Tracking the “Who” and “Why” behind targeted, semi-targeted and widespread attacks

Michael La Pilla
VeriSign iDefense Malicious Code Operations Team
21st Annual FIRST Conference Kyoto, Japan
29 June 2009
Topics For Today

- Misinformation vs Disinformation vs Truth
- Large Scale Incident Attribution Methods
- Spotting Other Researchers
- Scope Determination Techniques
- Aggressive Counter-attack Methods
Information

- information (n) - the communication or reception of knowledge or intelligence

Source: Merriam-Webster
Misnformation

- misinformation (n) - the *unintentional* communication or reception of false knowledge or intelligence

Source: Merriam-Webster
Disinformation

• disinfection (n) - false information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth

Source: Merriam-Webster
Gimmiv

- See where stolen data gets posted
- Anyone can retrieve data files if they know the file name
- Uses combinations of encryption and encoding so people can’t decrypt data
- See if they did anything stupid...
<table>
<thead>
<tr>
<th>Directory</th>
<th>Size</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>0 KB</td>
<td>09/19/08 17:57:46</td>
</tr>
<tr>
<td>+j:</td>
<td></td>
<td>09/19/08 09:23:22</td>
</tr>
<tr>
<td>8.zip</td>
<td>587 KB</td>
<td>10/23/08 14:05:41</td>
</tr>
<tr>
<td>server.zip</td>
<td>4284 KB</td>
<td>10/23/08 14:05:41</td>
</tr>
<tr>
<td>inetproc08x.aes</td>
<td>292 KB</td>
<td>09/19/08 13:47:56</td>
</tr>
<tr>
<td>n8.exe</td>
<td>388 KB</td>
<td>09/19/08 13:47:56</td>
</tr>
<tr>
<td>test8.php</td>
<td>5 KB</td>
<td>09/19/08 13:47:56</td>
</tr>
</tbody>
</table>
Gimmiv (con’t)
<?php
session_start();
if ($_GET['abc'])
{
    if ($_GET['abc'] == 1)
    {
        define("DOWN_CONTENTS", "inetproc25XX0X.aes");
    }
    else if ($_GET['abc'] == 2)
    {
        define("DOWN_CONTENTS", "inetproc25XX0X.aes");
    }
}
else
{
    define("DOWN_CONTENTS", "inetproc25XXX.aes");
}
//define("DOWN_CONTENTS","inetproc.aes");

define("DUMMY_IMAGE", "winter.jpg");
require_once 'zbase64.php';
require_once 'logging.php';

define ('SVC_MAGIC', 0x9CDE);
define ('SVC_AUTH1', 0x8A70);
define ('SVC_AUTH2', 0x8A71);
define ('SVC_GET', 0x0D7FA);

$_auth_pass = base64_decode('5c6/OkUGZPaeLP5uE1sgG3XqgUgUcd0paSapoCbxgeIs=');
logging::debug("COOKIE[ac] %s", $_COOKIE['ac']);

// check param
$req = Request::parse($_COOKIE['ac']);
if (!$req) {
    logging::debug("invalid request: need cookie");
    send_response();
    exit(0);
}

logging::debug("Request: 0x%x, 0x%x, %d", $req->magic, $req->tag, strlen($req->param));
switch($req->tag){
    case SVC_AUTH1:

Gimmiv (con’t)
Waledac

- Uses Nodes From Repeater (or Higher) as Proxies
- Manage DNS For Waledac Through These Proxies
修改本域名下的DNS

说明：
1. 修改信息会在24-48小时内生效。
2. 修改这个DNS后，原来的DNS进行解析的域名将无法获得正确的解析，可能会导致相应的网站无法访问和邮件无法收发。

### 注册域名fryroll.com下的DNS

1. 域名
   - fryroll.com

2. 已注册的DNS列表
   - ns5.fryroll.com
   - ns1.fryroll.com
   - ns6.fryroll.com
   - ns2.fryroll.com
   - ns3.fryroll.com
   - ns4.fryroll.com

返回管理页面
Waledac
Waledac

- Have Control
- Legal Issues
- Originating IP Not Waledac-based
- Original IP Tunneling Through LayeredTech
  - Seize Machine
  - Trace Next Hop Backward
Attackers vs Researchers

- Researcher Footprints
- IPs
- UAs
- OSs
- Files on the system (more on this later)
- Unavoidable
Attackers vs Researchers

- bad guys finding researchers (BBB)
Attackers vs Researchers

• researchers trying to hide (tigger)
Researcher vs Researcher

• researchers deceiving other researchers (TE)
Mike’s Top 5 Worst Researcher Actions of 2009

5. Blogging someone else’s exploit to get into an attacker’s control panel
4. Using an attacker’s shell shared on a mailing list to `rm -rf` stolen data and insert profanities to attacker
3. Helping an attacker firewall researchers
2. Destroying two years worth of access for press
1. Manually killing researchers connections that try to recover data
Small Scale Attacks

- [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]
How Targeted Is It?

- [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]
Dangers of Previous Slide

- [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]
Or You Can Do This...

- [SS of Fake Return Address e-mail]
Counter-Attack Methods

- Counter-Attack Disinformation Campaigns
- Tracking
- Hack-Back Attacks
Disinformation Diagramming

- [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]
Pre-Attack Tracking

• Search Web Site Logs

• Analyze and Correlate Visitors
  • Focus on Pages with Contacts
  • Pay Attention to Referrer
Post-Attack Tracking

• Save All E-mail Header Information
• Entice Attacker to Click URL
• E-mail back if address real
• Visit special URLs that will be keylogged
“Special” URLs

- Use scripts to capture IP and attempt to determine whether a proxy is used
  - Javascript
  - Java
  - Flash
  - Silverlight
  - DNS Resolution
“Special” URL Demo

• [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]
Hacking Back

- Direct Connection Backdoors Often Relayed Through Proxy
- Most Backdoors We Care About Written in C/C++
- Web-based Connect Back Usually ASP/PHP
Hacking Back Example

• [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]
Conclusions

Learn the Law
Conclusions

You Can’t Fight If You Don’t Know Who Your Enemy Is
Conclusions

• Fingerprint
• Look for footprints
• Use disinformation
• Beware of misinformation and disinformation
• Be careful what you say and do publicly
Q & A

Michael La Pilla
VeriSign iDefense Malicious Code Operations Team
mlapilla@idefense.com