



**FOR PUBLIC RELEASE: 10/22/09**

---

## **Email Security Research Overview**

Technical evaluation of email security controls to protect against directed/small scale email attacks

---

October 22, 2009

PacketFocus, LLC  
11900 State Hwy 160  
Hayden, Alabama 35079

Phone: (205) 994-6573 x5  
Email: [info@packetfocus.com](mailto:info@packetfocus.com)



User Attack Framework (**UAF**) Provided by:

## Contents

Contents.....	2
Document Control.....	3
Document History .....	3
Document Distribution.....	3
1 Assessment Results.....	4
1.1 Key Findings and Recommendations .....	4
2 Executive Summary.....	6
2.1 Understanding of Phishing .....	6
2.2 Test Objectives .....	8
2.3 Scope of work.....	8
2.4 Scenario Details .....	9
2.4.1 Scenario #1 .....	10
2.4.2 Phishing Site.....	11
2.4.3 What we found out about users that visited the phishing site. ....	12
3 Security Recommendations.....	14
4 About PhishCamp.com.....	15

## Document Control

### Document History

Version	Date	Author	Comments
0.1	Sept 25 2009	Joshua Perrymon	Final Draft
0.2	Oct 21 2009	Joshua Perrymon	Release Version

### Document Distribution

Version	Date	Comments
0.1	Sept 25 2009	PacketFocus Internal
0.2	Oct 21 2009	Released to Vendors
0.2	Oct 22 2009	Public version released to media
0.3	Oct 28 2009	Vulnerable Email Clients Released to Public
0.4	Nov 4 2009	Vulnerable Email Appliance/SaaS/Software Vendors Released
0.5	Nov 11 2009	Vulnerable SmartPhones Released

#### Author

Name: Joshua Perrymon, CEH, OPST, OP  
Position: CEO – PacketFocus

Phone: (205) 994-6573 x5

Email: [josh@packetfocus.com](mailto:josh@packetfocus.com)

Web: <http://www.packetfocus.com> , <http://www.phishcamp.com>

Twitter: <http://www.twitter.com/packetfocus>

LinkedIn: [www.linkedin.com/in/packetfocus](http://www.linkedin.com/in/packetfocus)

# 1 Assessment Results

## 1.1 Key Findings and Recommendations

Email Vendor/System Combinations	Results
Removed until 10/28/09	SUCCESS
Removed until 10/28/09	SUCCESS
Removed until 10/28/09	SUCCESS
Removed until 10/28/09	SUCCESS
Removed until 10/28/09	SUCCESS
Removed until 10/28/09	SUCCESS
Removed until 10/28/09	SUCCESS
Removed until 11/4/09	SUCCESS
Removed until 11/4/09	SUCCESS
Removed until 11/4/09	SUCCESS
Removed until 11/4/09	SUCCESS
Removed until 11/4/09	SUCCESS
Removed until 11/4/09	SUCCESS
Removed until 11/4/09	SUCCESS
Removed until 11/11/09	SUCCESS
Removed until 11/11/09	SUCCESS
Removed until 11/11/09	SUCCESS

**SUCCESS** = Phishing Email delivered to inbox without triggering any alerts or alarms.  
**FAIL** = Email is Identified as Phishing/SPAM and alarms or alerts are triggered.

Success Rate

100%

This assessment was designed to measure the effectiveness of available email security controls to protect against **directed/Small-scale** email attacks, as implemented in large enterprise environments. ***The results of this research prove that even the most current email security appliances/ services / clients cannot correctly identify directed Phishing emails, even when the senders email(From:) does not match up with the sending email server (Spoofer).*** For now, the user must make the decision to identify and properly respond to directed email attacks.



This research was not performed to identify weakness in specific vendors, it was to show that directed email attacks bypass the latest and most advanced email systems when configured properly. Before releasing this document, we have contacted all vendors in scope and provided open and fair opportunity to address this issue. *Vendor responses will be included in Appendix A.*

## 2 Executive Summary

### 2.1 Understanding of Phishing

**Phishing is often misunderstood.** At a high level, it can be described as using email to attack users directly. Unlike the telephone or in person, email attacks don't require voice or physical behaviour modifications to bypass natural user defences. Email based attacks rely on trust associations, and using familiar associations such as logos, verbiage, or existing applications they have interacted with in the past to be successful. Samples phishing scenarios used in modern attacks include webmail, VPN, social networks, and other easily identified web applications that require authentication. The goal of a successful phishing scenario sent by email is to have the user instantly trust the look and feel of the request. They process the attackers command like clicking a link or opening an attachment without triggering any alarms in their mind or thought process. The email is from what they think to be a trusted source, so they click on it.

Email Based Attacks	Voice Based Attacks	Physical Attacks
<ul style="list-style-type: none"><li>•No human interaction with the user</li><li>•Targets trust relationships</li><li>•Technology security control weakness</li></ul>	<ul style="list-style-type: none"><li>•Requires real-time interaction with a human</li><li>•Attacker must exploit trust through speech/tempo/tone</li><li>•Easily Recorded</li><li>•Legal issues with recording conversations</li></ul>	<ul style="list-style-type: none"><li>•Requires being onsite</li><li>•Increases risk of being caught on camera or by authorities</li><li>•Attacker must control voice and physical appearance</li><li>•Impersonation/Authority attacks common</li><li>•Trespassing/Etc</li></ul>

Attack payloads vary from credential harvesting, browser exploitation, or malware infestation but can include all of the above in a multi-layered attack. Traditionally, phishing attacks have been sent to millions of users. This could be thought of as SPAM as it leaves a large footprint around the Internet.

Modern phishing attacks are directed towards a single organization to become much more effective as they leave a very small footprint. Most times, the email server, and the phishing web server have never been recognized in the past so there are no records of them being malicious. An enterprise may have 10,000 employees with email access, and the attacker may only target 5-10 in a single attack. All he needs is one (1) user responding to the phishing email to gain access if that is the motivation and design of the attack.

The skill level used in this assessment the reflected effort that a skilled attacker would undertake to perform a targeted attack against an organization. The only difference is that this assessment was performed in a controlled environment with all target email users contacted before sending the email, so we were testing the technology and not the user's response.

# Common Payloads

Client Exploits

Credential Harvesting

Browser/OS

Malware/Spyware

Real-time MITM of tokens

No credentials were stored or processed during this assessment. And no personnel or related company participant information will be revealed publically.

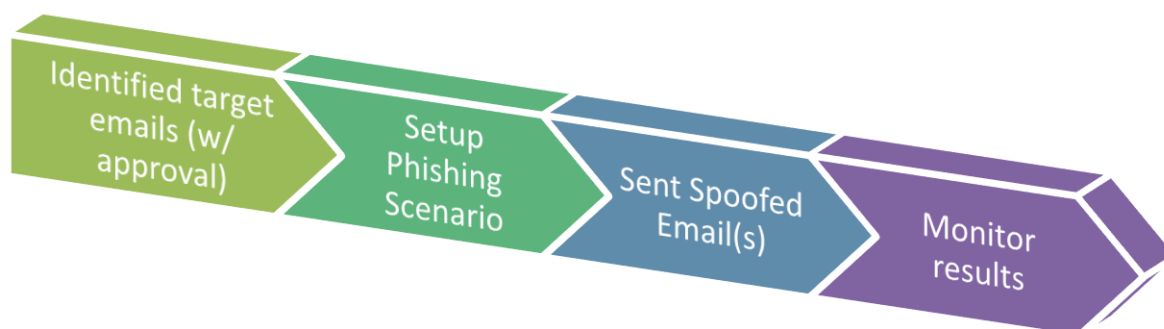
## 2.2 Test Objectives

The objective of this assessment was to measure the effectiveness of current email security controls in Enterprise networks, not the user response. The assessment was performed using the UAF (User Attack Framework) designed by PacketFocus ([www.phishcamp.com](http://www.phishcamp.com)). This framework was based on the manual process we have used for over 10 years, and is the most advanced test framework of its kind available commercially in today's market.

The problem with manual phishing assessments is not sending the emails; it is measure and monitoring the results. The framework solves this key issue by closely tracking each email from creation, to capture and analysis of user generated traffic back to the hosted phishing site. If included in the scope of work, the framework can be used to perform active exploitation on Client devices such as PC's, Desktops, Smartphone's, Etc.

## 2.3 Scope of work

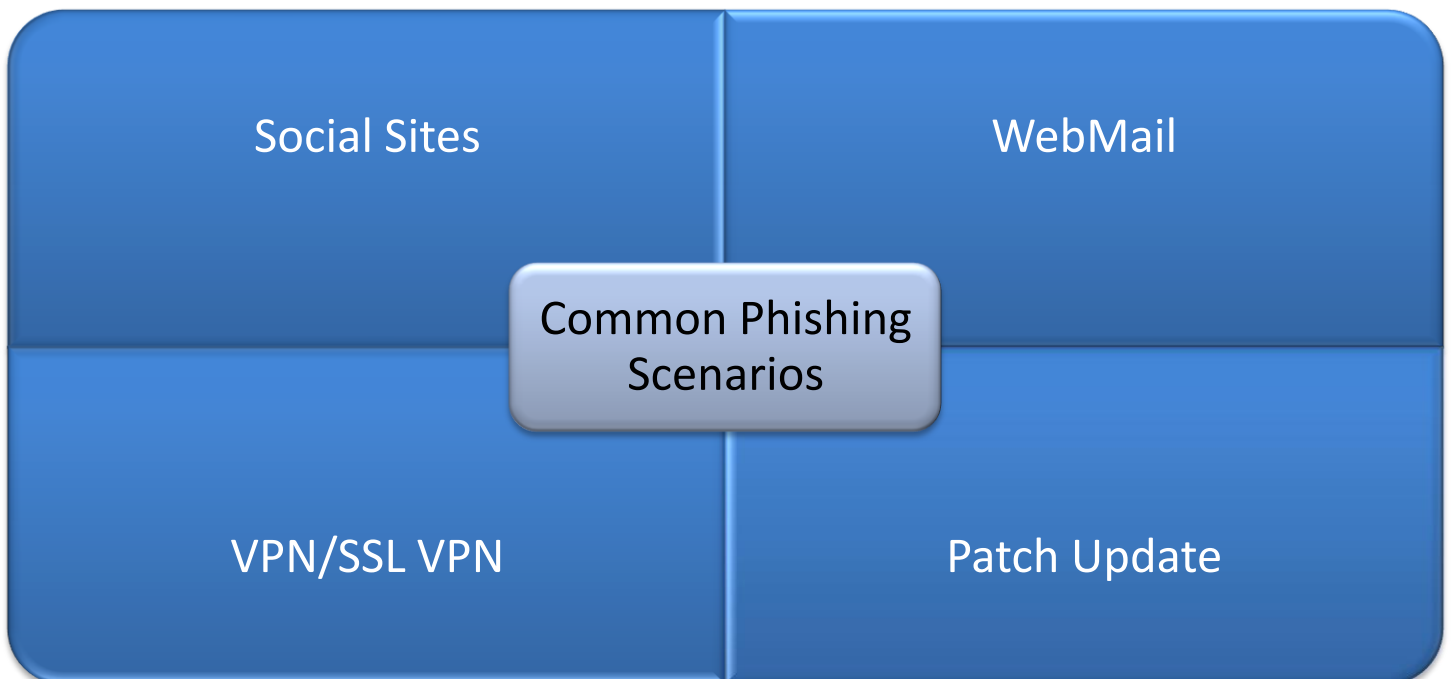
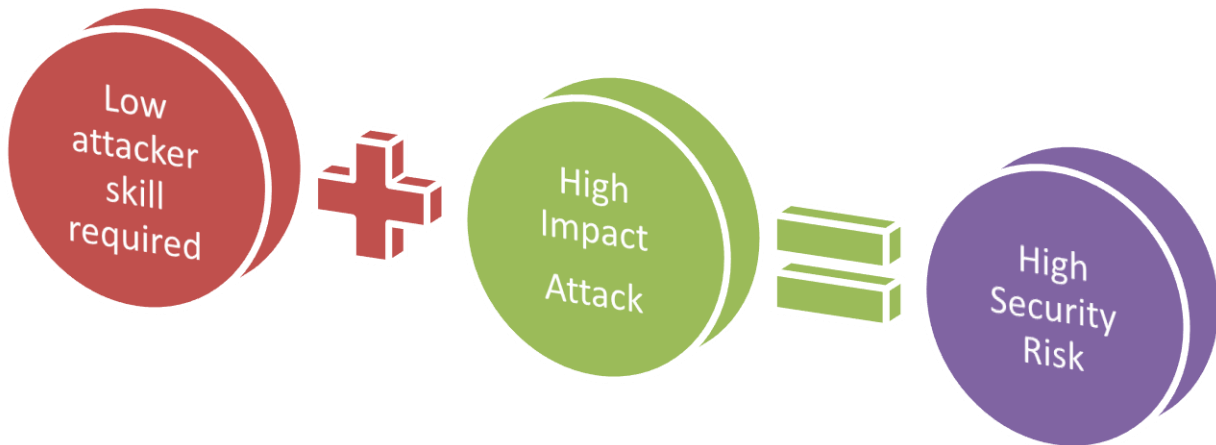
PacketFocus contacted each individual within targeted companies to ask permission before sending any phishing emails. The UAF was configured to send the same email to all participants. No changes were made to the phishing email or phishing site other than changing the TO: address for each target.



For this assessment, no active exploitation was performed nor attempted. Tracking cookies were used if a user access the phishing site provide in the email body, and server side scripts were used to direct users to different sites based on User Agent Data (OS, Browser, Etc).

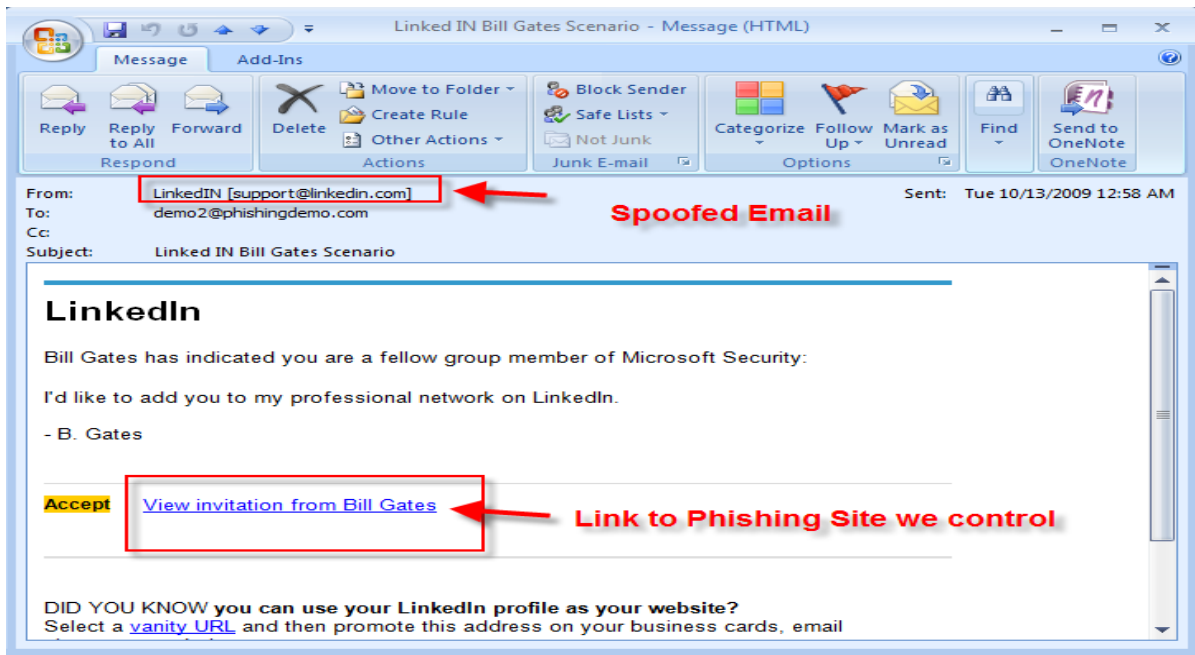
## 2.4 Scenario Details

PacketFocus designed a realistic attack scenario based on a well known Social Site. The technique was a simple “save-as” for the phishing email, with only minor modifications to the HTML code. This is common with what real world attacker would do, so for added realism we performed the same action.

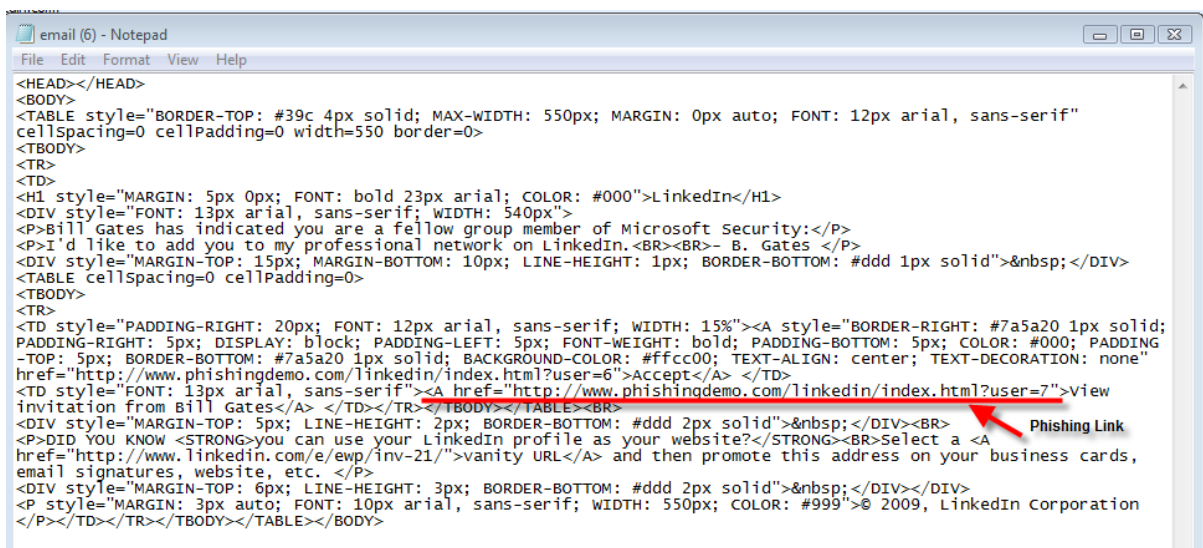


### 2.4.1 Scenario #1

This scenario was an invitation from LinkedIn, posing as an invitation from Bill Gates to join his network. LinkedIn was selected due to availability, and the fact that it is a social network recognized by most executives. This selection of LinkedIn was also based on the fact that linked-in email should be already identified by most existing email system(s), and this may have helped delivery through into the mailbox. The phishing link can be identified in the HTML source code below.



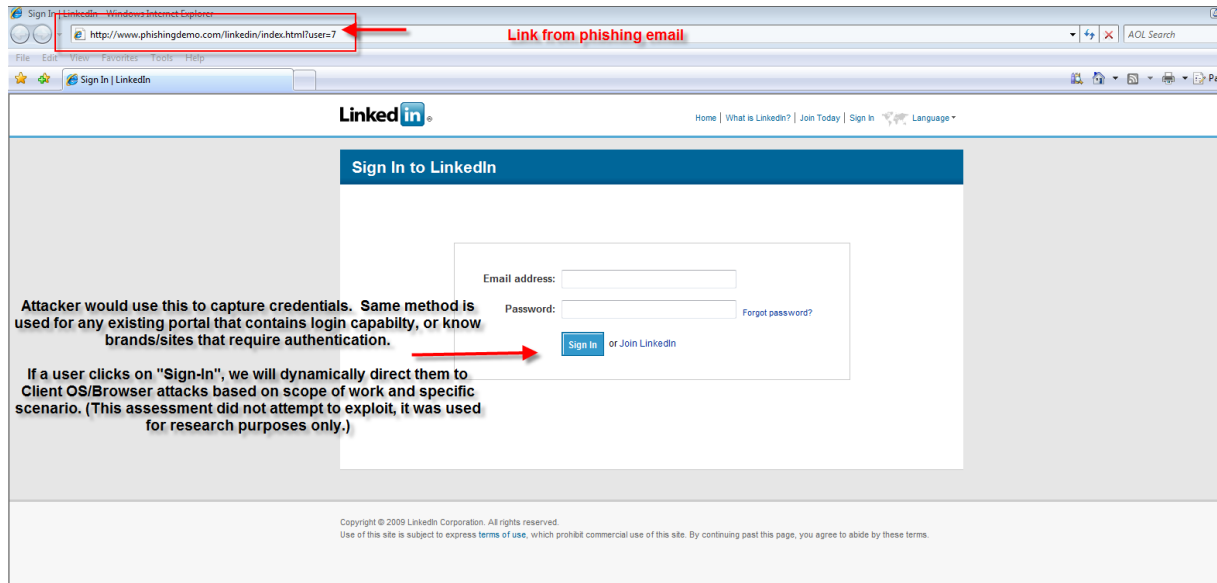
• Figure 1 : Scenario #1: Users asked to login to LinkedIn



• Figure 2 - Spoofed Email HTML Code

## 2.4.2 Phishing Site

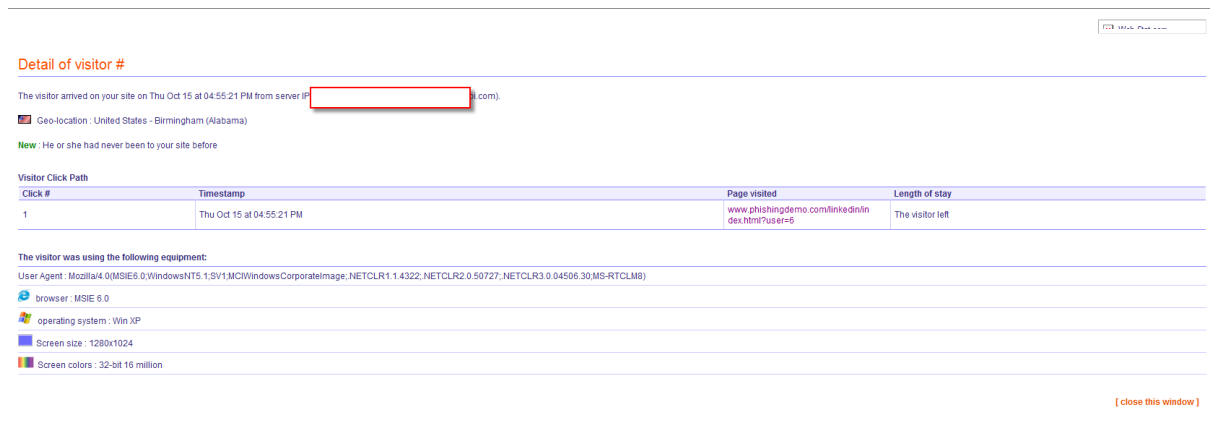
The Phishing site was based on the LinkedIn sign in page. The form action was changed so that the user would be redirected to a subsequent page on our site. No usernames or passwords were collected during this assessment. All targeted users were contacted before the phishing email was sent, and were expecting a LinkedIn invitation from Bill Gates.



• Figure 3 - Phishing Site used for both scenarios

## HTML Source Code in Appendix B

## 2.4.3 What we found out about users that visited the phishing site.



• Figure 4 - UAF Detailed results of each user that visits the phishing site

Another point that we would like to make, is the detailed information passed when a user visits a website. If you notice from the table above, detailed information is passed in USERAGENT headers and optionally parsed by web traffic analysis software. This data is held in web server logs, and is often used to target specific browsers, OS, browser plug-ins, etc.

### What we know about user that visit our phishing sites from UserAgent headers:

<b>TimeStamp</b>	Identifies exact time user visited the phishing site.
<b>UserID</b>	ID of the user, mapped back to phishing email
<b>GeoLocation</b>	Location of user
<b>IP Address</b>	IP Address of the Client/Target
<b>Browser</b>	Client Browser (IE 6.0)
<b>Operating System</b>	Client Operating System ( WIN XP)
<b>Screen Size</b>	1280 x 1024
<b>Screen Colors</b>	32-bit 16 million
<b>Referrer</b>	NA
<b>Page Visited</b>	Identifies pages visited by user on our phishing site
<b>Length Of Stay</b>	Identified how long the user was on the site.

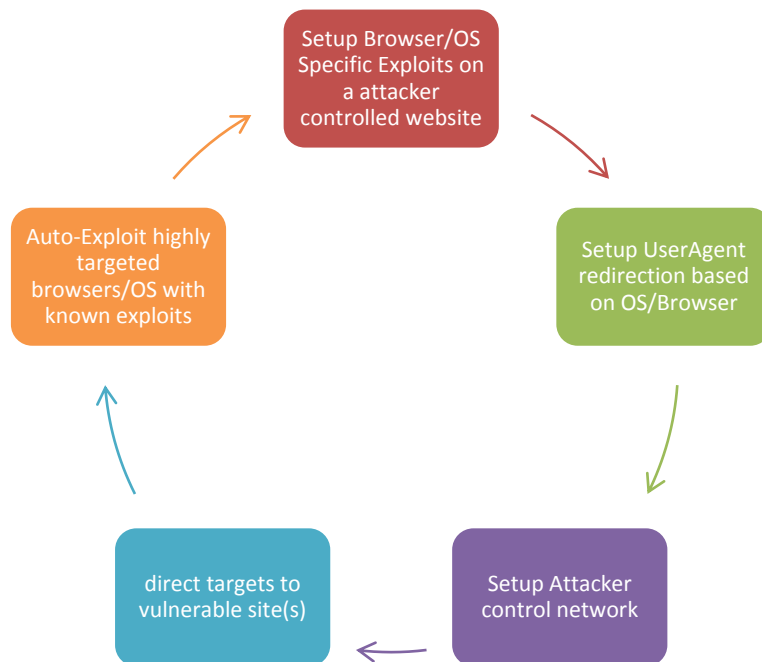
• Figure 5 - USERAGENT Details used to target client specific exploits

Specifically, we are interested in the IP address, the OS, Browser, and any plug-ins installed on the client. This information could be used in a multi-layered attack. We have scripts that read this USERAGENT information, and direct the targeted user to specific application pages.

An example of this could be if we had setup and tested a specific client exploit for Win XP and IE 6. Based on this exploit, we could direct only users with Windows XP AND IE6 to a specific page. If they don't have this specific OS/Browser combo they will be sent to another page. This is invaluable in increasing the chance of exploit success. It works by setting up the exploit (Browser, OS) then, redirecting a targeted user to this page. More open exploits in flash, adobe, images, JavaScript could be used more generally than specific exploits. This also maps back to the attackers intention/motivation/skill level. Some attackers may only want to

harvest credentials, while others may want to exploit clients in attempt to gain access into the internal network. Most this, this can be done by setting up scenarios to gather VPN, WebMail, AD Domain, and other remote access credentials.

Once an attacker has gained access to an internal email account, attachment payloads then become more easily exploitable as they are coming from a known trusted source (Real company email server). Attackers also then have access to internal email contact lists, distribution lists, etc.



### 3 Security Recommendations

This assessment was performed to identify the current security capabilities, among Enterprise email implementations. As identified, we cannot rely on technology to identify, detect, and protect against small scale directed attacks. The reliance must be put upon a proper security awareness program, along with the appropriate Incident response program. The user base should be tested regularly to identify weakness in technology, training, and Incident Response. Technology will eventually catch up to identify spoofed emails, so attackers will then focus on sending emails from valid domains and even companies own email servers. Attackers also target injection attacks in real company applications, and then use that as an attack vector. This way the phishing link would point back to the real site, but use XSS/CSRF to perform the attack. If the attacker has sufficient space for an XSS attack, then a login and password page could be rewritten on target websites and pose a significant risk.

During additional testing, we identified that client browsers, smart phones, email programs, etc have minimal email security controls as they usually work by downloading emails from an email server. If the attack gets to the email server, then it's probably going to be delivered directly to the client email program, and the browser will allow the user to open the link and open the phishing site without alerts or alarms.

Below is a sample process for identifying/mitigation of email based risk.

- 1) Identify existing email security policies and procedures
- 2) Identify Existing email based Incident Response policies and procedures
- 3) Perform an Assessment to identify email **RISK**  
**BASELINE in people and technology**
- 4) Implement technology changes if possible
- 5) Modify training, policies, and incident response as needed
- 6) Implement specific training based on company policies and procedures
- 7) Re-Test to identify change in baseline
- 8) Repeat process

- The reason for reviewing the email policies/processes and Incident response before each assessment is the purpose of the assessments are to identify what users should be doing, and if they are following those procedures. Policies should also define security controls that should be enforced technically.

## 4 About PhishCamp.com

After performing 100's of manual phishing assessments, PacketFocus CEO Joshua Perrymon identified the need for a scalable, managed email testing service to increase corporate protection and awareness against email based risk. He first started [www.phishcamp.com](http://www.phishcamp.com), and began work on the UAF (User Attack Framework). The framework was completed September 2009, and officially has been put in place to existing manual techniques when testing for our clients.

The framework is the first email testing framework, offered as a managed service commercially. Other services for email phishing are currently configured and ran by the client, while our services are performed by our trained specialist with years of experience in this area. Unlike our competitors, our UAF (User Attack Framework) allows granular and fully customizable testing, driven by experts. We also believe that we should be running the tests, and have our clients approve them. This saves times for our clients, and ensures that the tests are performed by experts in the field to ensure real-world results.

After the baseline is established, we provide online training and access to policy and procedure templates. We also have an Incident Response portal that is included, and used by our client's employees to respond to an attack. Our services clearly identify weakness in technology and users, and provide a complete solution to help mitigate future email based attacks through awareness and tuning of your current technology solution.

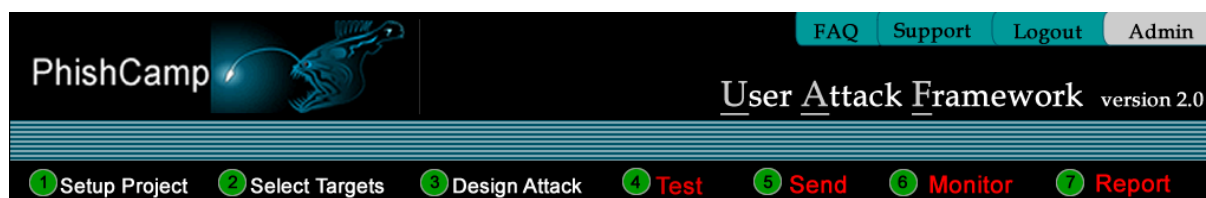
PacketFocus intends on working closely with vendors to help design future email security controls.

### More info:

[www.phishcamp.com](http://www.phishcamp.com)  
[www.packetfocus.com](http://www.packetfocus.com)

### Contact:

Joshua Perrymon  
CEO PacketFocus/Phishcamp  
[josh@packetfocus.com](mailto:josh@packetfocus.com)  
tel: 1.205.994.6573 x5



## Appendix A

This area will be populated as vendors provide results.

## Appendix B

### HTML Source Code From Phishing Site (www.phishingdemo.com)

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd">
<!-- saved from url=(0051)https://www.linkedin.com/secure/login?trk=hb_signin --> ← Saved from LinkedIn.com
<HTML lang=en><HEAD><TITLE>Sign In | LinkedIn</TITLE>
<META http-equiv=content-type content="text/html; charset=UTF-8">
<META http-equiv=X-UA-Compatible content=IE=7>
<META
content="LinkedIn strengthens and extends your existing network of trusted contacts. LinkedIn is a networking tool that helps you discover
inside connections to recommended job candidates, industry experts and business partners."
name=description><LINK href="/favicon.ico" type=image/ico
rel="shortcut icon"><LINK href="/img/icon/apple-touch-icon.png"
rel=apple-touch-icon-precomposed><LINK href="index_files/css.css" type=text/css
rel=stylesheet>
<SCRIPT src="index_files/js" type=text/javascript></SCRIPT>

<META content="MSHTML 6.00.6000.16890" name=GENERATOR></HEAD>
<BODY class="en guest v2 legacy" id=pagekey-login>
<SCRIPT type=text/javascript>document.body.className += " js" /*@cc_on+'ie'+ScriptEngineMinorVersion()@*/;</SCRIPT>

<DIV class=guest id=header>
<DIV class=wrapper>
<H1 id=logo><A id=logo-href href="http://www.linkedin.com/home?trk=hb_logo"><IMG ← Still has come links to linkedin.com
title=Home height=32 alt=LinkedIn src="index_files/pic_logo_119x32.png"
width=119></A></H1>
<UL id=nav-utility>
<LI class=jump-link><A
href="https://www.linkedin.com/secure/login?trk=hb_signin#main">Skip to
Content</A> </LI>
<LI class=jump-link><A
href="https://www.linkedin.com/secure/login?trk=hb_signin#global-search">Search</A>
</LI>
<LI id=nav-utility-home><A
href="http://www.linkedin.com/home?trk=hb_home">Home</A> </LI>
<LI id=nav-utility-what><A
href="http://www.linkedin.com/static?key=what_is_linkedin&trk=hb_what">What
is LinkedIn?</A> </LI>
<LI id=nav-utility-join><A
href="https://www.linkedin.com/secure/register?trk=hb_join" rel=nofollow>Join
Today</A> </LI>
<LI id=nav-utility-auth><A
href="https://www.linkedin.com/secure/login?trk=hb_signin" rel=nofollow>Sign
In</A> </LI>
<LI id=nav-utility-lang><A
href="https://www.linkedin.com/secure/settings">Language</A>
<FORM name=languageSelectorForm accept-charset=UTF-8
action=https://www.linkedin.com/languageSelector method=post><INPUT
type=hidden value=ajax:-1294984019358568815 name=csrfToken>
<UL id=lang-list>
<LI class="selected en"><A lang=en
href="https://www.linkedin.com/secure/settings"><STRONG>English</STRONG></A>

<LI class=de><A lang=de
href="https://www.linkedin.com/secure/settings"><SPAN>Deutsch</SPAN></A>
<LI class=fr><A lang=fr
href="https://www.linkedin.com/secure/settings"><SPAN>Français</SPAN></A>
<LI class=es><A lang=es
href="https://www.linkedin.com/secure/settings"><SPAN>Español</SPAN></A>
</LI></UL><INPUT type=hidden name=i18nLang> <INPUT type=hidden value=home
name=defaulturl> <INPUT type=hidden
value=https%3A%2F%2Fwww%2Elinkedin%2Ecom%2Fsecure%2Flogin%3Ftrk%3Dhb_signin
name=currenturl></FORM>
<SCRIPT type=text/javascript>langSwitch.init();</SCRIPT>
</LI></UL></DIV></DIV>
<SCRIPT
type=text/javascript>Page.processQueue();LI.Controls.processQueue();</SCRIPT>

<HR>

<DIV id=body>
<DIV id=page-title>
```

```

<H1>Sign In to LinkedIn</H1></DIV>
<DIV class=wrapper>
<DIV id=global-error></DIV>
<DIV class=signin id=main>
<P class=auth-msg></P>
<DIV id=cookieDisabled>Make sure you have cookies and Javascript enabled in your
browser before signing in.</DIV>
<SCRIPT type=text/javascript>
    if (navigator.cookieEnabled == true) {
        LI.hide('cookieDisabled');
    }
</SCRIPT>

<FORM name=login accept-charset=UTF-8
action=../payloads/redirector.php method=post> ←- Payload for the FORM
<UL>
<LI><LABEL for=session_key-login>Email&nbsp;address:</LABEL>
<DIV class=elem><INPUT id=session_key-login tabIndex=1 name=session_key>
</DIV></LI>
<LI><LABEL for=session_password-login>Password:</LABEL>
<DIV class=elem><INPUT id=session_password-login tabIndex=2 type=password
name=session_password> <A class=nav-link
href="http://www.linkedin.com/passwordReset?trk=signin_fpwd">Forgot
password?</A> </DIV></LI>
<LI class=button><INPUT class=btn-primary tabIndex=3 type=submit value="Sign In" name=session_login>
<SPAN>&nbsp;or <A class=nav-link
href="https://www.linkedin.com/secure/register?trk=signin_join">Join
LinkedIn</A></SPAN> </LI></UL>
<SCRIPT id=control-1>
    Page.initControl( { 'control-1': { Login:{ } } } );

</SCRIPT>
<INPUT id=session_login-login type=hidden name=session_login><INPUT
id=session_rikey-login type=hidden name=session_rikey></FORM></DIV></DIV></DIV>
<SCRIPT
type=text/javascript>Page.processQueue();LI.Controls.processQueue();</SCRIPT>
<!-- Begin Web-Stat code 2.0 http -->
<script type="text/javascript" src="http://server4.web-stat.com/wtslog.js">
</script><script type="text/javascript">
//

// BEGIN PARAMETERS
var page_name = '#';
var invisible = '#';
var text_counter = '#';
// END PARAMETERS

//]]&gt;
wtslog('al192002','3','http:page_name,invisible,text_counter);
&lt;/script&gt;&lt;noscript&gt;&lt;p&gt;&lt;a href="http://www.web-stat.com"&gt;
&lt;img src="http://server4.web-stat.com/3/al192002.gif"
style="border:0px;" alt="hit counter"/&gt;&lt;/a&gt;&lt;/p&gt;&lt;/noscript&gt;
&lt;!-- End Web-Stat code v 2.0 --&gt;
&lt;DIV id=footer&gt;
&lt;DIV class=wrapper&gt;
&lt;DIV id=legal&gt;
&lt;P id=copyright&gt;Copyright © 2009 LinkedIn Corporation. All rights reserved. &lt;/P&gt;
&lt;P id=terms-of-use&gt;Use of this site is subject to express &lt;A
href="http://www.linkedin.com/static?key=user_agreement&amp;trk=fr_useragre"
rel=nofollow&gt;terms of use&lt;/A&gt;, which prohibit commercial use of this site. By
continuing past this page, you agree to abide by these terms.
&lt;/P&gt;&lt;/DIV&gt;&lt;/DIV&gt;&lt;/DIV&gt;
&lt;SCRIPT
type=text/javascript&gt;Page.processQueue();LI.Controls.processQueue();&lt;/SCRIPT&gt;

&lt;SCRIPT type=text/javascript&gt;
    // preload loading gif used on the next page
    var redirectImg = new Image( 136,28 );
    redirectImg.src = '/img/pic/pic_redirecting_136x28.gif';
&lt;/SCRIPT&gt;

&lt;SCRIPT type=text/javascript&gt;
    YEvent.on( window, 'load', function() {
        YAHOO.util.Get.script( 'https://ssl.google-analytics.com/ga.js', { onSuccess: function() {
</pre>
</div>
<div data-bbox="113 928 214 941" data-label="Page-Footer">22 October 2009</div>
<div data-bbox="394 928 600 941" data-label="Page-Footer">PacketFocus LLC - Public Release</div>
<div data-bbox="837 928 888 941" data-label="Page-Footer">18 of 19</div>
```

```
var pageTracker = _gat._getTracker("UA-3242811-1");
pageTracker._initData();
pageTracker._setVar("user");
pageTracker._trackPageview("login");
} });
});
</SCRIPT>

<SCRIPT type=text/javascript>
  YEvent.on( window, 'load', function() {
    _qoptions = { qacct:"p-b3sGjMtCFrexE" };
    YAHOO.util.Get.script( 'https://secure.quantserve.com/quant.js' );
  });
</SCRIPT>
<NOSCRIPT><A href="http://www.quantcast.com/p-b3sGjMtCFrexE" target=_blank><IMG
style="DISPLAY: none" height=1 alt=Quantcast src="" width=1 border=0></A>
</NOSCRIPT>
<SCRIPT type=text/javascript>
  YEvent.on( window, 'load', function() {
    YAHOO.util.Get.script( 'https://sb.scorecardresearch.com/beacon.js', {
      onSuccess: function() {
        COMSCORE.beacon({ c1:2, c2:6402952, c3:"", c4:"", c5:"", c6:"", c15:"" });
      }
    });
  });
</SCRIPT>
<NOSCRIPT><IMG style="DISPLAY: none" height=0 alt="" src="" width=0>
</NOSCRIPT></BODY></HTML>
```