Keeping APTs in the Box !!

Driving the need for Consolidated IT Security

Gökhan Poyraz

Security Consultant, Fortinet

October 18, 2011

Advanced Persistent Threats

Advanced

- The hacker has the ability to evade detection and the capability to gain and maintain access to well-protected networks and sensitive information contained within them. The hacker is generally adaptive and well resourced

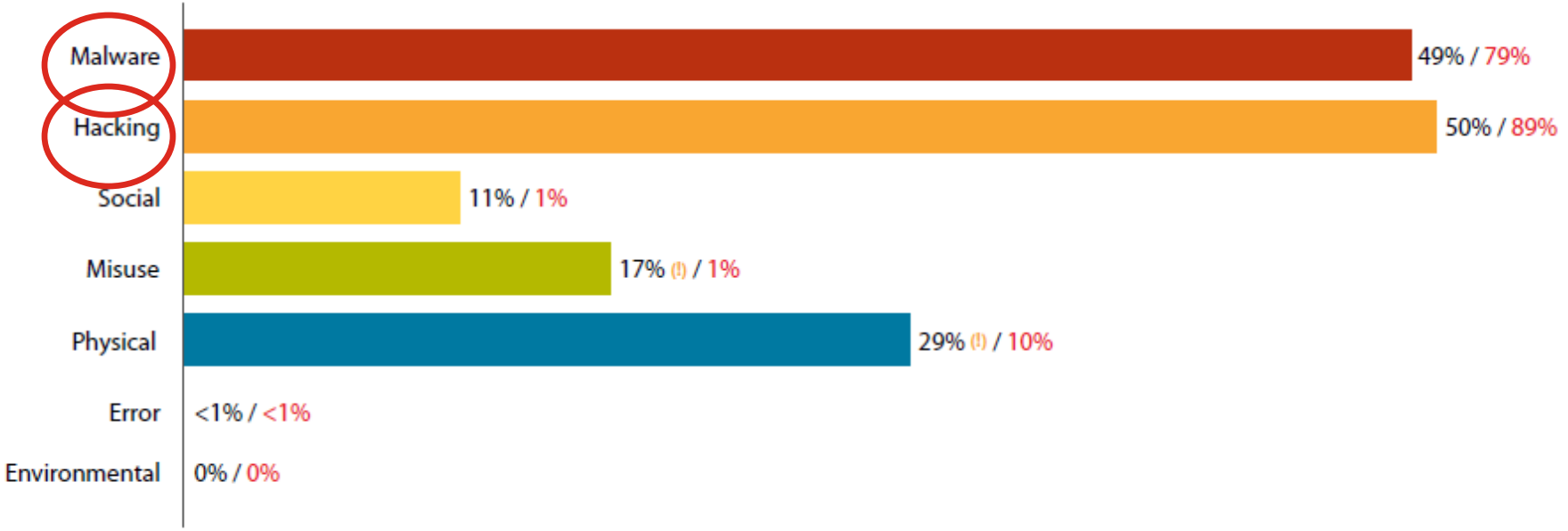
Persistent

- The persistent nature of the threat makes it difficult to prevent access to your computer network and, once the threat actor has successfully gained access to your network, very difficult to remove.

Threat

- The hacker has not only the intent but also the capability to gain access to sensitive information your organisation has stored electronically.

Verizon Data Breach (2011) Research Results



The APT Difference

APT	‘Regular’ Threat
Victim targeted and specific	Generalised threat to all internet users/assets
Multiple attack vector attempts on asset	One-hit and move on
Evolves attack modes as a function of victim response	Uni-dimensional
High value asset focused	‘Whatever we can get’

APT : Examples

State Sponsored Cyber War

- Google – Operation Aurora
  Exploitation of zero-day vulnerabilities in Internet Explorer . Crafted malware searches corporate intranet for specific IP repositories

Focused Malware

- Jan 12 2010, Google blogged that some of its IP was stolen via a Chinese sourced attack.
- Subsequently discovered vulnerabilities in its source code revision software.
- Malware opens up a backdoor connection masquerading as an SSL connection to command and control servers running on stolen RackSpace customer accounts
- In total 34 organisations are suspected to have been targeted.

Industrial Targeting

- Google
- Adobe Systems
- Juniper Networks
- RackSpace
- Symantec
- Morgan Stanley
- Dow Chemicals

.

APT : Examples

Reputation Destruction through Hack and Disclosure

- HBGary – Anonymous

  In an act of retaliation, hackers Anonymous hacked the HBGary website, stole documents and posted tens of thousands of email online and compromised the CEO's Twitter account

Targeted Revenge Hacking

- Feb5th-6th 2011, Hackers Anonymous hacked the HBGary website
- Highly sensitive documents disclosed from HBGary Federal implicating law firms and Bank of America in spying and discrediting tactics on Wikileaks
- On-going dismantling of HBGary Federal business.

.

HBGary

DETECT. DIAGNOSE. RESPOND.

APT : Examples

CIO Fears and Concerns

- Targeted Attack – Spear Phishing

  Using social engineering to distribute emails with links to malware, the emails are relevant to the corporation being targeted. Infected documents (PDF, DOC, XLS) can use software exploits to infect systems

Kneber (Zeus) Botnet

- In 2010 a spear phishing attack on US .mil and .gov employees by a Zeus variant infected 50,000+ end systems
- Data stolen included:
  - Corporate Login credentials
  - Email and webmail access
  - Online Banking sites
  - Social Network credentials
  - SSL Certificates

From: jeffreyc@greylogic.us [mailto:jeffreyc@greylogic.us]
Sent: Wednesday, February 10, 2010 7:34 AM
To:
Subject: Russian spear phishing attack against .mil and .gov employees

Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or InteLink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft(r) Windows(r) and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Download:

http://fcpra.org/downloads/winupdate.zip

or

http://www.sendspace.com/file/tj373l

APT : Examples

Destruction of Iranian industrial assets ?

- Stuxnet – Targeting Industrial Systems

  First publicly known worm to target industrial control systems (SCADA), containing malicious STL code in a PLC rootkit and Windows rootkit hiding the code. Included a zero-day vulnerability to spread via USB drives

Stuxnet Worm - Scada

- Windows computer worm discovered in July 2010
- Indiscriminate promulgation, but specialised payload
- Fakes industrial control sensor signals
- 58% of Iranian computers infected.
- Non Scada systems unaffected.
- Will self erase on 24th June 2012

Stuxnet virus: worm 'could be aimed at high-profile Iranian targets'

Security experts have identified malicious software, thought to be aimed at power stations and water plants in Iran.

Some security experts believe the Stuxnet worm was aimed at key parts of Iran's infrastructure, such as nuclear facilities, and may have been written or sanctioned by operatives from another nation. Photo: EPA

Share:

Recommend 91

Tweet 49

Technology News

News » Iran » Technology »

IN TECHNOLOGY

Gadgets taken apart

APT : Examples

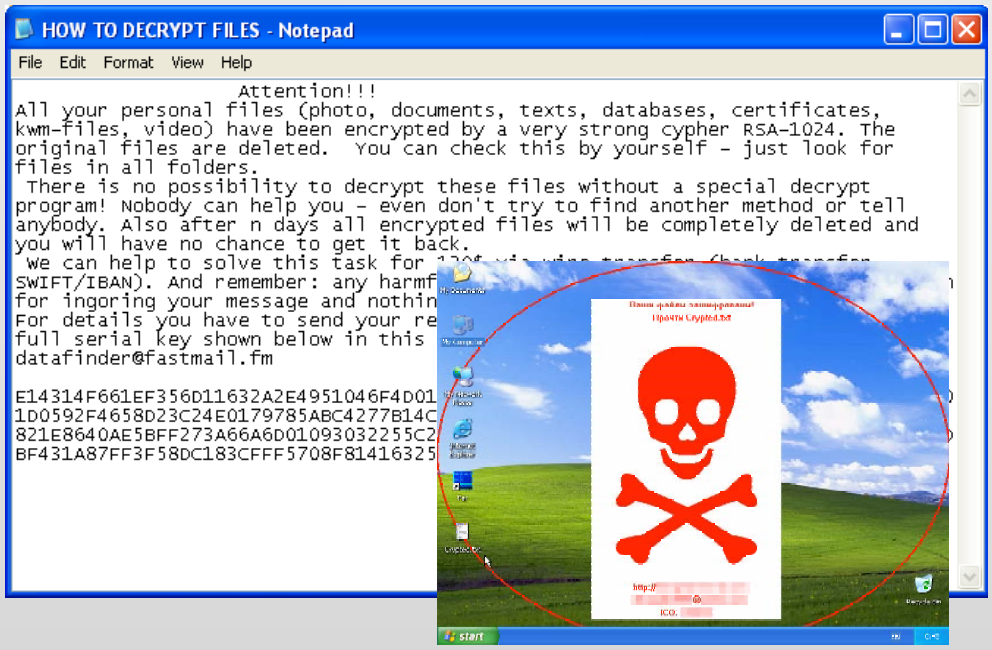
CIO Fears and Concerns

- Ransomware

  Once installed is very difficult to reverse, files are encrypted, this isn't just based on the fear that something might happen, once you are reading the ransom note your data has already been encrypted.

gpCode Ransomware

- Once installed searches hard drive for document and media files
- Files are encrypted with a 1024bit key which only the attacker has the decryption key
- Ransom note is displayed to user, system continues to operator but data is inaccessible
- Will encrypt xls, doc, pdf, txt, rar, zip, avi, jpg, mov, etc…



So what can you do ? – Technical Controls

- APD – "*Advanced/Adaptable Persistent Defense*"

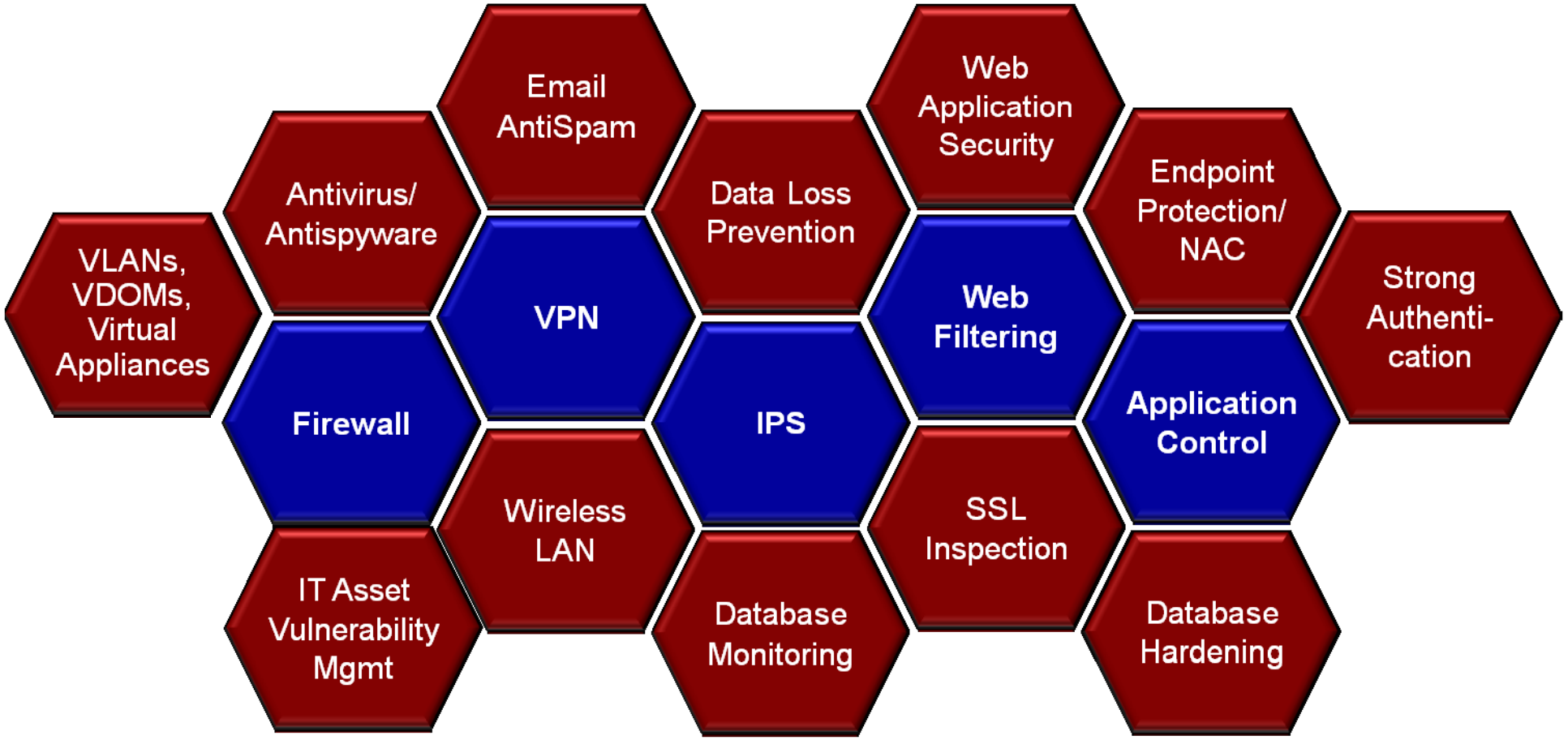
- Effective protection against multiple attack vectors
  - Mail, Application, Malware, Botnets
- Robust in-depth asset hardening
  - Networks, Web Apps, Data/Databases, Laptops, Servers
- Application Control
  - Risk/threat based application channel, P2P, Botnet CC
- Monitoring
  - Breach signatures on applications, networks, data and DLP
- Up to the minute managed protection
  - IT-wide signature maintenance.

A word on AETs – Advanced Evasion Techniques

- Coined by Stonesoft in 2010 to refer to methods of masking intrusions to avoid detection by known IPS vendors
- Actually nothing new! Evasion is a key element of APTs
- 124 AETs were registered with CERT in October 2010
- Fortinet's IPS was quickly updated to respond.
- Tease the marketing from reality!

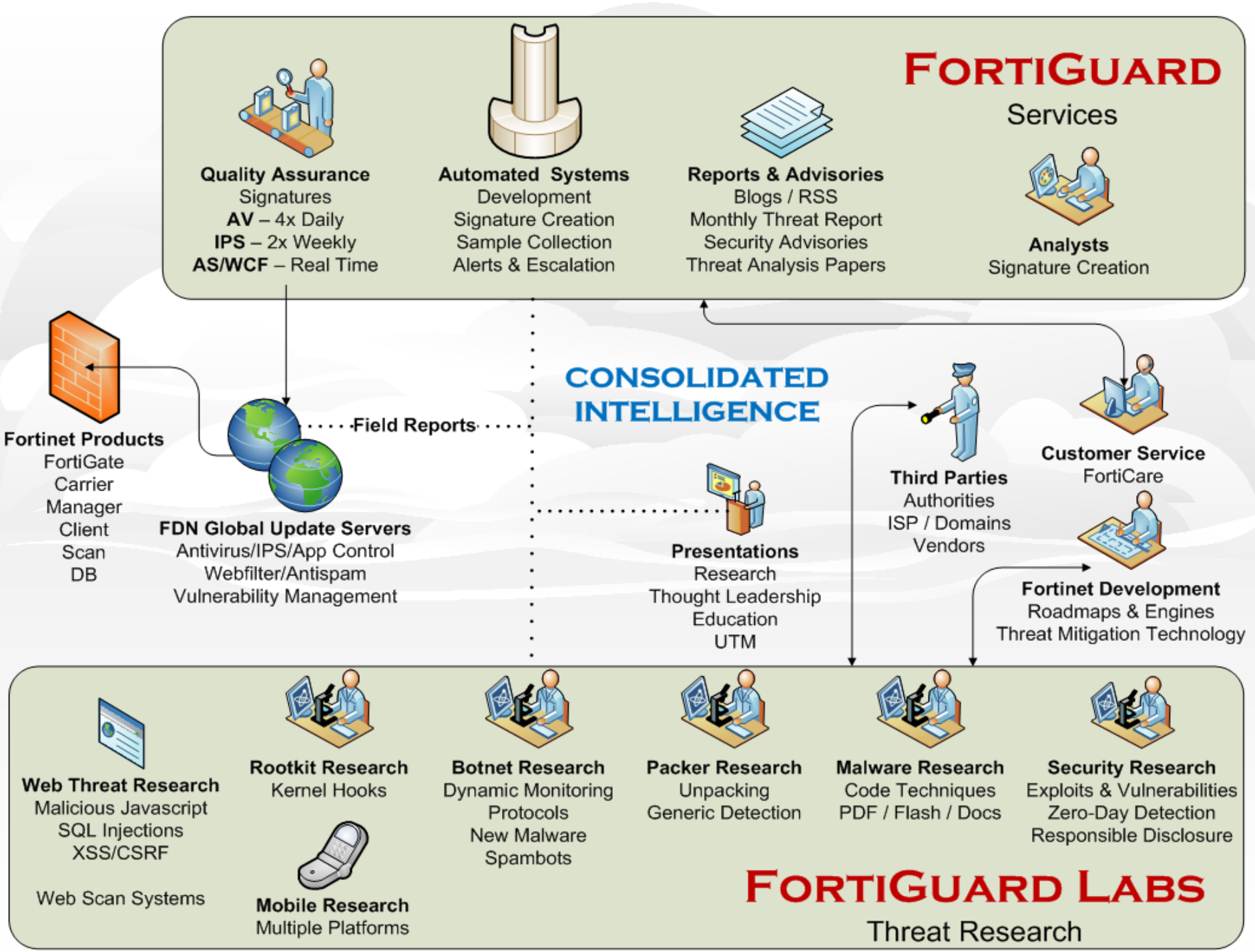
Fortinet 'APD' Security

Advanced Persistent Defense



FortiGuard Services – Real Time Updates

- **Application Control:** Unwanted Services and P2P Limiting
  Botnet command channel, compromised Facebook applications, independent of port or protocol
- **Intrusion Prevention:** Vulnerabilities and Exploits
  Browser and website attack code crafted by hackers and criminal gangs.
- **Web Filtering:** Multiple categories and Malicious sites
  Botnet command, phishing, search poisoning, inappropriate content
- **Vulnerability & Compliance Management:** Real time exploit updates
  Multiple scanning points FortiGate, FortiAnalyzer, FortiWeb, FortiDB, and FortiScan
- **Antispam:** Unsolicited messages
  Phishing, Malware, Social Engineering and Junk
- **Antivirus:** All malicious code
  Documents, macros, scripts, executables delivered via Web,
  Email, USB, Instant messaging, social networks, etc


FortiGuard
Services
Quality Assurance
Signatures
AV – 4x Daily
IPS – 2x Weekly
AS/WCF – Real Time
Automated Systems
Development
Signature Creation
Sample Collection
Alerts & Escalation
Reports & Advisories
Blogs / RSS
Monthly Threat Report
Security Advisories
Threat Analysis Papers
Analysts
Signature Creation
Fortinet Products
FortiGate
Carrier
Manager
Client
Scan
DB
FDN Global Update Servers
Antivirus/IPS/App Control
Webfilter/Antispam
Vulnerability Management
Field Reports
CONSOLIDATED
INTELLIGENCE
Presentations
Research
Thought Leadership
Education
UTM
Third Parties
Authorities
ISP / Domains
Vendors
Customer Service
FortiCare
Fortinet Development
Roadmaps & Engines
Threat Mitigation Technology
Web Threat Research
Malicious Javascript
SQL Injections
XSS/CSRF
Web Scan Systems
Rootkit Research
Kernel Hooks
Mobile Research
Multiple Platforms
Botnet Research
Dynamic Monitoring
Protocols
New Malware
Spambots
Packer Research
Unpacking
Generic Detection
Malware Research
Code Techniques
PDF / Flash / Docs
Security Research
Exploits & Vulnerabilities
Zero-Day Detection
Responsible Disclosure
FortiGuard Labs
Threat Research

APT vs APD : Beating the Zeus/Kneber Attack

- Email Sent – Contains link to compromised site

ANTISPAM

Mail message detected as spam (phishing)

- End user accesses phishing site, enters credentials, and criminals now have their details

WEB FILTER

Access to phishing website is blocked

- Phishing site sends BOT infection to user disguised as 'Security Update' application

ANTIVIRUS

Content scanning prevents malicious content from being downloaded

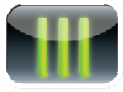
- End user executes BOT application, is infected and now all their data is compromised

INTRUSION DETECTION

Botnet command channel is blocked, no compromised data can be sent.
Security administrator is alerted to existed of an infected system.

Fortinet Security Solution Portfolio

Unified Threat Management



FortiGate
Network Security Platform

FortiAP
Network Security Platform

Centralized Management

FortiManager
Centralized Device Management

FortiAnalyzer
Centralized Logging and Reporting

Application Security

FortiMail
Messaging Security

FortiWeb
WAF with Load Balancer and Vulnerability Scanner

Security Services

FortiGuard
Real time Security Services

Host Security

FortiClient
Endpoint Security

FortiScan
IT Infrastructure Security

Data Security

FortiDB
Database Security

Customers Worldwide

7 of the top 10 Fortune companies in Americas

8 of the top 10 Fortune companies in EMEA

9 of the top 10 Fortune companies in APAC

10 of the top 10 Fortune Telecommunications companies

9 of the top 10 Fortune Retail & Commercial Banks

7 of top 10 Fortune Aerospace & Defense

Summary

- Advanced Persistent Threats
  - An evolution rather than revolution
- Overall threat landscape getting tougher
  - Hackers more focused in attack mode, more focus in objectives
- Immediate current events demand a security review
  - HBGary, Sony Playstation Network/SOE
- Advanced Persistent Defense
  - Multi-disciplined, consolidated security addressing all IT assets
- Business level visibility is driving risk management
  - Business level controls <-> technical level controls
- Fortinet is your ideal security technology partner
  - Complete solution and partner portfolio

Q & A

Gökhan Poyraz
gpoyraz@fortinet.com