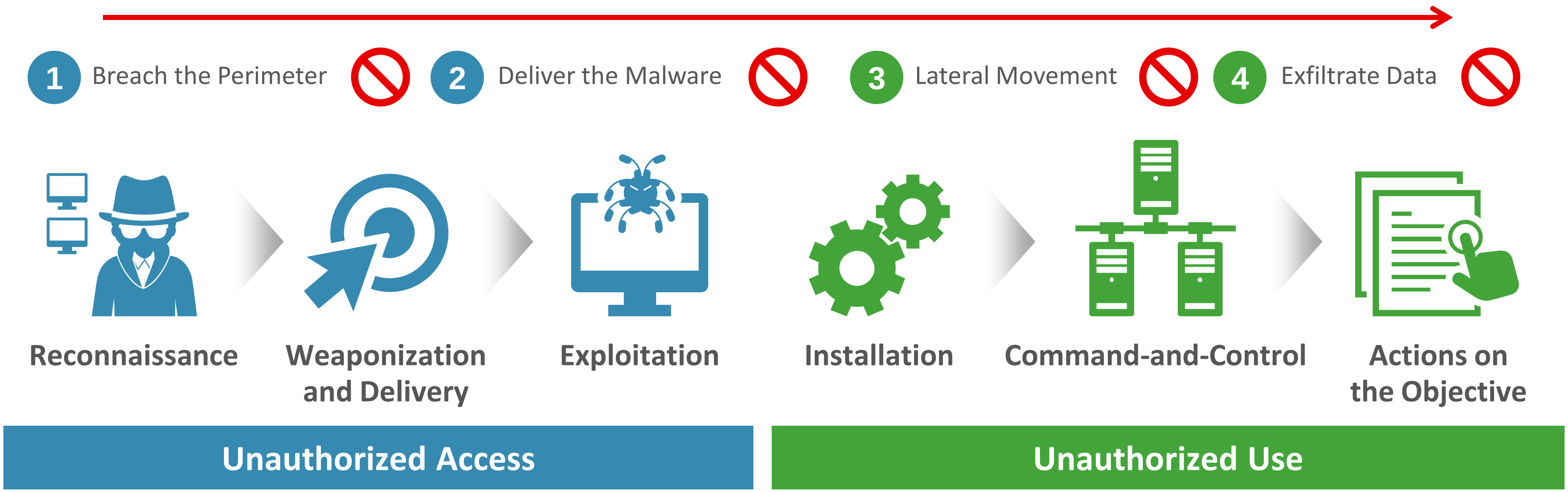
Between
Employees and
Devices within
the LAN

At the
Data Center
Edge and
between VMs

Within Private,
Public and
Hybrid Clouds

- Prevent attacks, both known and unknown
- Protect all users and applications, in the cloud or virtualized
- Integrate network and endpoint security
- Analytics that correlate across the cloud

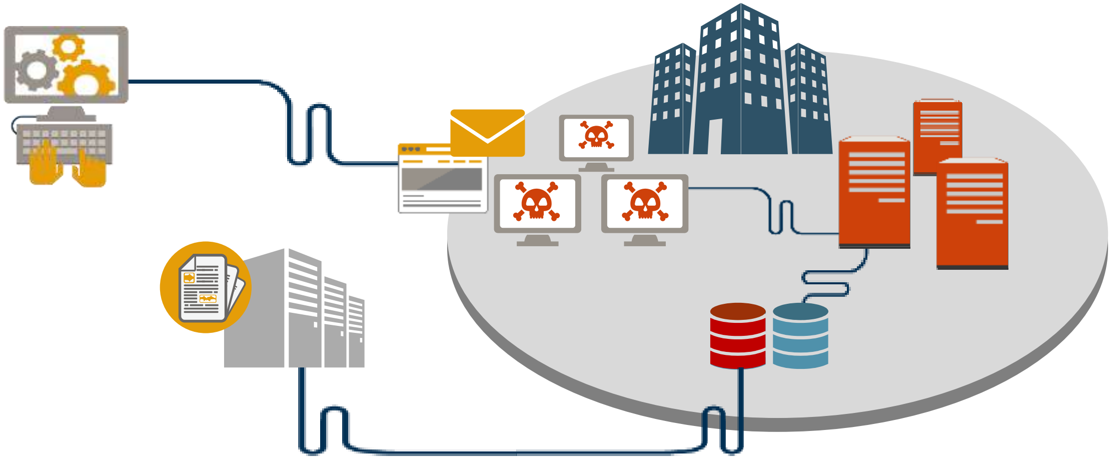
Preventing Across the Cyber Attack Lifecycle



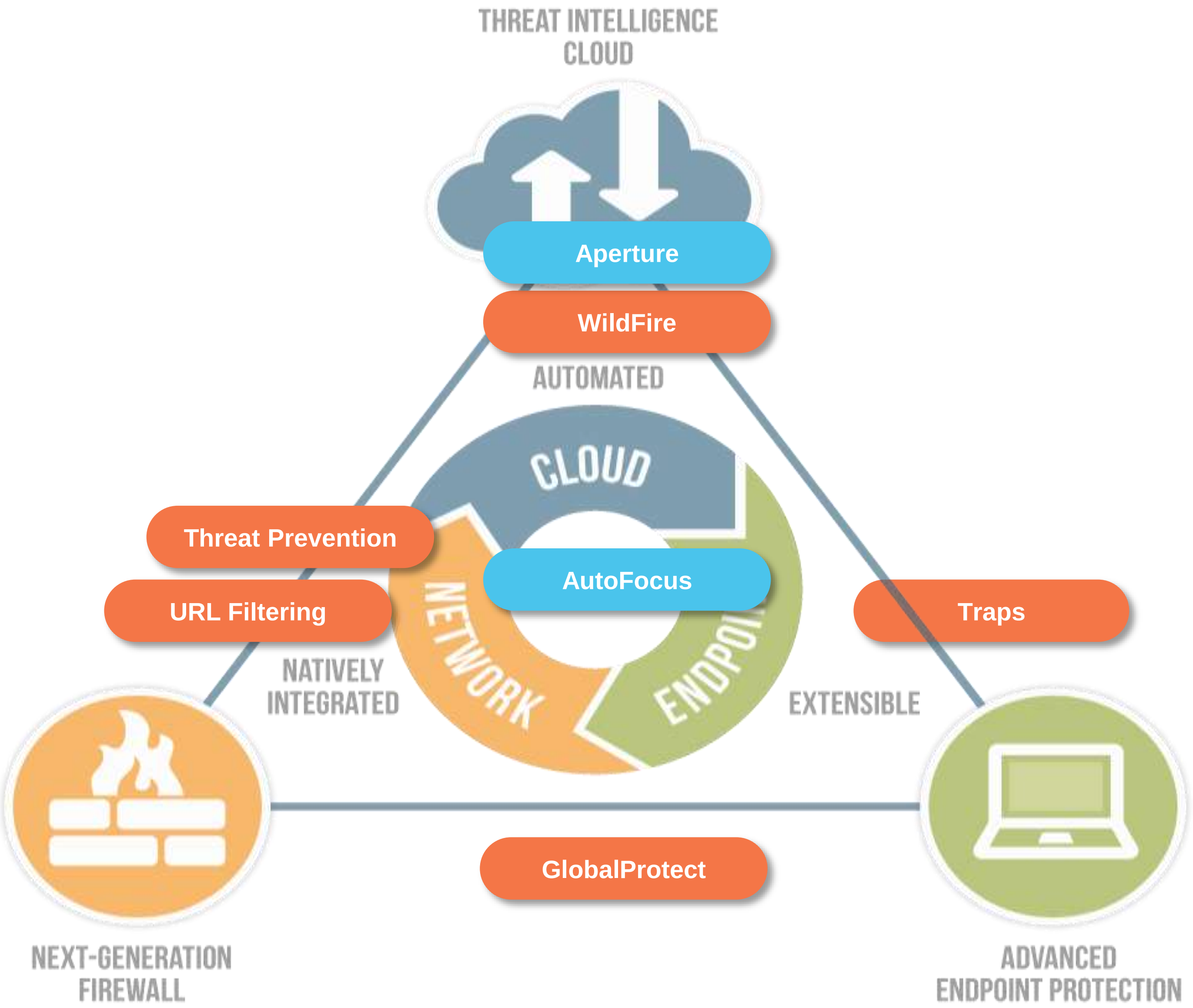
1 Breach the Perimeter 🚫 2 Deliver the Malware 🚫 3 Lateral Movement 🚫 4 Exfiltrate Data 🚫

Reconnaissance → Weaponization and Delivery → Exploitation → Installation → Command-and-Control → Actions on the Objective

Unauthorized Access	Unauthorized Use



Delivering continuous innovation



GRAZIE !