FortiGuard – Advanced Threat Response

Derek Manky
Global Security Strategist

FORTINET
High Performance Network Security

Threat Landscape Update & Strategy

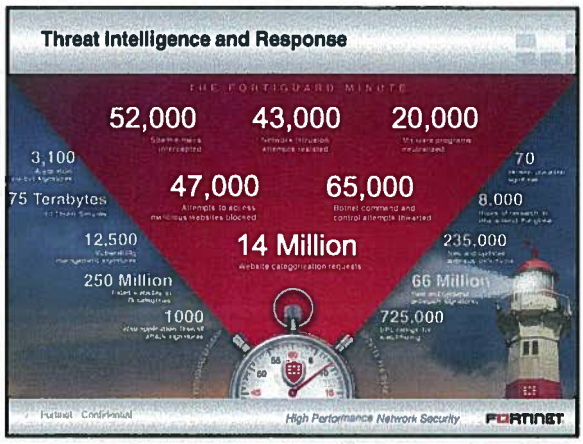
What is FortiGuard?

FortiGuard Services

Threat Intelligence & Response

- 200+ Researchers
- Millions of sensors
- Collaboration
  - »Threat Monitoring

Fortinet's Own



General Threat Environment

- Despite $30bn in IT security spending in 2012, attackers get through
  - Gartner estimates 3-5% of endpoints are compromised in the average enterprise
  - PwC reports that 20% of large organizations were penetrated by outsiders in 2012
  - Verizon investigated 47,000 security incidents in 2012
- 2013 was a tough year, including for financial services

Dec/Feb: ATM theft (across 20 countries) | March/Aug 15: New wave of DDoS attacks (JP Morgan C4L AMEX RBOS) | June: Vendor system hacked, client info stolen (Shore financial) | July: Beta breached, malware spreads to 2k+ computers, info stolen | Oct/Nov/Dec: Intrusion and theft of card info (Target, SA food service)

- Security risks range from DDoS to Direct Breach to Vendor Breaches to...

ATM Theft Closes 2012, Opens 2013

Dec/Feb: ATM theft (across a 20 countries) | March/Aug 15: New wave of DDoS attacks (JP Morgan C4L AMEX RBOS) | June: Vendor system hacked, client info stolen (Shore financial) | July: Beta breached, malware spreads to 2k+ computers, info stolen | Oct/Nov/Dec: Intrusion and theft of card info (Target, SA food service)

- **Incident**
  - Hackers infiltrated an Indian credit-card processing company
  - Then limits on the cards were raised
  - Finally, teams around the world made withdrawals
- **Damages/Resulting Action**
  - 4500 transactions, $5m in December
  - 36,000 transactions, $40m in Feb

- **Recommendations**
  - IPS
  - Vulnerability Management

http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-theft.html?pagewanted=all&_r=0

Ditto for DDoS in 2012/2013

Dec/Feb: ATM theft (across 20 countries) | Dec/March/Aug 15: New wave of DDoS attacks (Bank of West, Citi, AMEX, RBC®) | June: Vendor system hacked, client info stolen (Shore financial) | July: Bank breached malware spreads to 23 computers, info stolen | Oct/Nov/Dec: Intrusion and theft of card info (Target, SA food service)

- **Incident**
  - Multiple counts of DDoS taking online banking offline
  - Sometimes just a service interruption
  - Other times coordinated with financial theft
- **Damages/Resulting Action**
  - $900,000 stolen from one account
  - Multiple material impacts reported in financials
- **Recommendations**
  - Leverage DDoS service and products together
  - Big Data / Analytics

Financials only as strong as the weakest link

Dec/Feb: ATM theft (across 20 countries) | March/Aug 15: New wave of DDoS attacks (JP Morgan Citi, AMEX, RBC®) | June: Vendor system hacked, client info stolen (Shore financial) | July: Bank breached malware spreads to 23 computers, info stolen | Oct/Nov/Dec: Intrusion and theft of card info (Target, SA food service)

- **Incident (unconfirmed)**
  - Mortgage provider relies on vendors to process client information
  - Vendor's server was breached and personal information stolen in June, notified by vendor in August
  - Follows previous breach of systems from December through January
- **Damages/Resulting Action**
  - Cost of notification and credit monitoring
  - Cost of forensic investigation
  - Increased controls internally and with vendors
- **Recommendations**
  - Vendor selection (review Product Security)
  - Incident response

And even a single compromise can have significant impacts

Dec/Feb: ATM theft (across 20 countries) | March/Aug 15: New wave of DDoS attacks (JP Morgan Citi, AMEX, RBC®) | June: Vendor system hacked, client info stolen (Shore financial) | July: Bank breached, malware spreads to 23 computers, info stolen | Oct/Nov/Dec: Intrusion and theft of card info (Target, SA food service)

- **Incident (unconfirmed)**
  - Employee computer breached, malware spreads to 23 PCs
  - Designed to capture on-screen information
  - Initial compromise occurred in February, undetected until May
- **Damages/Resulting Action**
  - Believed to impact entire customer base (116k accounts)
  - Costs of notifications and forensic investigation
- **Recommendations**
  - UTM/Layered Security
  - Application Control / Egress Inspection

Retail Breaches Impact the Banks too

Dec/Feb: ATM theft (across 20 countries) | March/Aug 15: New wave of DDoS attacks (JP Morgan, Citi, AMEX, RBOS) | June: Vendor system hacked, client info stolen (Shore financial) | July: Bank breached, malware spreads to 23 computers, info stolen | Oct/Nov/Dec: Intrusion and theft of card info (Target, SA food service)

- **Incident (unconfirmed)**
  - Attackers purchased malware "BlackPOS" and slightly modified it to evade AV detection
  - Entry via a web server and subsequently installed the malware on Windows PoS devices
  - "Scraped" data was staged within Target on a server with FTP access and exfiltrated
- **Recommendations**
  - IPS
  - Sandbox
  - DLP

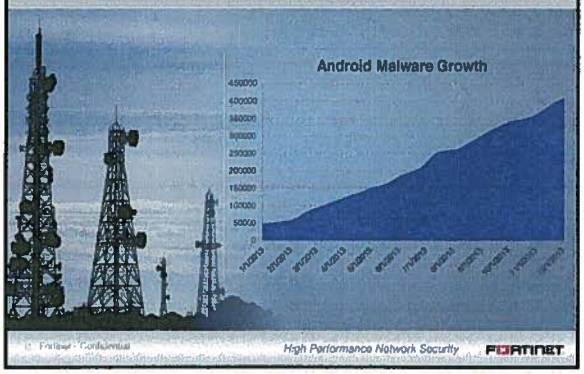
Banks may take their pound of flesh from Target over breach

Retail Breaches Impact the Banks Too

Dec/Feb: ATM theft (across 20 countries) | March/Aug 15: New wave of DDoS attacks (JP Morgan Citi, AMEX, RBOS) | June: Vendor system hacked, client info stolen (Shore financial) | July: Bata breached, malware spreads to 23 computers, info stolen | Oct/Nov/Dec: Intrusion and theft of card info (Target, SA food service)

- **Incident**
  - Attackers embedded Dexter malware on PoS
  - Customer payment information was scraped, stolen
  - Information sold and phony cards created
  - Infiltration/exfiltration unclear
- **Damages/Resulting Action**
  - Unusual level of fraud, ~$1m lost
  - Forensic investigation, incident response committee
- **Recommendations**
  - IPS
  - Sandbox/Antimalware

Threat Trends – Mobile (2013)



Advanced Threat Protection

Advanced Persistent Defense

Three Step Approach to APT Defense

Step 1 - Mitigate
- Mitigate threats before they enter your network
- Proactive is key

Step 2 - Discover
- Discover threats that have or tried to enter the network

UTM & NGFW | Sandbox | Incident Response

Summary

- **Defense Strategy**
- **Proactive:**
  - Protect Against APT (Gateway/MSS)
    - Threats need microseconds to be damaging
    - Rely on security experts
- **Reactive:**
  - Incident Response
    - Have a resource for incident response
    - Understand the threat
- **Free Proactive Planning**
  - Patch Management
  - Employee Education
    - Free RSS Feeds
    - Workshops
  - Leverage Managed Security
  - Encryption
  - Redundancy
  - Retention
  - Can be indirect through security vendor
  - BYOD planning