

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

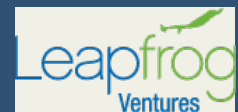
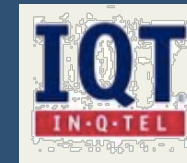
Solution

- 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



Silver Tail Systems

Positioned As A Leader In 2012 Web Fraud Magic Quadrant



“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

| Threats | Problem Statement | Addressing the Issue |
|--------------------------|--|--|
| Application Security | Web application vulnerabilities lead to significant financial, regulatory and reputational risks. | <ol style="list-style-type: none"> 1. Application scanning 2. Source code analysis <ol style="list-style-type: none"> 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. | <ol style="list-style-type: none"> 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. | <ol style="list-style-type: none"> 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. | <ol style="list-style-type: none"> 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 of 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

The screenshot shows the Cheating Network forum homepage. At the top, there's a navigation bar with links for Home, Forum, Rules, and What's New?. A search bar is on the right. Below the navigation bar, a large banner advertisement for the Nexus S 4G is displayed, featuring the text "Get a Nexus S™ 4G for FREE" and "Sprint". To the left of the banner, a "Site Navigation" menu lists links for Home, Rules, Forum, User CP, and FAQ. Below this, the "Online Users" section shows 13 members and 434 guests. The "Current Poll" section asks "Would you like a CN App Store" and shows results: Yes (55.56%), No (8.33%), and Maybe if I see it first... (36.11%). To the right of the poll, the "Stats" section displays forum statistics: 35,812 members, 91,954 threads, 839,423 posts, and Top Poster: Piru (9,212). Below the stats, a "Recent Threads" section lists several threads, including "\$10 Amazon for \$5...", "Free Pearl Earrings", and "[RELEASE] Auto Swag".

Get a Nexus S™ 4G for **FREE**
Google™ at 4G speeds.
Limited time offer
Online only. Free shipping. Valid for new lines of service only.
nexus S
Get it now
Restrictions apply.
Sprint

If this is your first visit, be sure to check out the **FAQ** by clicking the link above. You may have to register before you can post: click the register link above to proceed. To post your messages, please select the forum that you want to visit from the selection below.

» Site Navigation

- » Home
- » Rules
- » Forum
 - > User CP
 - > FAQ

» Online Users: 447

13 members and 434 guests
cashd00d Champofall21 aNcrypti0N ERich79 Force21 Fubbar Goaliekid jackpackage11 jeffjaff mahto1000 Orangie thebomb Thomas
Most users ever online was 3,200, 12-24-2010 at 10:03 AM.

» Current Poll

Would you like a CN App Store

Yes
55.56%

No
8.33%

Maybe if I see it first...
36.11%

Total Votes: 30
You may not vote on this poll.

» Stats

Members: 35,812
Threads: 91,954
Posts: 839,423
Top Poster: Piru (9,212)
Welcome to our newest member, arnob2sarkar

» Recent Threads

» \$10 Amazon for \$5...
03-15-2012 05:37 PM
by Spyderpig
Last post by Champofall21
Today 01:19 AM
37 Replies 1,060 Views

» Free Pearl Earrings
03-20-2012 01:02 PM
by cashd00d
Last post by cashd00d
Today 01:50 AM
5 Replies 695 Views

» [RELEASE] Auto Swag
02-04-2012 02:45 PM
by joshh131
Last post by joshh131

Cheating Network

Captcha Built In!

Search Single Content Type | Search Multiple Content Types

Search In

Search Types: ☐ All Types ☐ Posts ☐ Forums ☐ Visitor Messages

Search For

Keyword(s):

User Name: ☒ Exact name

Tag:

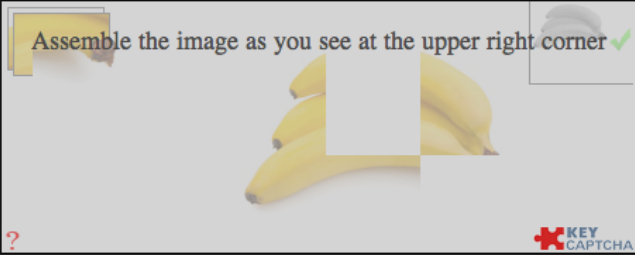
Additional Options

Find Posts:

Sort Results by:



















Antispam, complete the task:

Assemble the image as you see at the upper right corner ✓



KEY CAPTCHA

Cheating Network

| | | | | | |
|--|---|---|-------------------------------|------------------------------------|--------------------------------|
|  | [Release] Auto URL Refresher Started by Chence, Today 04:38 PM |  | Replies: 3 Views: 14 | Last Post: Today 05 by Chence | Forum: Public Bot / Exploit |
|  | Clixchoice - clixchoice.com Started by darwin, 02-25-2012 07:51 AM |  | Replies: 2 Views: 363 | Last Post: Today 04 by darwin | Forum: Paid To Click |
|  | Question Started by Chence, Today 01:12 PM |  | Replies: 3 Views: 217 | Last Post: Today 04 by Chence | Forum: Chit Chat |
|  | Youtube Partnership Started by lg342, 02-23-2011 08:35 PM |  | Replies: 7 Views: 364 | Last Post: Today 04 by mawr | Forum: Chit Chat |
|  | Sticky: [Release] Make your own bots Started by grapplinghook, 11-03-2008 06:28 PM 1 2 3 ... 6 |  | Replies: 126 Views: 26,592 | Last Post: Today 03 by docisemo | Forum: Public Bot / Exploit |
|  | GemBucks - ***Brand New*** - GPT Started by SearchAndWin, 02-03-2012 02:24 PM |  | Replies: 3 Views: 374 | Last Post: Today 03 by vReqRz | Forum: Get Paid To |
|  | Easy Guide to a Gaming Partnership on Started by Ewok, 03-15-2012 12:52 AM |  | Replies: 4 Views: 503 | Last Post: Today 03 by sk8 | Forum: Public Bot / Exploit |
|  | \$25 [redacted] gift card Started by oo7josh, 02-23-2012 12:24 PM 1 2 |  | Replies: 27 Views: 989 | Last Post: Today 03 by oo7josh | Forum: Received In The |
|  | \$50 from [redacted] Giftcards Started by Nexus, Yesterday 02:15 PM |  | Replies: 10 Views: 378 | Last Post: Today 03 by cashd00d | Forum: Received In The |

THE BOTNET



User Name

☐ Remember Me?

Login

Home

Register

Shop

IRC

Scammers

Today's Posts

User CP

Search



Show Google
how you like to
use the web.

We'll use the data to
make the Internet just
a little better.

Join the Screenwise
Trends Panel

Contest is now live! [Click for details](#)



Please like TBN!



Like

1k

Notices

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 no longer see ads inside of every thread or this guest notice.

Registration is free & takes only a few seconds! [Click here](#) & join our community today!

Lobby

| | Forum | Last Post | Threads | Posts |
|--|---|---|---------|---------|
| | Announcements The latest news and announcements! Contests | Youtube Forum by mixermax0 Today 09:06 AM | 141 | 5,176 |
| | General / Off Topic If it doesn't belong in another section, post it here. Subforum: Intros , The Internets | Ebay & paypal problem by FlyCoyotee Today 05:20 PM | 18,278 | 145,344 |
| | Our Community Community driven discussions. Subforum: Suggestions , Help! & IRC | Post Your Desktop by enchy Today 04:52 PM | 2,973 | 37,604 |
| | Check It Out Have something worth bragging about? Show us. | \$20 Center of Prizes Winner! by mantalcore Today 01:25 PM | 2,494 | 33,208 |

Cake

| | Forum | Last Post | Threads | Posts |
|--|---|--|---------|--------|
| | Make Money Share & discuss ways to profit with fellow money minded members. Subforum: GPT Money | best GPT site of all time!... by bestGPTreview Today 05:17 PM | 6,823 | 87,853 |

TBN – The Botting Network



| | |
|--------------------|-------------------|
| PROGRESSIVE 348 | STATE FARM 440 |
| NATIONWIDE 485 | AM. FAMILY 556 |

We make it easy
to compare rates and save.

Enter
ZIP Code:

[Get Your Free Quote](#)

All times are GMT -5. The time now is 05:30 PM.

[Contact Us](#) - [TBN](#) - [The Botting Network](#) - [Archive](#) - [Top](#)

Powered by vBulletin®
Copyright ©2000 - 2012, Jelsoft Enterprises Ltd.
The Botting Network, ©2011


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 Espresso 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



Do more and recharge less with the all-in-one mobile processor.

Learn More

New Paste

Optional Paste Settings

Syntax

None

Flag Expiration:

Never

Paste Exposure:

Public

Paste Name /

Title:

Submit



Hello Guest

Sign Up

or Login



Sign in with Facebook



Sign in with Twitter



Sign in with Google

You are currently not logged in, this means you can not edit or delete anything you paste. [Sign Up](#) or [Login](#)

Public Pastes

- ac | 14 sec ago
- Untitled | 13 sec ago
- Untitled | 19 sec ago
- Untitled | 20 sec ago
- Untitled | 20 sec ago
- Untitled | 24 sec ago
- Untitled | 25 sec ago
- Untitled | 25 sec ago

Recommended

3 Steps for a Faster PC

Three easy steps:

1. Click "Start Download".
2. Run the quick scan.
3. Fix the errors.

START
DOWNLOAD

Microsoft Partner



RegClean Pro

★★★★★

"winner of over 100 5-star awards"

Pastebin.com Tools & Applications



iPhone/iPad



Windows



Firefox



Chrome



WebOS



Android



Mac



Opera



Click.to



create new paste | api | trends | users | faq | tools | domains center | privacy | contact | stats | go pro

Follow us: [pastebin on facebook](#) | [pastebin on twitter](#) | [pastebin in the news](#)

Some friends: [hostshut](#) | [fileshut](#) | [hostlogr](#) | [w3patrol](#)

Pastebin v3.1 rendered in: 0.004 seconds



PASTE BIN

[Follow @pastebin](#)

search...

[create new paste](#)[trending pastes](#)[sign up](#) | [login](#) | [my alerts](#) | [my settings](#) | [my profile](#)**Do more and recharge less with the all-in-one mobile processor.**

Learn More



New Paste

Optional Paste Settings

Syntax Highlighting:

None

Paste Expiration:

Never

Paste Exposure:

Public

Paste Name / Title:

Submit

Hello Guest

[Sign Up](#)

or

[Login](#)[Sign in with Facebook](#)[Sign in with Twitter](#)[Sign in with Google](#)

Public Pastes

- [ac](#)
TCL | 14 sec ago
- [Untitled](#)
13 sec ago
- [Untitled](#)
19 sec ago
- [Untitled](#)
20 sec ago
- [Untitled](#)
20 sec ago
- [Untitled](#)
24 sec ago
- [Untitled](#)
25 sec ago
- [Untitled](#)
25 sec ago

Recommended

3 Steps for a Faster PC

Three easy steps:

1. Click "Start Download".
2. Run the quick scan.
3. Fix the errors.

START



PASTE BIN

[Follow @pastebin](#)

[create new paste](#)
[trending pastes](#)
[sign up](#) | [login](#) | [my alerts](#) | [my settings](#) | [my profile](#)


\$100 [redacted] Gift Card

BY: A GUEST ON FEB 24TH, 2012 | SYNTAX: **NONE** | SIZE: 0.56 KB | HITS: 16 | EXPIRES: NEVER

[DOWNLOAD](#) | [RAW](#) | [EMBED](#) | [REPORT ABUSE](#)

[f](#) 0

[t](#) 0

Public Pastes

- [Untitled](#) 7 sec ago
- [Untitled](#) 2 sec ago
- [Watch Clare vs Wat...](#) 1 min ago
- [Untitled](#) 5 sec ago
- [Untitled](#) 8 sec ago
- [Untitled](#) 9 sec ago
- [Untitled](#) 9 sec ago
- [Untitled](#) 14 sec ago

Snapdragon... Play On

[Learn More](#)


snapdragon
by Qualcomm



```

1. Giveaway of the Month: Get a $100 [redacted] Gift Card
2.
3. http://up2datenews.net/get-a-100-[redacted]gift-card/
4.
5.
6. Giveaway of the Month: Get a $100 [redacted] Gift Card
7.
8. http://up2datenews.net/get-a-100-[redacted]gift-card/
9.
10. Giveaway of the Month: Get a $100 [redacted] Gift Card
11.
12. http://up2datenews.net/get-a-100-[redacted]gift-card/
13.
14. Giveaway of the Month: Get a $100 [redacted] Gift Card
15.
16. http://up2datenews.net/get-a-100-[redacted]gift-card/
17.
18.
19. Giveaway of the Month: Get a $100 [redacted] Gift Card
20.
21. http://up2datenews.net/get-a-100-[redacted]gift-card/
    
```



Clean your



PASTEBIN

Follow @pastebin

search...



create new paste

trending pastes

sign up | login | my alerts | my settings | my profile



OpUkraine TARGET & HIVE LIST ~!

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

DOWNLOAD | RAW | EMBED | REPORT ABUSE

f 91

12

Public Pastes

- Untitled
0 sec ago
- Untitled
1 sec ago
- Untitled
2 sec ago
- Untitled
36 sec ago
- closure
Clojure | 5 sec ago
- Untitled
6 sec ago
- Untitled
7 sec ago
- 10F322test
8 sec ago

Breathe Fire Into Your Mobile Games

Learn More

snapdragon
by Qualcomm

```
1. OpUkraine
2. Targets today:
3.
4. 1.Ministry of Justice http://www.minjust.gov.ua/
5. 2.Ministry of Police http://mvs.gov.ua/
6. 3.Government`s Portal http://www.kmu.gov.ua/
7.
8. hive target 1: http://pastehtml.com/view/c0lrlmagc.htm
9. hive target 2: http://pastehtml.com/view/c0lstnsjg.html
10. hive target 3: http://pastehtml.com/view/c0lszt4r0.html
11.
12. backuphive target 1: http://pastehtml.com/view/c0lvsw7oy.html
13. backuphive target 2: http://pastehtml.com/view/c0lw4kb5e.html
14. backuphive target 3: http://pastehtml.com/view/c0lwg273p.html
15.
16. Facebook event at : http://www.facebook.com/events/422336941131837/
17.
18. We are Anonymous
19. We are Legion ~!
20. We do not Forgive
21. We do not Forget
22. Uefa, Ukraine Governm. & sponsors Expect Us ~!
```



Clean your

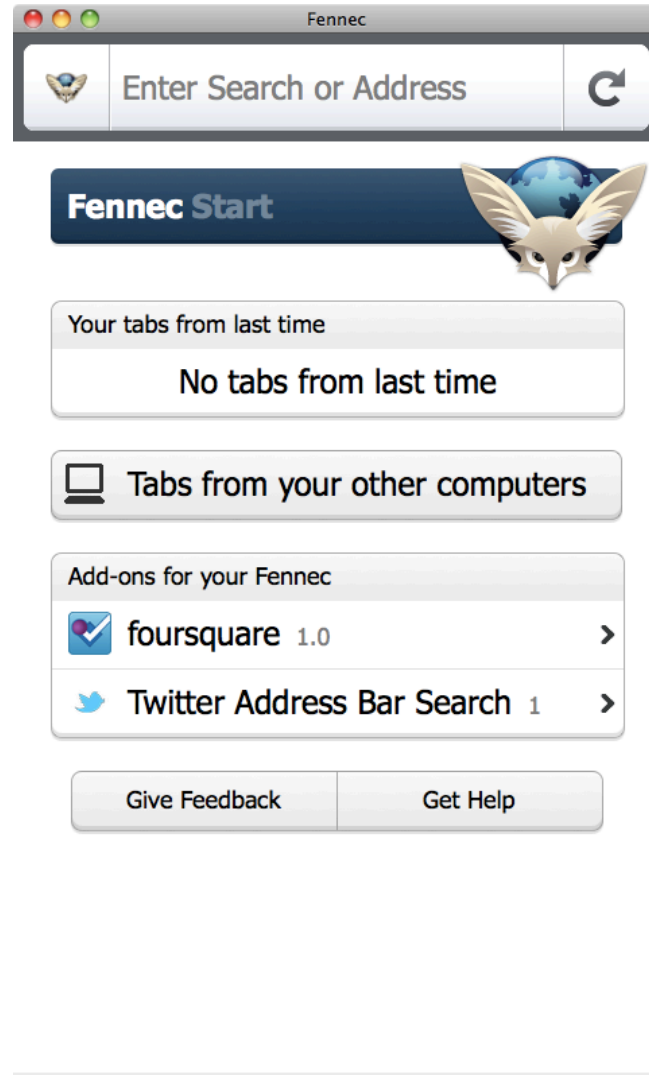
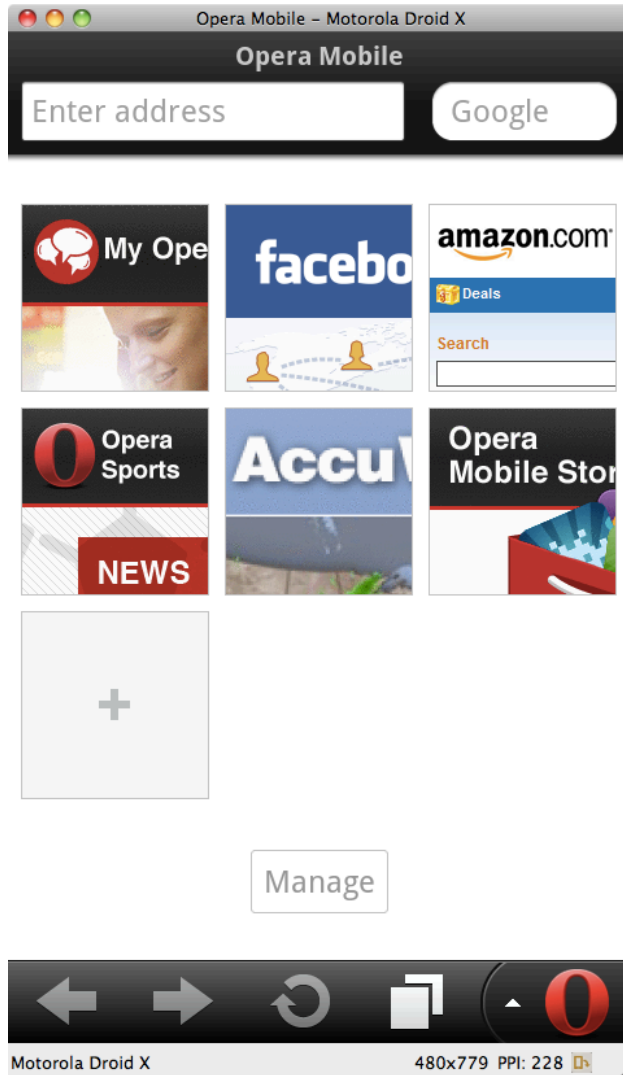
Where is Mobile in the Mix?

- Gartner Says Worldwide Smartphone Sales Soared in Fourth Quarter of 2011 With 47% Growth

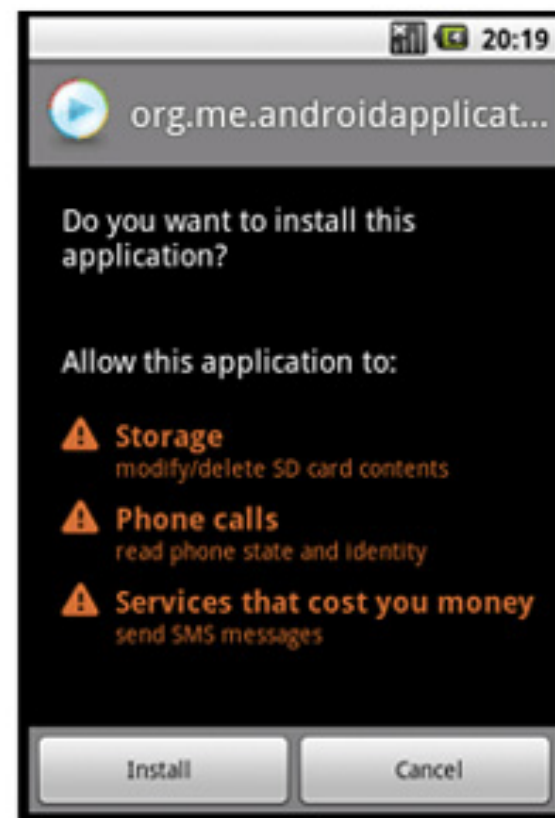
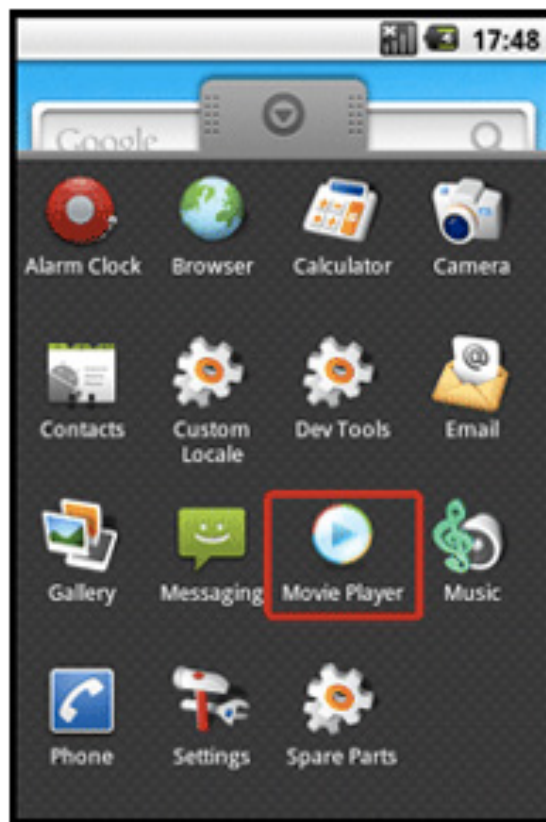
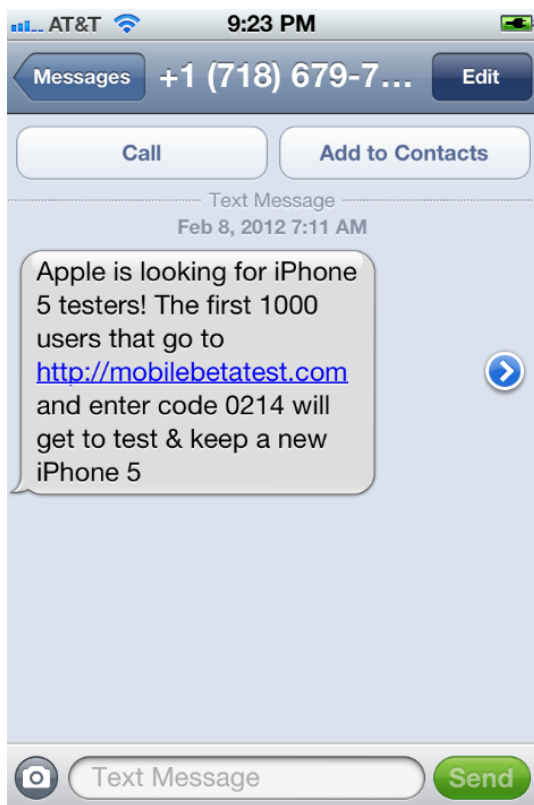
Mobile Issues

- 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)



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

| | | | | | | | |
|----------------------------|---------|--------|---------|-----------------------------|-------|-----------------------------|-------|
| | Per Day | Hourly | Average | BWSI Outage Frequency | Hours | AWSI Outage Frequency | Hours |
| Internal Bill Rate per Day | \$600 | \$75 | \$80.00 | | 4 | | 0.5 |
| External Bill Rate per Day | \$680 | \$85 | | | 2 | | 2 |

| Team to Research, Remediate, and Address the Issue | Before Web Session Intelligence | | | | After Web Session Intelligence | | | |
|--|---------------------------------|------|-------------|----------------|--------------------------------|------|-------------|----------------|
| | Resources | Time | Total Hours | Estimated Cost | Resources | Time | Total Hours | Estimated Cost |
| Operations | 10 | 80 | 800 | \$64,000 | 2 | 20 | 40 | \$3,200 |
| Program Team | 16 | 120 | 1920 | \$153,600 | 1 | 10 | 10 | \$800 |
| System Engineering | 6 | 120 | 720 | \$57,600 | 1 | 10 | 10 | \$800 |
| Development | 4 | 120 | 480 | \$38,400 | 1 | 10 | 10 | \$800 |
| InfoSec | 4 | 240 | 960 | \$76,800 | 2 | 30 | 60 | \$4,800 |
| QA | 4 | 120 | 480 | \$38,400 | 1 | 10 | 10 | \$800 |
| Call Center Support | 6 | 120 | 720 | \$57,600 | 1 | 10 | 10 | \$800 |
| Network Teams | 4 | 120 | 480 | \$38,400 | 1 | 40 | 40 | \$3,200 |
| Incident Management Team | 4 | 160 | 640 | \$51,200 | 1 | 40 | 40 | \$3,200 |
| Legal | 2 | 120 | 240 | \$19,200 | 1 | 20 | 20 | \$1,600 |
| Loss Prevention / Fraud | 2 | 120 | 240 | \$230,400 | 1 | 4 | 4 | \$320 |
| Totals | 62 | 1440 | 7680 | | 13 | 204 | 254 | |
| 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 | | | | \$2,564,442 | | | | \$154,795 |

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
- www.datalossdb.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