Countering Advanced Persistent Threats

Eric Chan
Solution Consulting Director
SouthEast Asia & Hong Kong
Some words about APT...
Some Numbers…

- $30bn in IT security spending in 2012 ... but attackers get through
- Gartner estimates 3-5% of endpoints are compromised in the average enterprise
- PwC reports that 24% of large organizations were penetrated by outsiders in 2013 (Up from 20% in 2012)
- Verizon investigated 63,000 security incidents in 2013 (Up from 47,000 in 2012)
2013: The Rise of the Advanced Persistent Threats

- 2013 was chock full of data breaches

- Many breaches remain undiscovered for months or a year
One Recent Example: Target

Target hack strips banks and credit unions of $200M

As Data Breach Woes Continue, Target's CEO Resigns
By Michael Riley and Dune Lawrence | May 05, 2014
One Recent Example: Target

http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/
Anatomy of APTs

- **Single out individual organizations** (or a small group of similar organizations in an industry)
- **Target** employees with **attacks crafted to fool even the wary**
- Leverage malware modified (and often tested) to **bypass traditional security controls**
- **Move stealthily** within the organization in search of data
- **Ex-filtrate that data** over a period of time
The APT Toolkit

- An attacker has a substantial arsenal of tools at the ready in order to launch and maintain their attack
  - Modified and often tested *malwares* to bypass traditional security controls
  - **Zero-day** and other exploits
  - **Social Engineering** aims to make a human target believe an attack is coming from a trusted source
  - **Insiders and recruits** can be helpful to install the attack inside a non-connected network
  - **Forged and Fake certificates** to impersonate a trusted web site
Zero-day Vulnerabilities
aka The Known Unknowns

- [...] attack that exploits a previously unknown vulnerability in a computer application
- A key component for maximizing the success of an APT
- Easy to find or buy on continuously growing grey market

<table>
<thead>
<tr>
<th>Known</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability publicly known</td>
<td>Vulnerability known to privileged group only</td>
</tr>
<tr>
<td>Risk assessment and mitigation possible</td>
<td>Risk assessment and mitigation not possible</td>
</tr>
<tr>
<td>Vulnerability not discovered</td>
<td>No exploitation or risk through not yet discovered issues</td>
</tr>
</tbody>
</table>

Advanced Persistent Threats

Something Different?
Disguise, Survive, Impact

**Disguise**
- Advanced threats focus on disguise to slip past security detection

**Survivability**
- Persistent threats aim to survive on systems as long as possible

**Impact**
- Threat to Hard drive data
- Stolen IP, customer data
- Blackmail & Ransom
- Critical infrastructure

Detect Disguise, Kill the Chain
Reduce Survivability, Break Impact
Protecting against Advanced Threats
Different Approaches to Addressing Advanced Threats

Figure 1. Five Styles of Advanced Threat Defense

Source: Gartner (August 2013)

Different Approaches to Addressing Advanced Threats

Gartner's "Five Styles of Advanced Threat Defense" Framework
Enterprises should consider using at least two in combination

- **Style 1- Network Behavior Analysis**
  - Establish baselines of normal traffic patterns, look for anomalies

- **Style 2- Network Forensics**
  - Capture and replay network traffic for incident response

- **Style 3- Payload Analysis**
  - Execute code in a contained, “sandbox” environment

- **Style 4- Endpoint Behavior Analysis**
  - Monitor the production system configuration for anomalies

- **Style 5- Endpoint Forensics**
  - Collect data from endpoints to aid in incident response and forensics
The Sandbox
What do we mean?

Sandbox has many meanings…

- Container to hold sand to improve rail adhesion
- Shallow playground construction to hold sand
- Virtual container in which untrusted programs can be safely run
- Soviet Anti-Ship Missile (SS-N-12)
Payload Analysis (aka “sandboxing”)

• **What is it?**
  » Virtual container, reflecting an end user desktop, in which untrusted programs can be safely examined

• **What happens in it?**
  » Code is executed in an contained, virtual environment
  » Activity is logged and is analyzed for suspect characteristics
  » Rating is determined based on system, file, web and traffic activity

• **Why is it important?**
  » Traditional security looks at static attributes (signature, heuristic, pattern, reputation, etc.) rather than dynamic activity
  » In many cases, a site or code is just the first, small stage

Unsafe action, escape attempt
Controlled communication inspection
Advanced Persistent Threat Solutions

Strategies for Dealing with Advanced Targeted Attacks (June 2013)

Figure 1. Defending Against Targeted Attacks Requires Lean-Forward Technologies and Processes

- Endpiont Protection
- Network Segmentation
- Firewall/IPS
- Secure Web Gateway

- NAC
- Mobile Device Security
- App. Whitelisting/Blacklisting
- SIEM
- Next-Generation Firewall

- Net/Computer Forensics
- Threat Intelligence
- Sandboxing
- DLP/DAM
- DAST

Fundamentals

Advanced Technology

Lean Forward

Vulnerability Management
Change Control/Privilege Management
Incident Response

Process

Situational Awareness

DAM = digital asset management; DAST = dynamic application security testing; DLP = data loss prevention; IPS = intrusion prevention system; NAC = network access control; SIEM = security information and event management.
Fortinet’s Approach: FortiSandbox
Introducing FortiSandbox

Defense against APTs & Unknown Threats
Advanced Threat Protection solution designed to identify and help customers thwart the highly targeted and tailored attacks that increasingly bypass traditional defenses and lurk within networks.

Advanced Threat Protection
- Multi-layered filtering with Code Emulator, AV engine, Cloud query and Virtual OS sandbox
- Handles multiple file types, includes files that are encrypted or obfuscated
- Examine files from various protocols, included those that uses SSL encryption

Flexible Operation Modes
- Receives file sample using integration with FortiGate/FortiMail, sniffer mode and manual file uploads
- Capture files from remote locations using deployed FortiGates

Monitoring and Reporting
- Detailed analysis reports and real-time monitoring and alerting
FortiSandbox - Design & Key Components

- Multi-tiered file processing optimizes resource usage to improve security, capacity and performance

Call Back Detection
- Identifies the ultimate aim, call back and exfiltration
  - FortiGuard verified

Full Virtual Sandbox
- Examines real-time, full lifecycle activity
  - Provides rich threat information

Code Emulation
- Quickly simulates intended activity
  - OS independent and immune to evasion/obfuscation

Cloud Query
- Checks FortiSandbox community intelligence
  - FortiGuard verified

AV Engine
- Applies top-rated (95%+ Reactive And Proactive) engine
  - Serves as an efficient pre-filter
FortiGate for Network Traffic Analysis

- Blocks known threats using IPS, Application Control, Web filtering, Botnet Detection and more
- Flags suspicious (or high risk) objects for more inspection
- Receives updated threat intelligence for inline prevention

FortiSandbox for Payload Analysis

- Runs objects in a contained environment, analyzing activity
- Provides a malicious or low, medium or high risk rating
- Uncovers threat lifecycle information and allows information sharing with FortiGuard experts for protection updates
FortiGate Integration

- Enable and configure the FortiSandbox in the FortiGate WebUI
  - FSA IP address
  - Notifier email address
Dashboard
On-Demand Drill-down Page
Detailed Analysis of Samples
**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

**Step 3 - Respond**
- **Respond** to any threats that have breached the network

- UTM & NGFW
- Sandbox
- Incident Response
The Integrated Approach

**UTM/NGFW:** FortiGate  
**+**  
**Sandbox:** FortiSandbox
Threat Research:
FortiGuard
FortiGuard

Threat Intelligence & Response

- 200+ Researchers
- 125,000+ Customers
- Millions of sensors
- Collaboration

» Threat Monitoring

Fortinet’s Own
Zero-Day Threat Research

BY THE NUMBERS

2013
› 18 Zero-Day Discoveries

2014
› 12 Remain Zero-Day (Q1)
› 100+ Goal for 2014
› Partnered with Exodus
› Includes SCADA

Since 2006
› 140 Zero-Day Discoveries

Yahoo Finance

Fortinet Leads Industry in Zero-Day Discoveries

Since 2006, Company’s FortiGuard Labs Has Uncovered 143 Zero-Day Vulnerabilities, 18 in 2013 Alone

SUNNYVALE, CA—(Marketwire - Apr 15, 2014) - Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- today announced that FortiGuard™ Labs, the global threat research and development center for Fortinet’s FortiGate® security appliances and FortiClient™ security software, has uncovered 143 new zero-day vulnerabilities in 2014...
FortiGuard AV Service
Final Words
NSS Labs Breach Detection Systems 2014 - Security Value Map

“A Recommend rating from NSS Labs indicates that a product has performed well and deserves strong consideration.”

A Caution rating from NSS Labs indicates that a product has performed poorly. Products that earn a Caution rating from NSS Labs should not be shortlisted or renewed.
NSS Labs BDS 2014 - FortiSandbox

- FortiSandbox Earned “NSS Labs Recommended” Status
- **Proven Security** – overall score of 99% for Breach Detection (majority in <3 minutes)
- **Real World Performance Validation for the Enterprise** – 1Gbps
- **Total Cost of Ownership** - $205
FortiSandbox: Advanced, Simple, Unique

More robust protection

- Dual-level Sandbox + Antimalware
  - Call Back Detection
  - Cloud Query
  - Virtual OS Sandbox
  - Code Emulation
  - AV Engine

Best price/performance

- All protocols, All functions, One box
  - MAIL (SMTP, POP3, IMAP, MAPI)
  - FTP
  - WEB
  - Instant Messenger

Integrated deployment

- Extension of In-place Infrastructure
  - Latest AV Signature Update
  - Headquarters (Enterprise Core)
  - File Submission Input Mode
  - Malicious Analysis Output

200K New Samples / Day (Monitored Threat Landscape)

50% Proactive Detection via AV Hour Zero, Day Zero
THANK YOU