AGENDA

CÁC MÓI HIỂM HỘA VÀ RỦI RO AN TOÀN THÔNG TIN

XU HƯỞNG VÀ GIẢI PHÁP PHÒNG CHỐNG

GIỚI THIỆU CÔNG NGHỆ FIREEYE
Antivirus is dead, says maker of Norton Antivirus

Antivirus is dead.

So sayeth Brian Dye, Symantec's senior vice president for information security, in a weekend interview with The Wall Street Journal. The words sound shocking.

Antivirus "is dead,"
Brian Dye, Symantec's senior vice president for information security. "We don't think of antivirus as a moneymaker in any way."

Antivirus products aim to prevent hackers from getting into a computer. But hackers often get in anyway these days.

http://online.wsj.com/news/article_email/SB10001424052702303417104579542140235850578-IMyQjAxMTA0MDAwNTEwNDUyWj
Acceleration of Advanced Targeted Attacks

- # of threats are up **5X**
- Nature of threats **changing**
  - From broad, scattershot to advanced, targeted, persistent
- Advanced **attacks accelerating**
  - High profile victims common (e.g., RSA, Symantec, Google)
  - Numerous APT attacks like Operation Aurora, Shady RAT, GhostNet, Night Dragon, Nitro

“Organizations face an evolving threat scenario that they are ill-prepared to deal with….advanced threats that have bypassed their traditional security protection techniques and reside undetected on their systems.”

Gartner, 2012
The Numbers Show a Harsh Reality

2/3 of U.S. firms report that they have been the victim of cyber attacks.

40% of all IT executives expect a major cyber-security incident.

115% CAGR unique malware since 2009.

9,000+ malicious websites identified per day.

95 new vulnerabilities discovered each week.

6.5x Number of cyber attacks since 2006.

Every second 14 adults become a victim of cyber crime.

* Based on FireEye end-user data
Playing a Catch Up Game???

208,184 Malware Download

124,289 Unique Malware

93,755 Malware Seen ONCE

75% of all the unique malware detected was ONCE
The High Cost of Being Unprepared

229 Days
Median # of days attackers are present on a victim network before detection.

Initial Breach

Source: M-Trends Report 2013

67% of Companies Learned They Were Breached from an External Entity

100% of Victims Had Up-To-Date Anti-Virus Signatures
Inside APT1

Monday, February 18, 2013: Mandiant released an intelligence report on threat group APT1

- Linked APT1 to PLA unit 61398
- Provided hard evidence
- Included 5 minute video showing footage of the attacker in action
- Released 3000+ actionable indicators of compromise (IOCs)
  - OpenIOC format
  - Malware reports
  - IPs/domain names
  - MD5s
  - SSL Certificates
- Set the bar for actionable intelligence sharing
The hackers, were all officers in Unit 61398 of the Third Department of the Chinese People’s Liberation Army. They worked from 8 a.m. to 6 p.m. with scheduled two-hour lunch breaks, and rarely working on weekends.

### Exposure vs. Breach

<table>
<thead>
<tr>
<th>Exposure</th>
<th>Breach</th>
</tr>
</thead>
</table>
| Multiple types of attacks over an extended period of time by persistent attackers | • 500TB of confidential data  
• Many legal issues  
• Continuing bad press |
| Compromised HVAC partner, then targeting POS                              | • 100M records lost  
• Loss of $500m to $750m in revenue  
• Removal of CEO |
| Employee phishing                                                         | • 145M user passwords  
• 7% loss in revenue growth |
| Targeted partner network and potential insiders                           | • 56M records  
• “We sell hammers” quote in the media |
| Sophisticated cyber attack                                                | • 78 Mil customer records leaked |
| Target attack                                                             | • 81Mil transferred from BB to Phillipines and Shri Lanka |
FireEye – Incident Response Investigations

FireEye hired to help probe Bangladesh Bank heist - source

BY JIM PINKLE

Anthem was the victim of a sophisticated cyber attack –

Important message from Joseph Swedish, President and CEO

To our valued provider partner:

Safeguarding your patients’ personal, financial and medical information is one of our top priorities, and because of that, we have state-of-the-art information security systems to protect your data. However, despite our efforts, Anthem was the target of a very sophisticated external cyber attack. These attackers gained unauthorized access to Anthem’s Information Technology (IT) system and have obtained personal information from our current and former members such as their names, birthdays, medical IDs/Social Security numbers, street addresses, email addresses and employment information, including income data. Based on what we know now, there is no evidence that credit card, provider or medical information, such as claims, test results, or diagnostic codes were targeted or compromised.

Once the attack was discovered, Anthem immediately made every effort to close the security vulnerability, contacted the Federal Bureau of Investigation (FBI) and began fully cooperating with their investigation. Anthem has also retained Mandiant, one of the world’s leading cybersecurity firms, to evaluate our systems and identify solutions based on the evolving landscape.
Sự kiện nổi bật trong năm 2015: Nhóm tân công APT30

Nhóm tân công APT30 được diện danh là nhóm tân công quốc gia Trung Quốc đã thực hiện một loạt các cuộc tấn công mạng có tổ chức và chuyên nghiệp vào các quốc gia trong khu vực Đông Á, bao gồm Việt Nam, Trung Quốc, Hàn Quốc, Nhật Bản, Philippines, Malaysia, Indonesia, Singapore, Brunei, và Việt Nam. Nhóm này đã tấn công vào các cơ quan quan trọng, các nhà chức trách và các doanh nghiệp lớn để thu thập thông tin và chiếm đoạt tài sản.

Vào năm 2015, nhóm tân công APT30 đã tấn công vào các cơ quan quan trọng, các doanh nghiệp lớn và các nhà chức trách của Việt Nam. Nhóm này đã sử dụng các chiến lược tấn công mạng tinh vi, bao gồm việc sử dụng mã độc, lừa dối người dùng và việc truy cập vào tài nguyên thông tin nhạy cảm.

Vì vậy, việc đánh giá và phản ứng lại các hoạt động tấn công của nhóm APT30 là một vấn đề quan trọng. Chính phủ và các cơ quan chính trị cần phải tìm cách tăng cường các biện pháp phòng ngừa và phản ứng để giảm thiểu ảnh hưởng của các hoạt động tấn công mạng này. Sự hợp tác giữa các quốc gia trong khu vực cũng là một yếu tố quan trọng trong việc đối phó với các hoạt động tấn công mạng này.
APT Example: **Council on Foreign Relations** attack

- **Client PC**
  - Custom Tools

- **HTTP**
  - Check browser version, country, first visit
  - Exploit for IE8
  - Backdoor download
  - C&C Callback

- **Compromised Domain**
  - [http://www.cfr.org](http://www.cfr.org)

- **Vulnerability Exploit**
  - Compromised Domain
  - Vulnerability
  - IE8

- **Malware Download**
  - Backdoor

- **C&C Callback / Data Exfiltration**
  - C&C Server: Dynamic DNS
  - provide.yourtrap.com

- **Lateral Spread**
  - XOR (0x83)

Independent, nonpartisan membership organization, think tank, and publisher:
- Influential in US foreign policy decisions
- Preeminent personalities and corporations as members
- Develops foreign policy leaders
- Accessed by lawmakers, govt. officials
APT: Multi-Staged & Multi-Vector Cyber Attack

1. Exploitation of System
2. Malware Executable Download
3. Callbacks and Control Established
4. Lateral Spread
5. Data Exfiltration

Exploit Detection is Critical. All Subsequent Stages can be Hidden or Obfuscated.
Demo APT Attack

1. Targeted Spearphish eMail sent

Messages with Malicious Binary and Link

Life Cycle

1. System Exploit
2. Binary Loading (if malicious code not in email)
3. Call-Back
4. Data Exfiltration

Victim

Mail Server

Active
Load Malware

Malware Code Host (Dropper)

Instructions

Data

Call-Back Server/Command and Control
### Why can’t our existing investment address such threats?

<table>
<thead>
<tr>
<th>Firewalls/NGFW</th>
<th>IPS</th>
<th>Secure Web Gateways</th>
<th>Anti-Spam Gateways</th>
<th>Desktop AV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block IP/port connections,</td>
<td>Attack-signature based</td>
<td>Some analysis of script-based</td>
<td>Relies largely on antivirus,</td>
<td>Signature-based detection (some</td>
</tr>
<tr>
<td>application-level</td>
<td>detection, shallow</td>
<td>malware, AV, IP/URL filtering;</td>
<td>signature-based detection (some behavioral);</td>
<td>behavioral); ineffective vs.</td>
</tr>
<tr>
<td>control, no visibility into</td>
<td>application analysis, high-</td>
<td>ineffective vs. advanced</td>
<td>no true spear phishing protection</td>
<td>advanced targeted attacks</td>
</tr>
<tr>
<td>exploits and ineffective vs.</td>
<td>false positives, no visibility into</td>
<td>targeted attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>advanced targeted attacks</td>
<td>advanced attack lifecycle</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Despite all this technology **95% of organizations are compromised**
An Old Model to Combat New Threats?

Legacy Pattern-Matching Detection Model

- Signature-based
- Reactive
- Only known threats
- False positives

New Virtual Machine-Based Detection Model

- Signature-less
- Dynamic, real time
- Known/unknown threats
- Minimal false positives
Chinese hackers allegedly spying on US weapons programs

Chinese hackers have gained access to secret designs for a slew of sophisticated US weapons programs, officials said Tuesday, possibly jeopardizing the American military’s technological edge.
Company Overview

• Since 2004 with HQ in Milpitas, CA
• Management Team
  – CEO Dave Dewalt (Former CEO of McAfee)
  – CTO, CSO Ashar Aziz (Former Sun MicroSystem)
  – Enrique Salem (Former CEO of Symantec)
  – Robert Lentz (Former CISO of US DOD)
  – Many more…
• Forbes
  “Hottest Security Company in Silicon Valley”
• Top-tier investors - Sequoia Capital, NorWest, Juniper, Silicon Valley Bank, Goldman Sachs, In-Q-Tel
IDC Market Research 2013

http://www.idc.com/getdoc.jsp?containerId=242346
Frost & Sullivan APT Market Research 2014

Competitive Analysis—Market Share

Key Takeaway: FireEye dominated the market, with Palo Alto Networks, Zscaler, and Trend Micro posing stiff competition.

Total APT Solutions Market: Percent Sales Breakdown, Asia-Pacific, 2014
Revenue = $117.9 Million

- FireEye: 23.2%
- Palo Alto Networks: 14.1%
- Zscaler: 9.5%
- Trend Micro: 7.5%
- Others* 17.8%
- AtrendLens: 4.6%
- Check Point: 4.6%
- Lastline: 5.0%
- Fortinet: 6.5%
- Websense: 3.5%
- Cisco: 4.4%


Note: All figures are rounded. The base year is 2014. Source: Frost & Sullivan
RESULTS

Detection Rate

- FireEye: 99.14%
- Trend Micro: 33.62%
- Check Point: 24.14%
- Vendor A: 21.55%
- McAfee: 12.93%
- AhnLab: 6.90%
- Fidelis: 5.17%
Upgrade Your Perimeter and Network-Based Security
- IPsec and SSL VPN Remote Access Connections
- Next-Generation Firewalls
- Intrusion Prevention Devices Best Practices
- Web Application Security

- **Advanced Threat Protection Appliances**

Advanced Threat Protection Appliances

**Best Practices**

Evaluate and deploy a network-based advanced threat detection/prevention technology to reduce the potential impact of zero-day malware and other targeted attacks.

Source: https://www.gartner.com/doc/2589029/best-practices-mitigating-advanced-persistent
On prevention vs. detection, Gartner says to rebalance purchasing

"Vendors evolving, some more than others [...] FireEye Inc. is at the top of the list, MacDonald said, not only with its January acquisition of Mandiant, but also recently by adding integrated, low-cost IPS capabilities to its threat prevention platform."

Neil MacDonald, Vice President and Distinguished Analyst, 20 year Gartner Analyst
Most Targeted verticals: Asia 2013

1. Financial Services
2. Government: Federal
3. High-Tech
4. Chemicals/Manufacturing/Mining
5. Services/Consulting/VAR
6. Education: Higher Education
7. Telecom (Internet, Phone & Cable)
8. Energy/Utilities/Petroleum Refining
9. Entertainment/Media/Hospitality
10. Government: State & Local

Source: FireEye Labs
Q4 2013 FireEye PoV By the Number

358 FireEye Web PoV Customers

98% Compromised

22% Had APT

Disclaimer: Data is from Web PoV and only when appliances have 2-way sharing license.
**Industry: Financial**

**Top APT**

<table>
<thead>
<tr>
<th>APT</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backdoor.APT.Houdini (29%)</td>
<td>Loss of sensitive information. Houdini is believed to be the developer’s name of VBS-based RAT known to target international energy industry and take part in spammed email campaign.</td>
</tr>
</tbody>
</table>

**Top Malware**

<table>
<thead>
<tr>
<th>Malware</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploit-browser (66%)</td>
<td>An attempt to compromise endpoint by exploiting vulnerability in the Web browser. If successful, attacker can install and execute malicious software without end users consent.</td>
</tr>
<tr>
<td>Exploit-kit.Neutrino (54%)</td>
<td>Infection with several types of malware that steal credentials or restrict access to computer and demand ransom.</td>
</tr>
</tbody>
</table>

**FireEye PoV**

- 71 Customers
- 99% Had APT
- 10% Customers Compromised

**Table (Per Week)**

<table>
<thead>
<tr>
<th>Category</th>
<th>Average</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Exploit</td>
<td>0.78</td>
<td>5.68</td>
</tr>
<tr>
<td>Malware Download</td>
<td>90.48</td>
<td>3183.1</td>
</tr>
<tr>
<td>Unique Malware</td>
<td>6.26</td>
<td>174.1</td>
</tr>
<tr>
<td>Unique Callback</td>
<td>24.21</td>
<td>1405.78</td>
</tr>
<tr>
<td>Impacted Hosts</td>
<td>34.85</td>
<td>1602.83</td>
</tr>
</tbody>
</table>
FSI Banking Customer

• Detected different numerous trojans and Backdoor.APT callbacks

• Commodity malwares (Trojan.Sality, Trojan.Ramnit, Trojan.Sasfis)

• Botnet callbacks (Conficker)

• APT Malwares (Backdoor.APT.Mongrall)

• Malicious binaries files and archives
<table>
<thead>
<tr>
<th>Vertical</th>
<th>Companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet, Networking, High Tech</td>
<td>Adobe, eBay, Juniper Networks, Yahoo!, Ricoh,</td>
</tr>
<tr>
<td></td>
<td>Cisco, VeriSign, PayPal, Facebook, Netflix,</td>
</tr>
<tr>
<td></td>
<td>Samsung, Twitter, Zynga</td>
</tr>
<tr>
<td>Financials, Utilities,</td>
<td>Prudential, PG&amp;E, General Atomics, HHMI,</td>
</tr>
<tr>
<td>Healthcare, Manufacturing</td>
<td>Thales, Simplot, UBS, Sallie Mae, blue of</td>
</tr>
<tr>
<td></td>
<td>California, Deloitte, Kynikos Associates</td>
</tr>
<tr>
<td>Federal Government</td>
<td>Government of Texas, Social Security</td>
</tr>
<tr>
<td></td>
<td>Administration, USA, General Aviation</td>
</tr>
<tr>
<td></td>
<td>Administration, Intelligence Community</td>
</tr>
<tr>
<td></td>
<td>NIST, MITRE, Sandia National Laboratories, USDA</td>
</tr>
<tr>
<td>Higher Education</td>
<td>Harvard, Stanford, UC Berkeley, UC Davis,</td>
</tr>
<tr>
<td></td>
<td>University of Washington, University of Oregon</td>
</tr>
<tr>
<td>State &amp; Local Government</td>
<td>Alameda County, City of Cupertino, County of</td>
</tr>
<tr>
<td></td>
<td>Ventura, mdrc, Vermont, DFW, General Assembly,</td>
</tr>
<tr>
<td></td>
<td>Illinois Momentum 2014</td>
</tr>
</tbody>
</table>
FireEye Technical Overview
Almost all security vendors will now say:
“Now I have a “APT” (Sandbox) Solution too!”
Typical FW + Sandbox Solution

Limitations of Sandbox approach

- No hardened hypervisor
- No multi-vector protection
- No multi-flow analysis
- In-the-clear executable files only
- Incoming file rate of 3-5/hour
- No cross-matrix of vulnerable SW
- No web exploit detection!
Why FW + Sandbox Solutions Miss APT Attacks

Limitations of Sandbox approach
- No hardened hypervisor
- No multi-vector protection
- No multi-flow analysis
- In-the-clear executable files only
- Incoming file rate of 3-5/hour
- No cross-matrix of vulnerable SW
- No web exploit detection!

This is NOT an APT prevention solution!
Threat Visibility of (FW + Sandbox) vs MVX

- Point of Attack
  - Email
  - File
  - Web
  - Sandbox
  - Mobile

- MVX
  - Multi vector
  - Multi flow
  - 1M+ objects/hour

- 8+ years R&D

- >1M Objects/hour

- <10 Objects/hour

- Unsophisticated Crimeware

- APT
FireEye Platform Advantages

- Multi-Flow Analysis
- Thousands of Permutations (files, OS, browser, apps)
- Bi-directional Cloud Sharing
- Multi-Vector Analysis
- Correlation of Information
- Time to Protection

MVX
FireEye Platform Advantages

- Multi-Flow Analysis
- Thousands of Permutations (files, OS, browser, apps)
- Multi-Vector Analysis
- Correlation of Information
- Bi-directional Cloud Sharing
- Time to Protection
FireEye Platform Advantages

- Multi-Flow Analysis
- Thousands of Permutations (files, OS, browser, apps)
- Multi-Vector Analysis
- Correlation of Information
- Bi-directional Cloud Sharing
- Time to Protection

Additional features:
- Web
- Email
- File
- Mobile
FireEye Platform Advantages

- **Multi-Flow Analysis**
- **Thousands of Permutations** (files, OS, browser, apps)
- **Bi-directional Cloud Sharing**
- **Time to Protection**
- **Cross-correlated Intelligence**
- **Multi-Vector Analysis**

Cross-enterprise platforms include:
- MVX
- Web
- Email
- File
- Mobile
- CMS
FireEye Platform Advantages

- Multi-Flow Analysis
- Thousands of Permutations (files, OS, browser, apps)
- Bi-directional Cloud Sharing
- Time to Protection

Cross-enterprise

Dynamic Threat Intelligence Cloud

MVX

Web
Email
File
Mobile

Cross-correlated Intelligence

Multi-Vector Analysis

Dynamic Threat Intelligence Cloud

CMS
FireEye Platform Advantages

- Multi-Flow Analysis
- Thousands of Permutations (files, OS, browser, apps)
- Bi-directional Cloud Sharing
- Time to Protection
- Dynamic Threat Intelligence Cloud
- Real Time Private Scalable Cross-Enterprise
- Cross-enterprise
- Cross-correlated Intelligence
- Multi-Vector Analysis
- CMS
- Mobile
- File
- Email
- Web
- MVX
FireEye Platform Advantages

- Multi-Flow Analysis
- Thousands of Permutations (files, OS, browser, apps)
- Multi-Vector Analysis
- Bi-directional Cloud Sharing
- Cross-correlated Intelligence
- Time to Protection

Dynamic Threat Intelligence Cloud

Cross-enterprise

Real Time
Private
Scalable
Cross-Enterprise
FireEye – giải pháp Tổng thể phòng chống APT

- Internet
  - Egress Router
  - Firewall
  - Core Switch
  - LAN
    - Network Threat Prevention (NX)
    - Forensics Platform (AX)
  - Clients
  - Anti-Spam GW
  - Email Threat Prevention (EX)
  - Mail Servers

- Datacenter
  - File Threat Prevention (FX)

- Cloud
  - Dynamic Threat Intelligence (DTI)
  - Mobile Threat Prevention (MTP)
  - Central Management (CM)
  - Network Forensics (PX)

- Network Threat Prevention (NX)
- Email Threat Prevention (EX)
- Forensics Platform (AX)
- File Threat Prevention (FX)
THANK YOU