Security Cameras: Corporate DFIR Tool of the Future?

Michael Viscuso
Vulnerability Research
Rootkits
Digital Forensics
Exploit Development
Incident Response
Malware Analysis
ACTIVITY
not a matter of IF, but WHEN
Malware responsible for 95% of all compromised records
Malware responsible for 95% of all compromised records

85% of intrusions took weeks or more to discover
Malware responsible for 95% of all compromised records

85% of intrusions took weeks or more to discover

92% of victims found out through a 3rd party
Protect   Detect   Respond   Recover

Typical resource allocation

90%        10%        0%        0%
Zappos Hacked: What You Need to Know

Zappos.com -- the online source for shoes -- was the victim of an attack that compromised account information for millions of customers. Zappos customers need to understand what is at stake, and be on alert for suspicious or malicious activity resulting from the attack.

By Tony Bradley
Mon, January 16, 2012
2 Comments

Most Recent Data breach Stories

- European League of Legends Game Players have Their Account Data Compromised
- Another Breach Reveals Weak Passwords: Will We Ever Learn?
- LinkedIn Provides Breach Update -- Sort Of
- Vupen Security Denies it's Been Hacked
Requires an expert

Log Analysis

Filesystem Forensics

Takes a ton of time
Cyber Liability & Data Breach Insurance Claims

A Study of Actual Payouts for Covered Data Breaches
‘Citadel’ Trojan Touts Trouble-Ticket System

Underground hacker forums are full of complaints from users angry that a developer of some popular banking Trojan or bot program has stopped supporting his product, stranding buyers with buggy botnets. Now, the proprietors of a new Zeus Trojan variant are marketing their malware as a social network that lets customers file bug reports, suggest and vote on new features in upcoming versions, and track trouble tickets that can be worked on by the developers and fellow users alike.

The Zeus offshoot, dubbed Citadel and advertised on several members-only hacker forums, is another software-as-a-service malware development. Its target audience? Those frustrated with virus writers who decide that coding their next creation is more lucrative and interesting than supporting current clients.

“Its no secret that the products in our field — without support from the developers — result in a piece of junk on your hard drive.
Underground hacker forums are full of complaints from users angry that a developer of some popular banking Trojan or bot program has stopped supporting his product, stranding buyers with buggy botnets. Now, the proprietors of a new ZeuS Trojan

The basic Citadel package — a bot builder and botnet administration panel — retails for $2,399 + a $125 monthly “rent,” but some of its most innovative features are sold as a la carte add-ons. Among those is a $395 software module that allows botmasters to sign up for a service which automatically updates the bot malware to evade the last antivirus signatures. The updates are deployed via a separate Jabber instant message bot, and each update costs an extra $15.

writers who decide that coding their next creation is more lucrative and interesting than supporting current clients.

“Its no secret that the products in our field — without support from the developers — result in a piece of junk on your hard drive.
<table>
<thead>
<tr>
<th>Breach</th>
<th>Attacker Cost</th>
<th>Defender Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$2,795</td>
<td>$0</td>
</tr>
<tr>
<td>1</td>
<td>$2,935</td>
<td>$200,000</td>
</tr>
<tr>
<td>2</td>
<td>$3,075</td>
<td>$400,000</td>
</tr>
<tr>
<td>3</td>
<td>$3,215</td>
<td>$600,000</td>
</tr>
<tr>
<td>4</td>
<td>$3,355</td>
<td>$800,000</td>
</tr>
<tr>
<td>5</td>
<td>$3,495</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>Breach</td>
<td>Attacker Cost</td>
<td>Defender Cost</td>
</tr>
<tr>
<td>--------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>0</td>
<td>$2,795</td>
<td>$0</td>
</tr>
<tr>
<td>1</td>
<td>$2,935</td>
<td>$200,000</td>
</tr>
<tr>
<td>2</td>
<td>$3,075</td>
<td>$400,000</td>
</tr>
<tr>
<td>3</td>
<td>$3,215</td>
<td>$600,000</td>
</tr>
<tr>
<td>4</td>
<td>$3,355</td>
<td>$800,000</td>
</tr>
<tr>
<td>5</td>
<td>$3,495</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>1409</td>
<td>$200,055</td>
<td>$281,800,000</td>
</tr>
</tbody>
</table>
Not sustainable
<table>
<thead>
<tr>
<th>Activity</th>
<th>Expert</th>
<th>Time</th>
<th>Disruption</th>
<th>Quality</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Interrogation</td>
<td>$</td>
<td></td>
<td>$</td>
<td>$</td>
<td>$$</td>
</tr>
<tr>
<td>Forensics</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td>$$$$$</td>
</tr>
</tbody>
</table>
FORENSICS = LCD
Another interesting session had Gerard Stegmaier and Paul Luehr discussing modern techniques to responding to data breaches. As sad as it may be, over the last three years malicious cyberspace attacks have risen 300%, so the providers who have contingency plans in place now will be much better off when responding to a data breach than those who wait to respond until it occurs. The best way to do this, both said, was to put in place a breach response plan. By
Computer Security
Incident Handling Guide (Draft)

Recommendations of the National Institute of Standards and Technology
2.6 Recommendations

The key recommendations presented in this section for organizing a computer security incident handling capability are summarized below.

- **Establish a formal incident response capability.** Organizations should be prepared to respond quickly and effectively when computer security defenses are breached. FISMA requires Federal agencies to establish incident response capabilities.

- **Create an incident response policy.** The incident response policy is the foundation of the incident response capability which outlines the procedures which are to be followed when an incident occurs.
### 3.1.1 Preparing to Handle Incidents

Table 3-1 lists tools and resources available that may be of value during incident handling.

<table>
<thead>
<tr>
<th>Incident Analysis Hardware and Software</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Digital forensic workstations</strong> and/or <strong>backup devices</strong> to create disk images, preserve log files, and save other relevant incident data</td>
</tr>
<tr>
<td><strong>Laptops</strong> for activities such as analyzing data, sniffing packets, and writing reports (see discussion below table)</td>
</tr>
<tr>
<td><strong>Spare workstations, servers, and networking equipment, or the virtualized equivalents</strong>, which may be used for many purposes, such as restoring backups and trying out malware</td>
</tr>
<tr>
<td><strong>Blank removable media</strong></td>
</tr>
<tr>
<td><strong>Portable printer</strong> to print copies of log files and other evidence from non-networked systems</td>
</tr>
<tr>
<td><strong>Packet sniffers and protocol analyzers</strong> to capture and analyze network traffic</td>
</tr>
<tr>
<td><strong>Digital forensic software</strong> to analyze disk images</td>
</tr>
<tr>
<td><strong>Removable media</strong> with trusted versions of programs to be used to gather evidence from systems</td>
</tr>
</tbody>
</table>
“Create a Breach Response Plan”

NIST

FTC

Experian

RIMS
Not sustainable
What does a digital surveillance camera look like?
What does a digital surveillance camera look like?

DATABASE LOGS

VPN logs

Email/OWA logs

Firewall Logs

System Logs
What does a digital surveillance camera look like?

IR logs?!
Why settle?
1. Execution
2. Filesystem
3. Registry
4. Network
1. Execution
2. Filesystem
3. Registry
4. Network
10 MB/host/day
IF IT WILL BE IMPORTANT THEN

IT IS IMPORTANT NOW
Call to Action
Call to Action

Protect  Detect  Respond  Recover

Typical resource allocation

Shift resources to the right

Required resource allocation
Call to Action
2012 SANS DF4IR SUMMIT

= Google
Call to Action
2013 SANS DF&IR SUMMIT
≠ Google