Emerging Threats – How Bad is it Out there?

June, 2012

Laz
Director of Strategy, Silver Tail Systems
laz@silvertailsystems.com
Twitter: iamlaz
Agenda

• Intros
• Emerging Threats - Real World Case Studies of What Cyber Criminals are Doing
• Where is Mobile in the Mix?
• Quantifying the Threats and Risks
• Reporting – What Leadership Teams are Looking for Today
Company Snapshot

Solution

• Web Session Intelligence Software
  • Two Products:
    • Forensics and Mitigator

• Detects Threats To Websites, Stops Fraud & Other Attacks

• Self Learning, No Training Required

• Provides Visibility Into Real Time Web Traffic For Analytics

• 5 Patents Pending

• Gartner Visionary

Awards

Investors
“The Web fraud detection market grew about 25% in 2011 as unrelenting cyberattacks and data breaches persisted.

Smaller vendors drove innovation, and their products were often added on top of existing.”

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Silver Tail Systems.
# The Threat Landscape

<table>
<thead>
<tr>
<th>Threats</th>
<th>Problem Statement</th>
<th>Addressing the Issue</th>
</tr>
</thead>
</table>
| **Application Security**        | Web application vulnerabilities lead to significant financial, regulatory and reputational risks. | 1. Application scanning  
2. Source code analysis  
   1. Web Sites  
   2. APIs  
   3. Mobile  
3. Manual review and pen test  
4. Review that submit button  
5. Determine how business logic can be abused |
| **Network/OS/Database**         | Validate that all network equipment and server operating systems are current, patched and secure from external threat, Trojans, and/or malware. | 1. Network and OS Scanning  
2. File Integrity Monitoring  
3. Database Scanning |
| **Malicious Activity/DDoS**     | Web site traffic has become a mix of good and bad behavior. As sophisticated bots make their way through your site, it is critical to understand they type of behavior and the motivation for the visitors on your site. | 1. Create an event classification system  
2. Alerts should be tied to the event classification system  
3. Be able to research on the malicious activity - quickly |
| **Emerging Threats**            | It has become increasingly difficult to identify, monitor, and respond to new threats to online, mobile, and social integration. | 1. Subscribe to a monitoring service that allows you to detect emerging threats  
2. Invest in emerging technology to address these types of issues |
Identifying Known Issues

• Identifying the issues through traditional testing:
  – Pen testing
  – Application/Network/OS Scans
  – Internal testing
  – Monitoring/SIEM
What About Unknown Issues?

• Some indicators that things are going bad
  – Always starts with a phone call
  – Site performance degrading over time, which resulted in a decline of sales due to bad performance
  – Increase in Customer Service phone calls
• Research is time consuming!
  – How can you justify pulling revenue generating resources off projects to investigate something?

How will this type of behavior hurt the company brand?
These are Still Well Known Issues

• Man in the Middle
• Man in the Browser
• Man in the Mobile

Criminal behavior looks much different than normal behavior
Some Unknown Issues

• People gaming the system to abuse marketing, sweepstakes, loyalty, and incentive programs
• Increase to fraudulent activities due to lack of visibility into the Web session – cyber criminals are getting more creative with their approach!
• Manipulating the session with Mobile devices
• Site scraping for content, pricing, or inventory/architecture probing
• DDoS (recon and actual attack) attacks

IDS/IPS/WAF and transaction-based solutions are being by-passed by cyber criminals
Research – Attack Ecosystem

• Cheating Network
  – This site will help the cyber criminal break your sweepstakes or Web-based promotion

• The Botting Network
  – This site will allow you to have a bot created for a small investment

• Pastebin
  – This site is great for cybercriminals to share information
Cheating Network
Cheating Network

Captcha Built In!
<table>
<thead>
<tr>
<th>Title</th>
<th>Started By/Date</th>
<th>Replies</th>
<th>Last Post</th>
<th>Forum</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Release] Auto URL Refresher</td>
<td>Chence, Today 04:38 PM</td>
<td>3</td>
<td>Today 05 by Chence</td>
<td>Public Bot / Exploit</td>
</tr>
<tr>
<td>Clixchoice - clixchoice.com</td>
<td>darwin, 02-25-2012 07:51 AM</td>
<td>2</td>
<td>Today 04 by darwin</td>
<td>Paid To Click</td>
</tr>
<tr>
<td>Quesion</td>
<td>Chence, Today 01:12 PM</td>
<td>3</td>
<td>Today 04 by Chence</td>
<td>Chit Chat</td>
</tr>
<tr>
<td>Youtube Partnership</td>
<td>lg342, 02-23-2011 08:35 PM</td>
<td>7</td>
<td>Today 04 by mawr</td>
<td>Chit Chat</td>
</tr>
<tr>
<td>Sticky: [Release] Make your own bots</td>
<td>grapplinghook, 11-03-2008 06:28 PM</td>
<td>126</td>
<td>Today 03 by docisemo</td>
<td>Public Bot / Exploit</td>
</tr>
<tr>
<td>GemBucks - <em><strong>Brand New</strong></em> - GPT</td>
<td>SearchAndWin, 02-03-2012 02:24 PM</td>
<td>3</td>
<td>Today 03 by vReqRz</td>
<td>Get Paid To</td>
</tr>
<tr>
<td>Easy Guide to a Gaming Partnership on</td>
<td>Ewok, 03-15-2012 12:52 AM</td>
<td>4</td>
<td>Today 03 by sk8</td>
<td>Public Bot / Exploit</td>
</tr>
<tr>
<td>$25 gift card</td>
<td>oo7josh, 02-23-2012 12:24 PM</td>
<td>27</td>
<td>Today 03 by oo7josh</td>
<td>Received In The</td>
</tr>
<tr>
<td>$50 from Giftcards</td>
<td>Nexus, Yesterday 02:15 PM</td>
<td>10</td>
<td>Today 03 by cashdo0d</td>
<td>Received In The</td>
</tr>
</tbody>
</table>
Why hello there, welcome to thebotnet.com.

You're viewing our boards as a guest which limits your access. By joining our free community, you can post topics, pm members, download & upload stuff, read exclusive threads, and many more special features. You'll also get access to all of our threads as a registered user.

Registration is free & takes only a few seconds! Click here & join our community today!
TBN – The Botting Network

We make it easy to compare rates and save.

Links: gun rights in america, free mixtapes, ubot coupon, top dubstep

TBN is about personal gain via the internet - we've mastered the art of receiving physical freebies, making a living online, winning sweepstakes, and programming bots that make the whole process a breeze.
Quantifying the Loss

03-17-2012, 01:09 PM

Hopefully this will motivate more to reap the benefits of botting. These were won from an instant win game in less than 2 weeks. From this rape I got the following:

- 384 $50 gift cards (Total is $19,200)
- 2 $3000 Espress machines (Boxes unopened - $6000)
- 8 $300 Coffee makers (Not shown - $2400)
- 5 $50 electric kettles ($250)
- 15 $200 Coffee grinders ($3000)

Used coupon for all machines. Plan to resell them at retail store at full price.

Total value: $30,850

$60,000 a Month Loss - $720,000 a Year Loss
| 1. Giveaway of the Month: Get a $100 Gift Card |
| 2. http://up2datenews.net/get-a-100-gift-card/ |
| 3. Giveaway of the Month: Get a $100 Gift Card |
| 4. http://up2datenews.net/get-a-100-gift-card/ |
| 5. Giveaway of the Month: Get a $100 Gift Card |
| 7. Giveaway of the Month: Get a $100 Gift Card |
| 8. http://up2datenews.net/get-a-100-gift-card/ |
| 9. Giveaway of the Month: Get a $100 Gift Card |
| 10. http://up2datenews.net/get-a-100-gift-card/ |
| 11. Giveaway of the Month: Get a $100 Gift Card |
| 12. http://up2datenews.net/get-a-100-gift-card/ |
| 13. Giveaway of the Month: Get a $100 Gift Card |
| 15. Giveaway of the Month: Get a $100 Gift Card |
| 17. Giveaway of the Month: Get a $100 Gift Card |
| 18. http://up2datenews.net/get-a-100-gift-card/ |
| 19. Giveaway of the Month: Get a $100 Gift Card |
| 20. http://up2datenews.net/get-a-100-gift-card/ |
OpUkraine TARGET & HIVE LIST ~!

BY: ANONYMS EUROPE ON JUN 6TH, 2012 | SYNTAX: NONE | SIZE: 0.71 KB | HITS: 952 | EXPIRES: NEVER

1. OpUkraine
2. Targets today:
6. hive target 1: http://pastehtml.com/view/c01r1magc.htm
7. hive target 2: http://pastehtml.com/view/c01lstsnjg.html
8. hive target 3: http://pastehtml.com/view/c01szt4r0.html
9. backuphive target 1: http://pastehtml.com/view/c0lvs7owy.html
10. backuphive target 2: http://pastehtml.com/view/c0lw4kb5e.html
12. Facebook event at: http://www.facebook.com/events/422336941131837/
13. We are Anonymous
14. We are Legion ~!
15. We do not Forgive
16. We do not Forget
17. Uefa, Ukraine Governm. & sponsors Expect Us ~!
Where is Mobile in the Mix?

• Gartner Says Worldwide Smartphone Sales Soared in Fourth Quarter of 2011 With 47% Growth
Mobile Issues

• Business Drivers
  – We want to have a multi channel solution to acquire and retain customers through the use of email updates, instant coupons, rebates, alerts, and other promotions to our customers
  – We want to communicate with all of our customers in near-realtime and make it easy for them to interact with us anytime/anywhere
What it Looks Like – Criminal View
SMS Trojans (SMiShing)

Apple is looking for iPhone 5 testers! The first 1000 users that go to http://mobilebetatest.com and enter code 0214 will get to test & keep a new iPhone 5
Increase in Malicious Behavior

• Who’s paying for malicious activities?
• Is this type of behavior violating the Terms of Use of your Web site agreement?
• Traditional malicious behavior is changing – not just hard dollars anymore
• Moving to other parts of the site to compromise the system and/or business logic

Engage Risk, Fraud, IT Ops, and Legal to Discuss the Emerging Threats
Quantifying the Risks

- What is the event?
- What is the threat event frequency?
- What is the threat capability?
- How does this impact the bottom line?
- How many suspicious clicks were there on the site?
- How fast are users moving through the site?
Reporting

• What types of information are you reporting on today?
  – PCI Compliance?
  – OS Patching Updates?
  – Time to Resolve Application Vulnerabilities?
Quantifying the Risks – DDoS Example

<table>
<thead>
<tr>
<th></th>
<th>Before Web Session Intelligence</th>
<th></th>
<th></th>
<th></th>
<th>After Web Session Intelligence</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Resources</td>
<td>Time</td>
<td>Total Hours</td>
<td>Estimated Cost</td>
<td>Resources</td>
<td>Time</td>
<td>Total Hours</td>
</tr>
<tr>
<td>Operations</td>
<td>10</td>
<td>80</td>
<td>800</td>
<td>$64,000</td>
<td>2</td>
<td>20</td>
<td>40</td>
</tr>
<tr>
<td>Program Team</td>
<td>16</td>
<td>120</td>
<td>1920</td>
<td>$153,600</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>System Engineering</td>
<td>6</td>
<td>120</td>
<td>720</td>
<td>$57,600</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Development</td>
<td>4</td>
<td>120</td>
<td>480</td>
<td>$38,400</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>InfoSec</td>
<td>4</td>
<td>240</td>
<td>960</td>
<td>$76,800</td>
<td>2</td>
<td>30</td>
<td>60</td>
</tr>
<tr>
<td>QA</td>
<td>4</td>
<td>120</td>
<td>480</td>
<td>$38,400</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Call Center Support</td>
<td>6</td>
<td>120</td>
<td>720</td>
<td>$57,600</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Network Teams</td>
<td>4</td>
<td>120</td>
<td>480</td>
<td>$38,400</td>
<td>1</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>Incident Management Team</td>
<td>4</td>
<td>160</td>
<td>640</td>
<td>$51,200</td>
<td>1</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>Legal</td>
<td>2</td>
<td>120</td>
<td>240</td>
<td>$19,200</td>
<td>1</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>Loss Prevention / Fraud</td>
<td>2</td>
<td>120</td>
<td>240</td>
<td>$230,400</td>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Totals</td>
<td>62</td>
<td>1440</td>
<td>7680</td>
<td>$825,600</td>
<td>13</td>
<td>204</td>
<td>254</td>
</tr>
</tbody>
</table>

| Total Internal Costs by Incident | $825,600 | 13 | 170 | 220 | $20,320 |
| Total Lost Revenue by Hour     | $456,621 |   |    |    | $57,078 |
| Total Loss Exposure Per Incident| $1,282,221| | | | $77,398 |

Estimated Loss Exposure by Year

Brand and Reputation Impact are Not Included in this Example
Staying Ahead – Where to Go

• OWASP Meetings
• ISSA Meetings
• ISACA Meetings
• US Secret Service Briefings
• FBI InfraGard
• E-crime Congress
• Financial Services - Information Sharing and Analysis Center (FS-ISAC) (Finance / Financial Services)
• Merchant Risk Council (MRC) (Online / Retail)
Resources

- www.cheatingnetwork.net
- www.cybercrime.gov
- wwwdatalossdb.org
- www.darkreading.com
- www.e-crimecongress.org
- www.fsisac.com
- www.isc2.org
- www.merchantriskcouncil.org
- www.owasp.org
- www.pastebin.com
- www.silvertailsystems.com
- www.thebotnet.com

Continue to Build Your Network of Subject Matter Experts!
Questions?

Thank You!

Laz
Director of Strategy, Silver Tail Systems
laz@silvertailsystems.com
Twitter: iamlaz