In the Cloud Security

Greg Day
Principal Security Analyst EMEA
AVERT member

July 28, 2009
The Tsunami

• Decades of threats, surely we have a handle on this?

• Estimated in excess $1 trillion loss through Cybercrime and data loss in 2008

  McAfee Unsecured Economies Report 2009

• Q1 2009 - 12 million new IP’s zombied since January!
  50 percent increase since 2008

  McAfee Quarterly threat Report Q1 2009

• Koobface - more than 800 new variants in March 09!

  McAfee Quarterly threat Report Q1 2009
Understand the motivation, to understand the methodology

Source: Chat Interview with the Dream Coders Team, the developers of MPack
Today anyone can be a cyber criminal!
Over 20 years of Anti-Virus

• Dr Solomon’s Anti-virus from 1990

• Looking for string match against known malware
The age old question - Is anti-virus dying?

- 1991: Michelangelo : 6 months?
- 1997: WM/Cap : 2 months?
- 1999: WM/Melissa : 1 Day?
- 2000: VBS/Loveletter : 4 hours?
- 2001: CodeRed/Nimda : 1 hour?
- 2003: Slammer : 3 mins?
- 2008: Mass Web compromises : secs?

DON’T PANIC
From Elephant to Chameleon
How threats have changed
Evolution of threats

1987 – Brain & Stoned (Early BSV)
1990 – Vienna modified to be polymorphic
1991 – Polymorphism hits the wild (Tequila)
1995 – WM/Concept (first Macro Virus)
1999 – Melissa Mass Mailer & ExploreZip reply mailer
2000 – Phage (Virus for Palm Pilot)
2001 – CodeRed & Nimda (utilise security vulnerabilities)
2002 – Klez & Bugbear (Droppers)
2003 – Slammer (Speed), Slapper (Unix, directed attack)
2004 – Turf wars (Bagle, Netsky, Sober, BOTs)
2005 – System & data theft (Trojan’s & Rootkit)
2007 – Rootkits, Packers, Recycling (Threat Longevity)
2008 – Drive-by infections,
Early proactive techniques
Heuristics (behavioural analysis)

• Positive & Negative analysis
• Protection against new file and/or macro viruses
• Checks for virus like characteristics
• Block execution of possible virus code (OAS)
• No cleaning as no exact match
• Tangible sample to send to virus lab
Speed…

The blended/zero day attack, bought the new solutions
<table>
<thead>
<tr>
<th>No.</th>
<th>Source Address</th>
<th>Dest Address</th>
<th>Summary</th>
<th>Len(Bytes)</th>
<th>Protocols</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>264</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.10]BART PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.56</td>
</tr>
<tr>
<td>265</td>
<td>Bart</td>
<td>0010A4EBD7A6</td>
<td>ARF: R PA=[10.1.1.10]BART HA=Bart PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.56</td>
</tr>
<tr>
<td>266</td>
<td>HOMER</td>
<td>BART</td>
<td>ICMP: Echo</td>
<td>106</td>
<td>ICMP</td>
<td>0:00:00.56</td>
</tr>
<tr>
<td>267</td>
<td>BART</td>
<td>HOMER</td>
<td>ICMP: Echo reply</td>
<td>106</td>
<td>ICMP</td>
<td>0:00:00.56</td>
</tr>
<tr>
<td>268</td>
<td>HOMER</td>
<td>BART</td>
<td>TCF: D=135 S=1462 SY SEQ=3480113163 LEN=0 WIN=16384</td>
<td>62</td>
<td></td>
<td>0:00:00.56</td>
</tr>
<tr>
<td>269</td>
<td>BART</td>
<td>HOMER</td>
<td>TCF: D=1462 S=135 SY ACK=3480113164 SEQ=1052707216 LEN=0 WIN=62</td>
<td>62</td>
<td></td>
<td>0:00:00.56</td>
</tr>
<tr>
<td>270</td>
<td>HOMER</td>
<td>BART</td>
<td>TCF: D=135 S=1462 ACK=1052707217 WIN=17520</td>
<td>60</td>
<td></td>
<td>0:00:00.56</td>
</tr>
<tr>
<td>271</td>
<td>HOMER</td>
<td>BART</td>
<td>MS/DCE: RPC(V5.0) Bind</td>
<td>126</td>
<td></td>
<td>0:00:00.56</td>
</tr>
<tr>
<td>272</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.11] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.56</td>
</tr>
<tr>
<td>273</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.12] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.56</td>
</tr>
<tr>
<td>274</td>
<td>BART</td>
<td>HOMER</td>
<td>MS/DCE: RPC(V5.0) Bind</td>
<td>126</td>
<td></td>
<td>0:00:00.56</td>
</tr>
<tr>
<td>275</td>
<td>HOMER</td>
<td>BART</td>
<td>MS/DCE: RPC Continuation of frame 275; 244 Bytes of data</td>
<td>1514</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>276</td>
<td>BART</td>
<td>HOMER</td>
<td>MS/DCE: RPC Continuation of frame 275; 244 Bytes of data</td>
<td>1514</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>277</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.13] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>278</td>
<td>BART</td>
<td>HOMER</td>
<td>TCF: D=1462 S=135 ACK=3480114940 WIN=17520</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>279</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.14] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>280</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.15] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>281</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.16] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>282</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.17] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>283</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.18] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>284</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.19] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>285</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.20] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>286</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.21] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>287</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.22] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>288</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.23] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>289</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.24] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>290</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.25] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>291</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.26] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>292</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.27] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>293</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.28] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>294</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.29] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
<tr>
<td>295</td>
<td>0010A4EBD7A6</td>
<td>Broadcast</td>
<td>ARF: C PA=[10.1.1.30] PRO=IP</td>
<td>60</td>
<td></td>
<td>0:00:00.57</td>
</tr>
</tbody>
</table>
You can see the RPC data is packed with repetitive no operation (NOP) data to exceed the buffer limit, which causes the overflow. This known vulnerability allows arbitrary code be to run with local system privileges.
Proactive behavioural protection (HIPS, NIPS, FW, Whitelisting etc…)

- Known Vulnerably detection
- Behavioural controls
  - RFC non-compliance
  - Anomaly detections
  - Policy controls
- Define web/email usage
- Lockdown Windows & Windows system folder
- Registry Modification
- Block un-used ports
- Proactive or Reactive?
- Blacklist non-corporate high risk apps

Conficker – AutoRun.inf
Proactive Behavioural Controls - limitations

- What did I really stop?
- Did it stop all of the attack?
- What else could it have done?

- We still want to identify the threat
- We sometimes need to clean up

- Assumes clean at point of install
Volume...

- 246% growth from 2006 to 2007
- 400%+ growth projected for 2008
- 2008 exceed projections

Source: McAfee Avert Labs

~350,000 projected for '08
The Great Zoo: McAfee Known Malware Samples

Count of dirty samples/hashes in the McAfee zoo
Shark – Compliable multi system back door Trojan
Now anyone can be a cyber criminal!

1. Setup server
2. Compile threat
3. Infected systems talk home!
4. See what you have!
5. Full control!
6. Enable keylogger
7. Control processes
We are proud to present a browser vulnerability test kit - the **Splot25** exploit pack.

The pack consists of 5 splotis:

- **IE MDAC** - the everpresent splotit, provides the main infection of old IE 6
- **IE Snapshot** - a unique script, infects IE 6 and 7
- **FF Embed** - an exploit for ancient FireFoxes
- **PDF** - the famous private Acrobat Reader splotit
- **PDF vis** - in our pack two PDFs cowork and show an all-right infection rate

According the results of tests done by administration, the infection hitrate is 13% to 30% depending on traffic types and countries. Tests were held using 7 different types of traff from different sellers, the infection rate **averages to 25%**.

**Splot25** contains a confortable single-file 150 kb installer which creates all the files and prepares the pack for its job. The pack has a nice no-frills design and convenient statistics.

The updates and AV cleans are included in the support. Additionally, you get a discount on significantly new splotis.

The pack is bound to the domain and the IP, all the splotis are bound to an URL. If you try to resell, decode, remove the boundaries, you will lose all the support, updates and guarantees.

**Price:**
- Splotit pack build - 2500 wmz
- Rebuild to a new domain - 2000 wmz
- Rebuild to a new domain if the old domain is in malware list - 50 wmz
- Rebuild to a new subdomain if the old domain is in mallist - free

Contacts: info@splot25.com
Mass infection of public web pages globally
(13 March 08)

- 200,000 web pages compromised
  - SQL injection
  - Vuls in .ASP pages running phpBB
  - Inserted JS to write IFRAME in header or body
    - MS06-014
    - RealPlayer (ActiveX Control)
    - Baofeng Storm (ActiveX control)
    - Ourgame GL World GlobalLink Chat (ActiveX Control)
- Daisy chains to China server
  - Drops down loaders
  - Steals gaming credentials
1. The victim visits a legitimate site that has been booby-trapped with hidden redirect code (*hidden iFrame*).
2. They are silently redirected to the server hosting the attack tool.
3. Depending on the browser, various vulnerabilities may be tested. Various malware are downloaded and executed.
4. The web pages accessible from the victim’s workstation are in turn booby-trapped.

*Example: IFrame & MPack*

*Botnet, RockPhish, Fast-Flux, DDoS, Identity theft, ...*
Regular “Protection Gap”

Protection gap of 24-72 hours with current solutions

Malware in the wild
Malware discovered
Protection is available
Protection is downloaded
Protection is deployed
Security in the Cloud
Next Gen “In the cloud” detection

Fingerprint Database

Internet
What is “in the Cloud scanning”?

- End-node reporting
- Very little system overhead
- Meta-data
In the cloud security - Blocking what we already know!

Non-replicating malware is static

And some replicating is static too (e.g. worms)

Can be detected with a fingerprint (MD5, SHA-1, SHA-2, etc.)

Black List of fingerprints

Replicating vs Non-Replicating Malware
**How does in the Cloud anti-virus work?**

1. **User receives new file via email or web**

2. **No detection with existing DATs, but the file is “suspicious”**

3. **Fingerprint of file is created and sent using Artemis**

4. **Artemis reviews this fingerprint and other inputs statistically across threat landscape**

5. **Artemis identifies threat and notifies client**

6. **VirusScan processes information and removes threat**
In the Cloud in action

Virus data file v5505 created Nov 10 2008
Scanning for 1 viruses, trojans and variants.
Using C:\goat\5200\EXTRA.DAT to scan for 1 additional virus(es).

Scanning C: [ ]
Scanning C:\GOAT\**.*
C:\GOAT\ticket_02.doc.exe ... Found trojan or variant Generic!Artemis !!!
C:\GOAT\MDOMAIN-example ... is OK.
C:\GOAT\spy-agent-trojan-example ... is OK.

Summary report on C:\GOAT\**.*
File(s)
   Total files: .............. 3
   Clean: ..................  2
   Not scanned: .................. 0
   Possibly Infected: ...... 1

Time: 00:00.08

C:\goat\5200>
In the cloud security - Identifying what we don’t know!

Software may be deemed “suspicious” based on Observed behaviours Source Detections by other products

Behaviours, sources, detections can be assigned a weight

Based on the resulting weight, software may be classified as “suspicious” with different degrees of certainty
## Closing the loop

### McAfee Avert Workflow (1.2.484)

#### Samples

<table>
<thead>
<tr>
<th>MD5</th>
<th>Filename</th>
<th>Owner</th>
<th>Occurrences</th>
<th>Status</th>
<th>Assignor</th>
<th>Detections</th>
</tr>
</thead>
<tbody>
<tr>
<td>3a14ba03f404d0d4d13b2588b64a403889</td>
<td>statement_jar-mst.doc.exe</td>
<td>Ken Holberg</td>
<td>1-15-15</td>
<td>closed</td>
<td>Ken Holberg</td>
<td></td>
</tr>
<tr>
<td>4903833</td>
<td>Malware</td>
<td></td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>16 Oct 21:38:43</td>
</tr>
<tr>
<td>4902641</td>
<td>Malware</td>
<td></td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>16 Oct 19:08:11</td>
</tr>
<tr>
<td>4902662</td>
<td>Malware</td>
<td></td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>16 Oct 18:09:06</td>
</tr>
<tr>
<td>4902381</td>
<td>PO QMI Statement_JVM-GCT.doc.exe</td>
<td>Chris Holberg</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>16 Oct 17:05:03</td>
</tr>
<tr>
<td>4902311</td>
<td>PO QMI sample</td>
<td>Chris Holberg</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>16 Oct 17:04:08</td>
</tr>
</tbody>
</table>

#### Analyst Functions

- Take Sample
- Assign Sample
- Unassign Sample
- Junk
- Resolve
- Update

---

Confidential McAfee Internal Use Only
Malware case study – Spy-Agent.bw

First seen
Auto-blacklisted

Artemis clients sent fingerprints ~2 hours before regular submission saw the file
Example:

U0B6gKhbtIZCoxyh0lneADS/RShS8iRCBSEvwfjekG/q4yDRgqEUXjHWKvnrySGa6QMdftrlpl5pAdJvOUAcNcvCjKvplfsxv8qBk4uRQQ60r5StRCXOpiA0Qy3fKmLRUZyNq1EyjLLPKgJDZI0nqHhRWX+TDgPgXRfW9wD06qE

Cryptographically strong actionable responses

Query specific

Immune to replay attacks
Cloud security compressed “Protection Gap”

Protection delivered in real-time

Malware in the wild

Protection is deployed

Case study – Spy-Agent.bw

- Artemis protection – ~32 minutes
- Regular protection – ~8.5 hours
  - Not including deployment time
I was blind, but now I see

Artemis customers

Malware Research

Risk and Compliance

Customer

Internet

SiteAdvisor

Vulnerability Research

SPAM Research

HIPs

Collective Threat Intelligence
Taking it to the next level
Collaborative Global Intelligence

Physical World

Deploy agents: Officers around the globe (MI5, MI6, FBI, CIA, Interpol.)
Global intelligence system: Share intelligence information. (e.g. criminal history, global finger printing system)

Results
Effective - Accurate detection of offenders
Pro-active - Stop them from coming in the country

Intelligence Agents

Cyber World

Deploy security probes: Around the globe (firewall, email gateways, web gateways)
Global intelligence system: Share cyber communication info. (e.g.: hackers, spammers, phishers)

Results
Effective - Accurate detection of bad IPs, domains
Pro-active - Deny connection to intruders to your enterprise
Global Data Monitoring is Fueled by the Network Effect of Real-Time Information Sharing from Thousands of Gateway Security Devices around the World
Intelligence: How It All Works….

This entire process happens constantly, every second, 7x24x365

1. Incoming traffic

2. McAfee Threat Intelligence queries

3. McAfee Threat Intelligence returns reputation info

4. McAfee Threat Intelligence updates records with new reputation info

TS-enabled appliance
Responder Architecture

- Legacy protocol based on customized DNS servers
- Enhanced proprietary protocol (UDP over SSL)

Analysis Systems

- Historical data
- Message data/metadata
- Neighborhood data
- Ownership data
- Spamtraps and honeypots
- Blacklists
### What does it monitor?

- **Email**
  - IP Reputation
  - Message Reputation
- **Web**
  - URL Categories
  - Web Reputation
- **Intrusion/FW**
  - IP/Protocol Reputation
  - Geo-Location
  - IPS Attack Vector Correlation

#### Dimensions

<table>
<thead>
<tr>
<th>Email</th>
<th>Hack Attack</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hacker sites</td>
<td>DoS, DDoS, misc other attacks</td>
</tr>
<tr>
<td>Virus Phishing</td>
<td>Compromised or malicious web sites or URLs</td>
<td>ActiveX, Java, VB code from infected web sites</td>
</tr>
<tr>
<td>Malware</td>
<td>Zombies, Botnets, other sources</td>
<td>Image spam, Virus, worms, Trojans</td>
</tr>
</tbody>
</table>

#### Connection Reputation

- IP
- Domain
- URL

#### Content Reputation

- Attachment
- Image
- Message
Message Reputation

1. Known spammer sends message
2. Message is blocked
3. Unknown sender sends similar message
4. Message is recognized and blocked
5. Unknown sender sends different message
6. Message is associated with new machine in a botnet and blocked

Allows Reputations to Move Across Identities and Protocols
Web Reputation Breakout for Q209 on 6/04/09

- Neutral: 54%
- Suspicious: 22%
- Malicious: 19%
- Trusted: 0%
- Unverified: 5%
Building Web Reputation

Raw Data
- TrustedSource for Email
- Domain Registrations
- WHOIS data
- WebWasher classifiers
- SmartFilter categories
- Web access logs
- Malware URLs
- Phishing URLs
- Spam URLs
- Fortune 1000 websites
- Blacklists
- Whitelists

Analysis
- Correlation Mapping (Joint Conditional Mapping)
- Support Vector Machine classification of all parameters
- Parked Domain Identifier
- Neighborhood Classification
- Real-Time Classifier
- GEO Location
- Host information:
  - DNS
  - WHOIS
  - OS
  - Webserver
  - Certificate information

Reputation Service

Size
- 75 Million Hosts

Precision
- More Precise (-180 - +180)
- Identified zombies, malware, suspicious

Reputation Range
-180  +180
-180  Bad
-120  Suspicious
-100  Good
TrustedSource Web Database

- Category-based filtering + reputation based filtering = best protection available

- 96 URL categories

- TrustedSource global intelligence augments numerous categories such as Spam, Malicious Sites, Phishing, Hacking/Computer Crime

- Reputation-based filtering for today’s Web 2.0 threats
  - Provides an additional layer of security
  - Malicious sites, Spyware, Hacking, P2P, IM and more

- 31+ Million URLs (contains IPs, HTTP and HTTPS URLs)

- Automated proactive and reactive URL gathering systems

- Human review of URLs by multi-lingual/cultural Web Analysts
  - Global coverage (language and regions)

- Real-time updates
www.TrustedSource.Org

- Public Portal
- View reputations for domains, IP addresses or URLs
- Sending patterns of the senders
- Analytical information:
  - country of origin
  - network ownership
  - hosts for known senders within each domain
- Snapshot of global email trends, including a map illustrating country of origin for email attacks
- Graphs displaying overall email and spam volume trends
- ROI Calculator
- ZombieMeter
- Domain Health Check
- Latest malware threats
- Blogs from experts
- Top spam senders