May 30, 2012

Malware Notification and Remediation
Tools and Techniques

NIST Workshop: Technical Aspects of Botnet

Michael Glenn
5 Steps to Malware Remediation

User Education

- Prevention
- Detection
- Notification
- Remediation
- Recovery
## Notification and Remediation Techniques

<table>
<thead>
<tr>
<th>Method</th>
<th>Cost</th>
<th>Notify Effect</th>
<th>RemEDIATE Effect</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Low</td>
<td>Low – Moderate</td>
<td>Low - Moderate</td>
<td>Cost</td>
<td>Easy to spoof</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Account DB</td>
</tr>
<tr>
<td>Telephone Call</td>
<td>Low - High</td>
<td>Moderate</td>
<td>Very Low - High</td>
<td>Cost</td>
<td>Account DB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cost</td>
</tr>
<tr>
<td>Postal Mail</td>
<td>High</td>
<td>Moderate</td>
<td>Low</td>
<td></td>
<td>Very Costly Remediation</td>
</tr>
<tr>
<td>SMS</td>
<td>Low</td>
<td>Low - Moderate</td>
<td>Very Low</td>
<td>Cost</td>
<td>Account DB</td>
</tr>
<tr>
<td>Instant Message</td>
<td>Low</td>
<td>Low - Moderate</td>
<td>Low</td>
<td>Cost</td>
<td>Easy to spoof</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Account DB</td>
</tr>
<tr>
<td>Walled Garden</td>
<td>Low</td>
<td>Medium - High</td>
<td>Medium - High</td>
<td>Direct Interaction</td>
<td>Infected Device Identification</td>
</tr>
<tr>
<td>Web Browser</td>
<td>Low</td>
<td>Medium - High</td>
<td>Low - High</td>
<td>Direct Interaction</td>
<td>Easy to Bypass</td>
</tr>
</tbody>
</table>
CenturyLink Notification & Remediation Program

Prevention
• Anti-virus Provided, Broadband Modem Firewall, NAT
• User Education Materials

Detection
• Rely on Trusted Third Party Reports
• Do Not Monitor Customer Traffic

Notification
• Leaky Walled Garden, Port 80 Web Traffic Redirection

Remediation
• 5 Step Process with Locally Hosted Tools
• Special Notifications and Tools by Malware Family
Consumer Internet Protection Program

Goals:

- Automate the notification of customers of AUP violations (today malware infected customers)
- Assist customers in a self help manner to clean their computers of the infection
- Educate users about the dangers of malware and good Internet security practices

System primarily justified through the lowering of tier 1 support calls. Additional benefits include:

- Better customer satisfaction with broadband product
- Lower customer churn
- Lower SPAM complaints
- Reduced level of DDoS attacks

General Philosophy

• Assume majority of infected customers are not malicious, merely infected co-victims

• Treat them with respect

• Warn them of the risk to their personal information

• Educate them regarding good security practices

• Provide them self-help tools

• Do not lock them into the walled garden
DNS Override

End User PC(s) → End User Modem (PPP client) → ISP Access Routers → ISP RADIUS Servers → Captive DNS Servers → Walled Garden Web/Proxy Servers → Web Servers

PPP LCP negotiation → PPP auth request username/password → PPP auth response → PPP IPCP negotiation → DNS override IPs

RADIUS auth request → RADIUS auth response → DNS override IPs

DNS request for (to override IP)
www.adventureworks.com

DNS response
walled garden IP

Web request
http://www.adventureworks.com/page1.html

Web proxy request

Web response
walled garden content
Policy Based Routing

PPP LCP negotiation
PPP auth request
username/password
PPP auth response
PPP IPCP negotiation

RADIUS auth request
RADIUS auth response
PPP parameters

DNS request
www.adventureworks.com

Normal DNS response

Web request (routed to walled garden web/proxy servers via policy based routing on ISP IP network)
http://www.adventureworks.com/page1.html

Web proxy request
Web proxy response

Web response
walled garden content
Tunneled Traffic
Michael Glenn – Director Enterprise Security Technology
Email: Michael.Glenn at CenturyLink.com