Threats Moving To Mobile Devices

Source: McAfee Labs, Q1, 2013

2 billion new mobile endpoints in 2013!!

Source: McAfee Labs, Q1, 2013
The number of reports of data breaches via hacking, malware, fraud, and insiders has more than doubled since 2009. In the Q4 2011 alone we saw more than 40 breaches publically reported. Although the last three months are not the record holder in this area, data breach events continue to increase.
As operating systems and applications have become more “hardened” against attack, cybercriminals have turned their attention to more vulnerable subsystems. The “storage stack” is an increasingly popular target as a successful Master Boot Record attack allows the target to be rooted and either added to a botnet or otherwise compromised.
Spam vs. Ham

Global Email Volume, in Trillions of Messages

- Monthly Spam
- Legitimate Email

![Graph showing the comparison between monthly spam and legitimate email volume from April 2012 to March 2013. The graph indicates a significant increase in spam volume towards the end of the period.](image-url)
Attackers continue to use more and more “signed binaries” to circumvent endpoint malware detection. Using stolen or fabricated certificates, cybercriminals can often defeat standard firewall and intrusion prevention filtering rules.
Cybercriminals continued their movement away from botnets as the primary distribution mechanism for malware. They now prefer malicious web sites that implement “drive by downloads”. This approach has the advantage of being more nimble and less susceptible to law enforcement take downs.
FakeAlert is the McAfee name for rogue anti-spyware or anti-viruses which are considered as malware (Trojan sub-family). Also known as scareware.
The leading network threat this quarter came via Microsoft remote procedure calls. This was followed by a very close race between SQL-injection and cross-site scripting attacks. These two attacks are very much remote in nature, meaning they can be launched at selected targets around the globe.

Top Network Threat by Type

- Remote Procedure Call: 26%
- SQL Injection: 21%
- Cross-Site Scripting: 19%
- CGI Command Execution: 12%
- Browser: 15%
- Others: 7%

Network Threat Trends
APT Network Security Attack

Reconnaissance
- Map org chart (identify attack targets)
- Social reconnaissance (acquire email, IM, etc.)
- Recruit, blackmail insiders

Social Engineering Targeted Malware
- Phishing email (malicious PDF, DOC, etc. w/shellcode)
- Candy drops around blgd (Thumb drives, DVD’s)
- Gain physical access (impersonate cleaning crew, etc.)

Establish Covert Backdoor
- Gain elevated user privileges
- Laterally move within network & establish backdoors
- Inject additional Malware

Establish Command & Control Infrastructure
- Install system admin tools (Keyloggers, Trojans, etc.)
- Establish encrypted SSL tunnel

Complete Objectives
- Ex-filtrate Intellectual Property, Trade Secrets
- Install Trojans in source code
- Control critical systems

Maintain Persistence
- Revamp Malware to avoid detection
- Utilize other attack methods to maintain presence
- Continue monitoring networks, users, data
Stuxnet proved that malicious code can create a real world, kinetic response. Recent incidents directed at water utilities in the United States show that these facilities are of increasing interest to attackers. The more attention is focused on SCADA and infrastructure systems, the more insecurity seems to come to light. We expect to see this insecurity lead to greater threats through exploit toolkits and frameworks as well as the increased targeting of utilities and energy ICS systems in particular.
WHAT IT TAKES TO MAKE OUR ORGANIZATION SAFE

WHAT WE MUST KNOW...

- **Who** Am I Dealing With
- What Is the **Purpose**
- What **Data** Is Accessed
- Evaluate **Risk**
- Continuous **Monitoring**
- Learning and **Intelligence**

DATA WE NEED TO EVALUATE...

- IP Address
- Web Reputation
- Affiliations
- Email Address
- Network Activity
- File Reputation
- Application
- **Sender Reputation**
- DNS Server
- Domain(s)
- Web Activity
- Data Activity
- Protocol/Port
- Mail Activity
- URL

Domain(s)
Web Activity
Data Activity
Protocol/Port
Mail Activity
URL
Behavioral Analysis and Algorithmic Filtering

**VolumeRank**
EXAMINE RAW MAIL VOLUMES TO DETECT BULK SENDERS

Example: Spammers typically send in bulk, however many legitimate senders also send in bulk

**SocialRank**
EXAMINE RELATIONSHIP BETWEEN SENDERS TO DETERMINE GOOD PARTICIPANTS

Example: Spammers makes lots of outbound connects but hardly any inbound (unlike normal businesses)

**PersistenceRank**
EXAMINE LONGEVITY/CONTINUITY OF THE EMAIL SENDER

Example: Legitimate senders send e-mail on regular basis and they are stable (unlike spammers/zombies)
Discovering ZeroDay and Targeted Attacks
Live Walkthrough

McAfee Global Threat Intelligence

YOU FIND ON-PREM
- Advanced Threat Defense
- Target-Specific Sandboxing
- Emulation Engine
- Efficient AV Signatures
- GTI Reputation
- 3rd Party Threat Data
- JAR Analysis
- .exe Analysis
- PDF Analysis
- Network Threat Response

LIVE E-MAIL RECEIVED 08-27-2013

URL REDIRECT TO MALWARE SITE

MFE FINDS VIA CLOUD
REPUTATION CHECK OF THE URL PASSES

PayLoad appears to be a .scr inside a .zip

YOU FIND ON-PREM

- Advanced Threat Defense
- Target-Specific Sandboxing
- Emulation Engine

- Efficient AV Signatures
- GTI Reputation
- 3rd Party Threat Data

- JAR Analysis
- .exe Analysis
- PDF Analysis

Network Threat Response

MFE FINDS VIA CLOUD
Discovering ZeroDay and Targeted Attacks
Live Walkthrough

DUE TO ZERO DAY, FEW A/V SIGNATURE CATCHES

YOU FIND ON-PREM

- Advanced Threat Defense
- Target-Specific Sandboxing
- Emulation Engine
- Efficient AV Signatures
- GTI Reputation
- 3rd Party Threat Data
- JAR Analysis
- .exe Analysis
- PDF Analysis
- Network Threat Response

MFE FINDS VIA CLOUD

**virusTotal**

```
<table>
<thead>
<tr>
<th>SHA256</th>
<th>5e59097b1ab24f508a8e9fac859507c406689d599b6e4ba3b8880b78a7371eb</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>pdf_1Z12Y6169096771351.scr</td>
</tr>
<tr>
<td>Detection ratio</td>
<td>2 / 45</td>
</tr>
<tr>
<td>Analysis date</td>
<td>2013-08-27 15:27:00 UTC  (37 minutes ago)</td>
</tr>
<tr>
<td>TotalDefense</td>
<td>✓</td>
</tr>
<tr>
<td>TrendMicro</td>
<td>✓</td>
</tr>
<tr>
<td>TrendMicro-HouseCall</td>
<td>✓</td>
</tr>
<tr>
<td>VBA32</td>
<td>✓</td>
</tr>
<tr>
<td>VIPRE</td>
<td>✓</td>
</tr>
<tr>
<td>ViRobot</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>20130827</td>
</tr>
<tr>
<td></td>
<td>20130827</td>
</tr>
<tr>
<td></td>
<td>20130826</td>
</tr>
<tr>
<td></td>
<td>20130827</td>
</tr>
<tr>
<td></td>
<td>20130827</td>
</tr>
<tr>
<td></td>
<td>20130827</td>
</tr>
</tbody>
</table>
```

McAfee Global Threat Intelligence
Discovering ZeroDay and Targeted Attacks
Live Walkthrough

EXECUTION DEMONSTRATES:

- Efficient AV Signatures
- GTI Reputation
- Target-Specific Sandboxing
- Emulation Engine
- Advanced Threat Defense
- JAR Analysis
- .exe Analysis
- PDF Analysis
- Network Threat Response
- MFE FINDS VIA CLOUD

YOU FIND ON-PREM

MFE FINDS VIA CLOUD

McAfee Global Threat Intelligence

Malware Detected

The transferred file contained a virus and was therefore blocked.

URL: http://www.cooplapara.com.ar/blog/pdf_1212y6169096771351.zip
Media Type: application/x-executable

Advanced Threat Defense Results:
MATID Hash: 066bec76edda8366a0976485b2eb036f
MATID Severity: 5
File Name: pdf_1212y6169096771351_scr.exe
Verdict: Subject is malicious

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistence, Installation Boot Survival</td>
<td>5</td>
</tr>
<tr>
<td>Hiding, Camouflage, Stealthiness, Detection and Removal Protection</td>
<td>5</td>
</tr>
<tr>
<td>Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection</td>
<td>3</td>
</tr>
<tr>
<td>Spreading</td>
<td>5</td>
</tr>
<tr>
<td>Exploiting, Shellcode</td>
<td>4</td>
</tr>
<tr>
<td>Networking</td>
<td>0</td>
</tr>
<tr>
<td>Data spying, Sniffing, Keylogging, Ebanking Fraud</td>
<td>5</td>
</tr>
</tbody>
</table>

Behavior
- Installs itself into Appdata and behaves like Zbot
- Created active content under RECYCLER folder
- Infected Analyzer "boot" application
- Detected active embedded content in the sample
- Obtained and used icon of legit system application
- Examined content under Analyzer temporary directory
- Deleted file(s) from the Analyzer folder
- Injects into a different process memory and changes the access protection of the committed pages
- Wrote (injected) data to an area of a foreign process memory
- Set callback function to control system and computer's hardware events
- Enumerated all running system's processes in the snapshot
- Contained long sleep
- Created named mutex object
- Created and set up new security descriptor for the running process
- Created itself in suspended state and waited for the resuming thread call
- Updated information in a system access control list (SACL)
- Changed the protection attribute of the process
WHAT'S LEARNED THROUGH EXECUTION:

**Behaviors**
- Uses obfuscation techniques
- Utilizes VM detection
- Will utilize host to spread to others
- Will spy on and/or record data

**Indicators**
- Creates active content in Recycler
- Embedded executable content
- Grabbed approved system icon to re-use
- Changes memory access protection
- Set function to control system/hardware events
- Changed process protection attributes
- Captured all running processes for examination

YOU FIND ON-PREM

- Advanced Threat Defense
  - Target-Specific Sandboxing
  - Emulation Engine
- Efficient AV Signatures
- GTI Reputation
- 3rd Party Threat Data
- JAR Analysis
- .exe Analysis
- PDF Analysis
- Network Threat Response

McAfee Global Threat Intelligence

MFE FINDS VIA CLOUD
Host Based Security System
Current Baseline

McAfee Agent (MA)
- Securely interfaces with ePO to install and update products

Host IPS/FW (HIPS)
- Provides protection from both known and zero-day threats
  - Application Control
  - Stateful desktop firewall

Rogue System Detection (RSD)
- Identify unmanaged hosts

Asset Baseline Monitor (ABM)
- Detect system-level changes per INFOCON Policy SD 527-1

Policy Auditor (PA)
- Measure compliance to and report on configuration standards (Patch level, STIG, FDCC, etc.)

Device Control (DCM is a part of HDLP)
- Control what devices can connect to hosts
- Restrict USB storage devices
- Restrict CD/DVD Write operations

AV Program
HBSS Program
Upgradeable

ePO
McAfee Agent
Managed Systems
Anti-Virus (AV)
Anti-Spyware (AS)
Host IPS/Firewall (HIPS)
Policy Auditor (PA)
Host Data Loss Prevention (HDLP)
Rogue System Detection (RSD)
Asset Baseline Monitor (ABM)
Deployed POR System Challenges

• Limited or unreliable bandwidth to the device
  – Standard HBSS components require frequent downloads and update of various definition files (eg. AntiVirus, HIPS, etc.) which can be quite large (100M+)
  – The standard HBSS components rely on these files in order to effectively protect the device
  – A device that has access to a maximum transmission speed of 100K with several seconds of delay can take over 4 hours to download one file

• No bandwidth to the device
  – There are many systems that operate in a stand-alone fashion and are not connected to the network so updating the required files is difficult

• Limited capability of the device (OS, CPU, memory, disk space, etc.)
  – There are many older systems with older CPUs, older OS, limited memory and disk space and are not able to run standard HBSS components

• Targeted, zero day attacks
  – Attacks on weapons platforms are going to be targeted and not detected via a signature or virus definition
Whitelist created during install-time by scanning system for applications, libraries, drivers, scripts.

1. Application attempts to launch
   - Could be an executable or OS component
2. MAC verifies binary code from Whitelist
3. If not in Whitelist, then program is not launched.
   - Attempt is logged for alerts and auditing
Recommended Package
Disconnected Network, Disadvantaged Bandwidth, Firm/Fixed Function Devices

**McAfee Agent (MA)**
- Securely interfaces with ePO to install and update products

**Application Control**
- Protection from unauthorized applications
- Dynamically managed whitelists

**Change Control**
- Enforces policies to prevent unauthorized changes to critical files, directories, and configurations

**Rogue System Detection (RSD)**
- Identify unmanaged hosts

**Device Control (DCM is a part of HDLP)**
- Control what devices can connect to hosts
- Restrict USB storage devices
- Restrict CD/DVD Write operations

**HBSS Program**
Disconnected Network / Disadvantaged Bandwidth

Tactical Community User

MCAFEE APPLICATION & CHANGE CONTROL DEPLOYMENT SCENARIOS

A. ePO MANAGED DEPLOYMENT

1. Deploy McAfee Agent (MA) via ePO
2. Deploy Application Control (AC) & Change Control (CC) via ePO
3. Enable/Enforce Policy via ePO
4. Event Monitoring/Reporting via ePO

Joint Estimate is 1,100 Systems for Deployment Scenario A

B. THIRD PARTY IMAGE DISTRIBUTION VIA CD/DVD (DISK IMAGE)

1. Build Client Image on CD/DVD (includes MA, AC & CC)
2. Load Image to Client Systems

Joint Estimate is 5,500 Systems for Deployment Scenario B

NOTE: Package delivery via Systems Management tool (e.g. SCCM/SMS) is an alternative.
Firm/Fixed Function

Tactical ↔ Garrison