Who am I?

• Raphael Mudge
  – Principal, Strategic Cyber LLC
  – Developer, Cobalt Strike
  – Resident, Washington DC
Overview

• How to get a Foothold
• Message Delivery
• Code Execution
• Egress
• Stay Quiet
How to Get a Foothold

1. Map client-side attack surface
2. Create Virtual Machine for testing purposes
3. Use Virtual Machine to select best attack
4. Configure and disguise the attack
5. Email attack package to victim
Now, walk this minefield

Sender Policy Framework

Mail Anti-virus Gateway

Message Delivered

Host Anti-virus

Positive C2

Firewall

Intrusion Detection System

Post Exploitation

Code Execution

Legend
Low Risk to Attacker
Moderate Risk to Attacker
High Risk to Attacker
Message Delivery

• **Defense (DKIM, SPF, and DMARC)** identify spoofed messages

• **Attacker**
  send email from attacker controlled domain
  OR
  spoof a domain with no validation information
Sending a message (SMTP)

# telnet mail server 25
HELO whatever.com
MAIL FROM: <bounceaddress@whatever.com>
RCPT TO: <target email here>
DATA
message data
.
QUIT
Sending a message (SMTP)

# telnet mail server 25
HELO whatever.com

MAIL FROM: <bounceaddress@whatever.com>
RCPT TO: <target email here>

DATA
message data
.
QUIT
# Sending a message (SMTP)

```
# telnet mail server 25
HELO whatever.com
MAIL FROM: <bounceaddress@whatever.com>
RCPT TO: <target email here>
DATA
message data
.
QUIT
```
Anti-Spoofing

• Sender Policy Framework (SPF)
  – dig +short TXT domain.com
• DomainKeys Identified Mail (DKIM)
• Domain-based Message Authentication, Reporting and Conformance (DMARC)
  – dig +short TXT _dmarc.domain.com
• Accepted Domains (MS Exchange Feature)
### Tips for Message Delivery Success

#### Spear Phish

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To</td>
<td>user@mint</td>
<td></td>
</tr>
<tr>
<td>To_Name</td>
<td>Lou User</td>
<td></td>
</tr>
<tr>
<td>Targets</td>
<td>/root/targets.txt</td>
<td></td>
</tr>
<tr>
<td>Template</td>
<td>/root/message.txt</td>
<td></td>
</tr>
<tr>
<td>Attachment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embed URL</td>
<td><a href="http://www.mymaliciousdomain.com/whatever">http://www.mymaliciousdomain.com/whatever</a></td>
<td>Don't attach an executable</td>
</tr>
<tr>
<td>Mail Server</td>
<td>192.168.95.187</td>
<td></td>
</tr>
<tr>
<td>Bounce To</td>
<td><a href="mailto:raffi@strategiccyber.com">raffi@strategiccyber.com</a></td>
<td></td>
</tr>
</tbody>
</table>

#### Tips

**RCPT TO**
Make sure target emails are in a domain that your SMTP server will deliver to.

**DATA**
1. Use %To% and %To_Name% to personalize
2. Update plaintext URL references to %URL%

**File Attachment**
- Don't attach an executable

**URL (Replaced in Template)**
- Replace IP address with FQDN

**SMTP Server**
- Use MX record of target's domain OR
- Use server for phishing domain that you own

**MAIL FROM**
1. Check that domain does not have SPF record
2. Do not use your target's domain here
3. Make sure From: address in Template matches (optional to get past some spam filters)
Code Execution

- **Defense (Anti-virus)**
  check for known bad and stop it

- **Attacker**
  get code into memory without known bad
Anti-virus Constraints

• False positives are bad
• Non-intrusive (?)
• Only checks file at certain points
  – When loaded in browser
  – When written to disk
How does Anti-virus work?

- Check for known signature
- Apply heuristic to detect bad behavior
- Emulate binary to defeat packers and crypters
1. Find out or guess which anti-virus is in use
2. Put anti-virus on test Virtual Machine
3. Select undetected attack or modify existing attack
What gets caught by anti-virus?

STAGERS

and Exploits
What is a Stager?

send exploit with stage 1

download stage 2

encrypted C2
Getting Past AV (EXE)

• Use AV-safe stager EXE
  – Easy to write in a pinch
  – Tools exist to generate AV-safe stagers (e.g. Veil)

• Avoid an EXE if possible
  – exploit/windows/smb/psexec_psh
  – exploit/windows/misc/psh_web_delivery
Stager (Meterp Reverse TCP)

1. Connect to attacker
2. Read integer containing stage-2 length
3. Read [stage length] bytes
4. Allocate RWX buffer
5. Move connection to EDI register
6. Copy stage data to RWX buffer
7. Pass control to stage

See:
https://github.com/rsmudge/metasploit-loader
### EXE Stager VirusTotal Results...

<table>
<thead>
<tr>
<th>SHA256</th>
<th>afe34bfe2215b048915b1d55324f1679d598a0741123bc24274d4edc6e395a8d</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA1</td>
<td>370a759dec1846dec60620926550a4909a510b4a</td>
</tr>
<tr>
<td>MD5</td>
<td>78a908b1a6e7e3ab507cb736074f3780</td>
</tr>
<tr>
<td>File size</td>
<td>51.9 KB ( 53118 bytes )</td>
</tr>
<tr>
<td>File name</td>
<td>loader.exe</td>
</tr>
<tr>
<td>File type</td>
<td>Win32 EXE</td>
</tr>
<tr>
<td>Detection ratio</td>
<td>2 / 42</td>
</tr>
<tr>
<td>Analysis date</td>
<td>2012-09-13 03:33:16 UTC ( 0 minutes ago )</td>
</tr>
</tbody>
</table>
EXE Stager VirusTotal Results...

SHA256: afe34bfe2215b048915b1d55324f1679d598a0741123bc24274d4edc6e395a8d

File name: loader.exe

Detection ratio: 3 / 47

Analysis date: 2013-10-06 22:30:02 UTC (0 minutes ago)
Getting Past AV (Exploit)

• Use AV-Safe Client-side Exploit
  – Custom Java Applet Attack
  – MS Office Macro

• Modify Metasploit Client-side Exploit
  – Change strings in module
Code Execution

- **Defense (Application Whitelisting)** do not allow unapproved applications.

- **Attacker** get agent into memory using a white-listed application.
• Use attacks that inject directly into memory
  – Custom Java Applet Attack
  – MS Office Macro

• Get into memory with PowerShell
  – exploit/windows/smb/psexec_psh
  – exploit/windows/misc/psh_web_delivery
Egress

1. Get code execution

2. Execute payload

3. Establish session TCP/35675
Egress

1. Get code execution

Exploit Modules
Auxiliary Modules

2. Execute payload

multi/handler

Firewall

3. Establish session
HTTPS / 443

Payload
Egress

- **Defense (Firewall)**
  limit which protocols may leave network
- **Attacker**
  communicate over allowed protocol
Egress (Typical)

- Deny all outbound traffic
- Allow egress only through a proxy device
  - Attack traffic must conform to expected protocol
  - Must pass other checks as well...
- Attacker Limitation: Staging!
Payload Staging

• Stagers are sized constrained
  – smaller is better
• If payload can’t stage... it can’t execute
• If protocol works for staging; C2 is OK
Payload Staging

- Set `EnableStageEncoding` to avoid this...
Metasploit Framework HTTP/HTTPS Stagers
- Transparent Proxy? OK
- Automatic NTLM Auth to Proxy? OK
- Static Username and Password on Proxy? Not OK

Other ways out? DNS
- ~184 bytes per DNS TXT record request
- ~550 DNS TXT requests to move 100KB of data
Staying Quiet

• **Defense (Network Security Monitoring)**
  alert on observed attacker actions on network

• **Attacker**
  – Limit noisy activity
  – Use low & slow C2 strategy
Limit Noisy Activity

• Do not scan hosts...
  – (ab)use active directory to discover hosts
• Use Windows commands to accomplish goals
  – upload / schedule an executable via a command shell is safer than launching an exploit
• Use normal clients to interact with systems
  – Browser Pivot to interact with internal websites
  – RDP, SSH, etc.
# Enumerate w/o Scanning

<table>
<thead>
<tr>
<th>How do I...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find out which domain I trust</td>
<td>net view /DOMAIN</td>
</tr>
<tr>
<td>See some hosts in the domain</td>
<td>net view /DOMAIN:[domain]</td>
</tr>
<tr>
<td>See which hosts are DCs for a domain</td>
<td>nltest /dclist:[domain]</td>
</tr>
<tr>
<td>Map a NetBIOS name to an IPv4 address</td>
<td>ping –n 1 -4 [name]</td>
</tr>
</tbody>
</table>
Lateral Movement w/o PsExec

- Where are you an administrator?
  windows/gather/local_admin_search_enum
- Copy a file to a host
  copy file.exe \host\C$
- What time is it on the target host? (cmd.exe)
  net time \\host
- Schedule a task to run (cmd.exe)
  at \\host hh:mm c:\file.exe

Note: at is deprecated. Use schtasks or wmic
No Shell Needed...

- Use UNC path to reference files on other host
- List files in c:\foo on remote host
  \dir \\host\C$\foo
- Copy remote c:\foo\secrets.txt to current host
  \copy \\host\C$\foo\secrets.txt .
- Go shopping for files on remote host
  \dir /S \\host\C$ >files.txt
Low and Slow C2

• Use a slow asynchronous payload!
  – sleep time of minutes to hours (with jitter)
  – Call home to multiple domains

• When you go interactive...
  – Spawn interactive sessions to another server
    (don’t burn your primary C2 server)
  – Go interactive only when necessary (or at night)
• Get a Foothold
• Message Delivery
• Code Execution
• Egress
• Stay Quiet
Learn More

Tradecraft Course
http://www.advancedpentest.com/training

My Contact Information
raffi@strategiccyber.com

Correspondence in 140 chars
@armitagehacker