WHERE EXISTING SECURITY MEASURES FAIL

Dr. Felix Leder <felix.leder@bluecoat.com>

André Engel <andre.engel@bluecoat.com>
BUSINESS ASSURANCE TECHNOLOGY

- Security and Policy Enforcement Center
  - SG & SG-VA Web Security Service
  - WebFilter
  - SSL Visibility
  - Content Analysis
  - Malware Analysis
  - DLP
  - FW/IDS on X-Series

- Mobility Empowerment Center
  - Mobile Device Security Service

- Trusted Applications Center
  - Web App Reverse Proxy

- Performance Center
  - MACH5 CacheFlow
  - PacketShaper

- Resolution Center
  - Reporter SW
  - Hosted Reporting Intelligence Center
  - Security Analytics Appliance with Threat Blades

BUSINESS ASSURANCE PLATFORM

- Open Environment for Best-of-Breed Solutions
- Proxy-Based Architecture
- Global Cloud Infrastructure
- Threat, Web & Application Intelligence
- Scalable Virtualization Platform
- Rich Security Analytics
LEADING CUSTOMER FRANCHISE

86% of FORTUNE Global 500 Companies

Over 30% of FORTUNE Global 10K Companies

16 Largest Service Providers in the World

Worldwide Government Organizations

Over 15,000 highly satisfied customers spanning major enterprises worldwide
ADVANCED PERSISTENT THREAT

“Let me think who is the target?”

“Well its YOU ….still YOU”
“Your company assets”

“YOUR Employees”
“social engineering becomes the easy way “

“YOUR Customers”
“breach you as the weakest Link”

Firewalls
IDS/IPS
Patches
Antivirus

IDS/IPS
Firewalls
Patches
Antivirus

“Let me think who is the target?”

“Well its YOU ….still YOU”
“Your company assets”

“YOUR Employees”
“social engineering becomes the easy way “

“YOUR Customers”
“breach you as the weakest Link”
Most popular hash tag ever

- 6500 time tweeted in 1 minute
- 3.4 million tweet in just one 24 hour period

Miscreant say “Jesus Charlie too”

- Exploited #JesuisCharlie hash tag
- Used RAT Dark Comet
Internally a computer:
  - CPU, RAM (you can buy more)
  - Ethernet ports / WiFi
  - Hard disk

Hard disk
  - Often stores the full print history
    - Public announcements
    - Contracts
    - Financial numbers
    - Strictly confidential documents

“Smart printers” may contain original document type

- Do you have anti-virus on your printer?
- When did you last update your printer’s firmware?
MOBILE DEVICES

- **BYOD is happening**
  - Are you sure there are no private wifi hotspots on your premises?

Access to emails, documents, contacts

- **Device has sensors**
  - Microphone
  - Camera
  - GPS
  - Light sensor
  - Accelerometer
"I HAVE NOTHING TO HIDE"

... AS EASY AS \texttt{Something.to lose}

- SEARCH
  - Results: Found 683 Applications!
  - Displaying Results 0-30 Of 683
  - NEXT 30>>
Android is not limited to phones/tablets

- Fridges
- Watches/ goggles / wearable’
- ...

- Full Internet Connectivity
- Known bugs/vulnerabilities

Every product has bugs:

- Depends on 3rd party?
- Google is not always patching (Webview vulnerability < Kitkat
Antivirus exists for mobile devices
• Impossible for deep analysis without jail-breaking the phone (same security for everybody is a good concept)
• Only sees threats on the surface
• Usually limited to known threats

Attackers can use exploits and undermine security

⇒ Asymmetric scenario

Old devices are usually not updated by the vendor
WAR STORY – TARGETTING EXECUTIVES, POLITICIANS, MILITARY

Who?

Where?

When?

What?
“Yeah we have ANTIVIRUS”

Hey what’s about your egress points themselves?

“Yeah we have Firewalls”
POINT OF SALES

Restaurant: Ordering, bookkeeping, billing

Shop: Payment, automatic ordering

Larger orgs: Customer profiling

Windows embedded POS ready

How to install endpoint security/antivirus?
**Prevention is required to remove the noise:**

- **Host antivirus**
  - Removes mass malware
  - As soon as something is on the endpoint, it is too late
  - Printers, fridges, mobile devices?

- **Network content analysis**
  - Stops before reaching endpoint
  - Can react on outgoing data
  - What about SSL?
Whitelists:
- Works (if not compromised)
- Try once and never try again

Reputation / Big-data / Crowd
- You benefit from other incidents seen across the world in real-time
- Machine learning about “dirty” machines
- Blue Coat processes
  - ~300,000 files / 24h
  - ~6,000,000,000 URL ratings / 24h
BURNING QUESTION TODAY

How To Prevent My Organisation From Suffering Security Breaches?

Am I Ready To Respond?

Security Breach will Happen!
NETWORK TO ENDPOINT VISIBILITY AND DEFENSE

Five Styles of Advanced Threat Defense

Built Upon
Full Network Visibility
+
Full Endpoint Visibility
Detect and react quickly, and learn

Big-data inside your organization?
• Data collection
• Correlation
• Are you able to track every step of intruders in your network?

Detection capabilities for unknown events – Sandboxing
• What about mobile?
• Really targeted malware is environment specific
• “Gold images” – customize to look like one of your real systems
• Really targeted can evade “generic behavioral detection”
LIFECYCLE DEFENSE

Ongoing Operations
Detect & Protect
Block All Known Threats

Incident Resolution
Investigate & Remediate Breach
Threat Profiling & Eradication

Fortify & Operationalize

Retrospective Escalation

Incident Containment
Analyze & Mitigate
Novel Threat Interpretation

Unknown Event Escalation

GLOBAL INTELLIGENCE NETWORK
Attacker asymmetry:

Targeted to bypass general-purpose detections

Tripwires to turn tables:
• Spot irregular movements in network
• Custom patterns in sandboxes
• Bait files in sandboxes
• Set up “honeypots”
DON'T BE THE VICTIM
**MESSAGE**

**APTs are Omni-present**

**You don’t control your infrastructure any longer**

**Continuous response (tools)**
- Collect the right data
- Ability to correlate
- Learn

**Tripwires are essential**
QUESTIONS?! 

Felix Leder <felix.leder@bluecoat.com>
André Engel <andre.engel@bluecoat.com>