

JASIRC Notice Number: **JN-2011-24**

Publication Date: **June 27, 2011**

Revision Date: **N/A**

Topic: **Security Administration**

Title: **Weekly Security Summary**

## **Items this Week**

### **Articles**

- ITSO Security Trends Presentation Now Available
- Malware Protection for Macs
- Facial Recognition Software Automatically Enabled in Facebook

### **Reader's Questions**

Question: What is Cygwin?

### **Features**

- Security Operations Center Malware/Intrusion Detection Events
- Symantec Corner
- Patches and Updates
- Today's News

### **For Our Technical Readers**

Reverse Engineering Infected PDFs

## **Articles**

### **ITSO Security Trends Presentation Now Available**

The security briefing by ITSO staff at the May 2011 Technical Users Group (TUG) in Las Vegas is now available for viewing. This must-see hour-long presentation, "Trends from the IT Security Assessments and Security Tools and Service," talks about the findings based on security assessment visits to 30 courts and discusses security tools available to courts to help combat threats to the Judiciary networks and data.

The presentation is available at the following link:



<http://mediasuite.multicastmedia.com/player.php?p=b70p6i37>

Note: Because of the length of the video, it may be slow to load.

The presentation was held on day two of the conference. Information about the TUG conference including links to handouts and other presentation is available at:

<http://tug.circ9.dcn/>

## Malware Protection for Macs

Due to the recent spread of MacDefender fake antivirus; this article discusses malware protection for users with Macs. While such fake antivirus problems are reported frequently for Windows operating systems, they are a new trend for Mac computers.

Federal employees within the Judiciary can download Symantec Antivirus for Macs. Symantec Antivirus is part of the Symantec Endpoint Protection (SEP) zipped file available at the following sites:

[http://itso.res.gtwy.dcn/Symantec\\_Endpoint\\_Protection\\_11.0.6\\_MP3\\_Xplat\\_EN\\_DVD.zip](http://itso.res.gtwy.dcn/Symantec_Endpoint_Protection_11.0.6_MP3_Xplat_EN_DVD.zip)  
[http://itso.lsm.gtwy.dcn/Symantec\\_Endpoint\\_Protection\\_11.0.6\\_MP3\\_Xplat\\_EN\\_DVD.zip](http://itso.lsm.gtwy.dcn/Symantec_Endpoint_Protection_11.0.6_MP3_Xplat_EN_DVD.zip)

After the zip file has been downloaded, users click on the folder, “SEP\_MAC” to install this version of SEP.

MacDefender is a type of fake antivirus designed to attack Macs using OS X. The malware targets computers running Safari, Apple’s web browser. The user clicks on a link, usually from a poisoned search result, to download software stored in a zip file and agrees to install it. However, unknown to the user, it has been infected and malware gets installed. MacDefender then appears as pop-ups on the user’s screen claiming that the computer has been infected and the user needs to download, for a fee, an antivirus solution. Since there is a fee demanded, this type of program is also referred to as ransomware.

In response to this threat, in early June 2011, Apple modified xprotect.plist, which is part of Mac’s OS X Snow Leopard 10.6, to detect MacDefender and warn users who have accidentally downloaded the malware. Apple also modified xprotect.plist to check for signature updates automatically every 24 hours. Unfortunately, within eight hours the creators of MacDefender were able to work around Apple’s fix. The xprotect.plist also only scans files that have been downloaded from the Internet. If malware is downloaded through BitTorrent (or other torrenting software), through a shared network, or from a USB stick, xprotect.plist will not scan and warn the user about malware. IT security professionals recommend that Mac users install an antivirus program instead of relying completely on xprotect.plist.

One additional safety precaution that Mac users should implement is to prevent Safari from automatically opening downloaded files. To make this change, go into Safari’s preference

page and click on the “General” tab. At the bottom is a checkbox, “Open ‘safe’ files after downloading.” Make sure this checkbox is not checked.

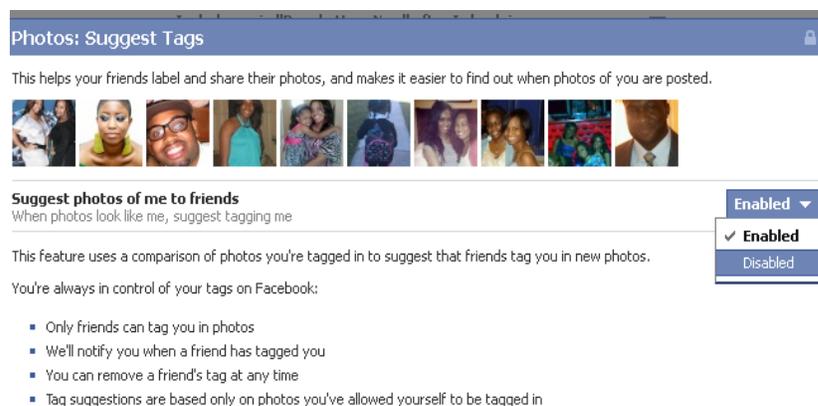
In addition to antivirus software, Mac users should also follow security best practices in being cautious when clicking on links and downloading software from reliable sources. *KM*

## Facial Recognition Software Automatically Enabled in Facebook

Facebook has recently enabled facial recognition software on its popular social networking site. When Facebook members upload an image, the software checks other images associated with their friends in its database to see whether any faces in the uploaded image match anything in its database. If a match is made, the software provides the member’s name as a suggested tag to the Facebook member uploading the image. Both the “search function for a match when uploading images” as well as “being listed as a potential match” are automatically enabled by Facebook.

While members cannot prevent the search when they upload images, they do not have to accept any suggested tags. Members, however, can get Facebook to exclude their names from searches so that their names will not appear as suggestions when friends upload an image. To do this:

1. Go to “Privacy Settings.”
2. Click “Customize settings.”
3. Scroll down to “Suggest photos of me to friends” and click the “Edit Settings” button. The following screen is displayed:



4. Click the box where it says “Enabled” and select “Disabled.”
5. Click “Okay” to accept the changes.

Users who wish to maintain a degree of privacy while using Facebook should consider disabling the “suggest tags” feature. *KM*

## Reader's Questions

### Question: What is Cygwin?

**Answer:** “Cygwin is a collection of tools that provide a Linux look and feel environment for a computer running Windows.<sup>1</sup>” Cygwin is a Unix system-call emulation library, named `cygwin1.dll` that acts like a Linux application programming interface (API) layer, which in turn, provides Linux API functionality to a Windows environment. Administrators may find Cygwin helpful when they need to use a Unix or Linux tool in a Windows environment.

Cygwin is installed by downloading and running the `setup.exe` file from <http://cygwin.com/setup.exe>. During the setup process, a user will be able to select:

- The Cygwin root directory (where Cygwin is installed)
- From where the associated Cygwin files should be downloaded from (mirror sites)
- Which optional Cygwin packages should be installed

When installation has completed, the Cygwin root directory will look very much like a typical GNU/Linux or Unix environment. Multiple subdirectories will be created including:

- `bin` (application and DLL storage)
- `etc` (configuration files)
- `home` (a personal directory for each Windows user)
- `lib` (static libraries)
- `tmp` (temporary files)
- `usr` (additional software)
- `var` (log files)

Note: Cygwin will not allow a user to run Linux Applications natively on Windows. The user will have to either recompile the program for Windows from the source, or run many of the assorted packages<sup>2</sup> from the shell environment.

Next week, the JASIRC team will provide a Cygwin installation tutorial as well as tutorial about Pasco, which works within the Cygwin environment. Pasco is a program that was developed to aid in the reconstruction of a user's Internet activity. *AM*

---

<sup>1</sup> Source:

<http://cygwin.com/>

Source:

<sup>2</sup> <http://cygwin.com/packages/>

## Security Operations Center Malware/Intrusion Detection Events

ITSO's Security Operations Center (SOC), working with the courts, addressed the following Internet-based attacks against the Judiciary this week:

- **Trojan/Malware Dropper:** The SOC team notified eight courts after observing hosts downloading a malicious PHP file from external website's located in Romania, Latvia, Germany, and Russia. The SOC team will follow up with the courts as needed.
- **FakeAV:** The SOC team notified two courts after observing hosts accessing a website hosted in Germany and Romania and downloading Fake Antivirus software. One court scanned the machine and removed Trojan.Gen and Trojan.fakav! The SOC team will follow up with the other court as needed.
- **SOC Mentoring Program:** This week, there was one participant in the SOC Mentoring Program that visited the AO.

## Symantec Corner

### Symantec Security Response: Signature Updates

Symantec provides signature updates on a regular basis as new threats emerge and existing threats evolve. Keeping Judiciary systems up to date with current signatures is a vital part of a proactive security posture. Symantec has added new virus definitions detected between 6/20/2011 and 6/26/2011 including the following:

- Trojan.Spamship is a Trojan horse that sends spam emails.
- Android.Jsmshider is a Trojan horse that opens a back door on Android devices.
- Backdoor.Specfix is a Trojan horse that opens a back door on the compromised computer.
- Android.Ggracker is a Trojan horse for Android devices that sends SMS messages to a premium-rate number.

For additional information, visit Symantec's website at:

<http://securityresponse.symantec.com>

## Patches and Updates

Below are reports on patches and updates for software commonly used within the Judiciary. Users are advised to download and install these patches to help maintain security. Note that these patches are available for download at the vendor's website, or through live updates; they are not distributed through email. Emails that claim to be from Microsoft or other vendors claiming that a security patch is attached are malware and should be deleted immediately.

### **Firefox 5 Release, Firefox 4 Reaches End of Life (EOL)**

On Tuesday, June 21<sup>st</sup>, 2011, Mozilla released the latest version of Firefox, Firefox 5 (FF5.) The update includes previous updates that were found in Firefox4 along with some browser enhancements. Some of these features include a redesigned user interface and moving the Do Not Track privacy features to all platforms, as well as placing its options menu under the "Privacy" menu. Firefox is now the first browser to implement the Do Not Track on multiple platforms. CSS Animations, along with other enhanced background features have also been added for Firefox 5.

Following the latest security update for Firefox 4, Mozilla has announced that the product has reached its EOL (end of life) and that updates will no longer be pushed to this version. Users will still be reminded of updates, but instead of downloading and updating to version 4, they will have to upgrade to FF5.

News Sources:

[http://www.washingtonpost.com/blogs/faster-forward/post/firefox-5-offers-small-improvements-do-not-track/2011/06/22/AGDf5lfH\\_blog.html](http://www.washingtonpost.com/blogs/faster-forward/post/firefox-5-offers-small-improvements-do-not-track/2011/06/22/AGDf5lfH_blog.html)

<http://www.ibtimes.com/articles/167537/20110622/mozilla-stops-security-support-for-firefox-4-firefox-5-firefox-3-6-google-chrome-eol-end-of-life-sec.htm>

## Today's News

### **WordPress.org Compromised**

On June 21<sup>st</sup>, 2011, WordPress.org released a statement that when several popular plug-ins were updated, they contained well-disguised backdoors planted by a malicious entity. Once WordPress found out about the intrusion, they rolled back the changes that were made to these plug-ins and pushed the updates to the plug-ins client side. WordPress has also shut down access to the plug-ins repository while the investigation continues. The investigation will include reviews of other plug-ins in the repository in a search for malicious updates to the content. WordPress has also Force-Reset all passwords on Wordpress.org. The plug-ins that have been rolled back due to the compromise are: AddThis, WPtouch, and W3 Total Cache.

Users with WordPress accounts who use these plug-ins should update them immediately.

News Source:

<http://wordpress.org/news/2011/06/passwords-reset/>

## **New Trojan Created to Steal Bitcoins**

A new Trojan, Infostealer.Coinbit, has been detected. Its primary goal is to target the digital currency, Bitcoin. The new malware is designed to steal victims' online wallets and email it back to the attackers. Bitcoins are a form of virtual currency created in 2009 that allows users to transfer “moneys” anonymously online without going through a bank. Some online merchants accept this form of currency and it can even be traded for actual dollars. It is suspected that the malware was being distributed via links sent through a Bitcoin forum chat application.

Bitcoin has gained attention recently because of its use for payment for illegal transactions. The hacker group LulzSec also announced their use of Bitcoins by receiving donations of more than \$7,200 worth of the currency. Because of its popularity and the amount of Bitcoins available for purchase, it is believed that similar code will find its way into other malware.

In order to avoid being a victim of malware of this kind, Bitcoin users should encrypt their digital wallets and use strong passwords to prevent attackers from using brute-force tactics to force their wallets open.

News Source:

<http://www.scmagazineus.com/new-trojan-aims-to-steal-bitcoin-virtual-currency/article/205585/>

## **Dropbox Left Login Door Open for 4 Hours**

Dropbox, the cloud-based file storage and synchronization service, has reported that on June 19<sup>th</sup> 2011, an erroneous code update allowed logins without authentication and allowed users to access files held by other users of the file synchronization service. The mistake went undetected for approximately four hours but was fixed within five minutes of discovery. Dropbox says less than one percent of users who had login activity during that time were affected. Those affected users will be informed of the activity that took place with their accounts. There have also been negative reports about Dropbox due to its encryption and access claims; originally they said that “no one” could see data stored in the system. They have since retracted that statement stating now that employees can access the files when legally required.

It is best to stay aware of any compromises that take place with services and applications. If patches and updates are made available, it is a best practice to apply those updates as soon as possible to avoid any major issues. Dropbox does not have an Agreement with the Judiciary to obligate them to protect U.S. Courts' data, therefore it is not a good practice to store work files using Dropbox.

New Sources:

<http://www.h-online.com/security/news/item/Dropbox-left-login-door-open-for-4-hours-1264195.html>

<http://www.net-security.org/secworld.php?id=11194>

## **Sega Hacked, 1.3 Million Accounts Compromised**

An attack on Sega Corporation and its database was reported and confirmed by the company once its Pass system was taken offline this week. The breach compromised 1.3 million users' email addresses, dates of birth, and encrypted passwords. No payment information was acquired however. The Pass system is still offline but all passwords to the compromised accounts have been reset. The hackers of Sega have not been identified.

Users with Sega Pass system accounts should look out for any phishing schemes that may have resulted from this security breach. Remember to always check the validity of any sender and notify the company of any cyber attacks.

News Source:

<http://www.net-security.org/secworld.php?id=11191>

## **Spam e-books Plague Amazon's Kindle Store**

Spammers have been scamming Amazon's e-book buyers out of their money. They are tricking users into purchasing their falsely advertised books by using an already published book, changing the title, author, and cover and reselling it. Spammers also are using a piece of software that packages public domain content that adds a cover and title and submits it for sale.

Because the process of checking the authenticity of a book is so fast, Amazon is not able to weed out the fake e-books from legitimate submissions. The approval process is only 48-hours and does not require any form of payment to sell on the Amazon market. It has been suggested that Amazon charge authors to publish in order to cut back on potential profits for spammers.

Before buying an e-book, users should pay attention to the feedback of that publisher and use encrypted site access when making an online purchase. If users have purchased an e-book that is spam, they should report the author and have them blocked from Amazon's web site.

News Source:

<http://www.net-security.org/secworld.php?id=11192>

## **New Zeus Emails Cloaked as Federal Reserve, IRS Messages**

A new Zeus Trojan is out to attack small to mid-size organizations by piggy-backing on the trusted names of the Federal Reserve and the Internal Revenue Service. Victims will receive an email allegedly from these trusted entities asking for some type of action. The email entices recipients to open a link and install an executable file, which is the Zeus Trojan. The purpose of this Trojan is to gain access to important financial information. The individuals in charge of the organization's finances are targeted for this reason. When the individual clicks on the link, the data-stealing Trojan will capture the corporate banking credentials. For example, this week, an email informed recipient that their federal tax payment was canceled by their bank and to encouraged them to click the link enclosed.

There is not yet a fix for this Trojan because it continues to be repackaged and sent out to thousands of users. To protect against this malware, users should check the source of all links and contact their tax preparers directly if there seems to be something strange about the email received. Remember, banks and financial institutions will direct users to their secure sites before needing to enter any personally identifiable information. Users should also use caution in clicking on links in emails.

News Source:

<http://www.scmagazineus.com/new-zeus-emails-cloaked-as-fed-irs-messages/article/205920/>

## **For Our Technical Readers**

### **Reverse Engineering Infected PDFs**

Adobe PDF files are a popular method for sending information to end users since Adobe Readers are available for almost every operating system, including some mobile devices. The popularity of PDFs as well as vulnerabilities in the software, however, has made them one of the primary delivery systems for exploits and general malware. This article describes how PDFs can be infected, as well as a Linux tool that administrators can use to reverse engineer an infected PDF to understand the malicious code that has been embedded.

PDF, or portable document format, is not a programming language, it is a page description language. PDF specifies how the content of a page is rendered. The file is made up of a header, objects, a cross-reference table (to locate objects), and a trailer.

How can a PDF file be used to deliver an executable file? This can be done in many ways. The most prevalent way is to embed an executable file within the PDF. The executable file uses JavaScript and shellcode to run the malicious code when a user opens the PDF, and it places a file on the user's hard drive. Another common method is to use JavaScript to launch shellcode that will reach out to an external host, download the malware, and execute it on the

user's host. As malware writers became more experienced with writing PDF exploits, the amount of obfuscating and exploit techniques began to grow.

REMnux is a Linux-based tool available for analyzing suspicious PDF files. The tool may be downloaded as a VM or ISO image from: <http://zeltser.com/remnux/>. REMnux comes packed with scripts and features that include Jsunpack-n and other tools to analyze suspicious PDF files, along with other malware-centric features.

If using the pre-made VM image, administrators need to install VMTools as well. To do so:

1. Click on "VM" in the top menu of the VMware Server console and select "Install VMware Tools."
2. Click "Install" on the presented prompt.
3. Copy the VMware Tools from the mounted ISO to a temporary folder:  
**cp /media/cdrom/VMwareTools-[version].tar.gz /tmp/**
4. Switch to the tmp folder:  
**cd /tmp**
5. Unpack the file:  
**tar xvfz VMwareTools-[version].tar.gz**
6. Change directories to where the unpacked file has been stored:  
**cd /vmware-tools[distrib]**
7. Run the VMware Tools setup script:  
**sudo ./vmware-install.pl**
8. A string of questions will be asked; accept the default answer by hitting return to each question.
9. Running the following will bring up the VMware Tools properties menu:  
**vm-ware-toolbox &**

Note: Administrators that are performing malware investigations should take caution to prevent their computer from becoming infected by the malware they are researching.
---

## Scenario

A user forwards an email with an attached PDF (newbenefits.pdf) to the court's IT security administrator. The email is from an external email address and claims that the PDF contains important information about changes in the Federal benefits package. The administrator believes that the email is part of phishing attack and, after warning the court, wants to analyze the infected PDF to develop any countermeasures in case other users open the attachment.

To analyze the “newbenefits.pdf” file:

1. The administrator enters a Linux console and changes directories to the ~/jsunpack-n directory. This is done by entering: **cd /home/remnux/jsunpack-n/** or **cd ~/jsunpack-n/**.
2. The administrator enters the command **make clean** to clean up any previous PDF malware investigations.
3. The administrator launches “pdf.py” script. The “pdf.py” script is written in Python and will locate script and action-related strings in whatever PDF file is being analyzed. To run “pdf.py”, the administrator enters the following:

File Location

File Name

```
./pdf.py ~/jsunpack-n/samples/newbenefits.pdf
```

This script will produce an output file named “[original file-name].out.” In the case of the above scenario, the output file will be called newbenefits.pdf.out.

4. The administrator opens the output file with an editor, such as vi by entering the command: **vi ~/jsunpack-n/samples/newbenefits.pdf.out**. To exit vi, the administrator types the following command: “ESC (escape key)”, “:”, “q!”.

```
info.creationdate = String('D\x3a20090506204524\x2b08\x5cx2700\x5cx27\x29'); this
s.creationdate = info.creationdate;
app.doc.creationdate = String('D\x3a20090506204524\x2b08\x5cx2700\x5cx27\x29');
info.moddate = String('D\x3a20090516213035\x2b08\x5cx2700\x5cx27\x29'); this.mod
date = info.moddate;
app.doc.moddate = String('D\x3a20090516213035\x2b08\x5cx2700\x5cx27\x29');
info.producer = String('DocuCom\x20PDF\x20Core\x20Library\x29'); this.producer =
info.producer;
app.doc.producer = String('DocuCom\x20PDF\x20Core\x20Library\x29');
info.author = String('Zeon\x20Technical\x20Publications\x29'); this.author = inf
o.author;
app.doc.author = String('Zeon\x20Technical\x20Publications\x29');
info.moddate = String('323030392f30352f31362032313a3330'); this.moddate = info.m
oddate;
app.doc.moddate = String('323030392f30352f31362032313a3330');
c = []; zzzpages.push(c); this.numPages = zzzpages.length;

//jsunpack End PDF headers
ÿ^M
function spary() {^M
@
```

5. The top of file contains the PDF headers. Next, the administrator sees the beginning of a function named “spary.”

Note: The following two screen captures were cropped for brevity, however, the code repeated for a number of lines.



“\x67\x65\x74\x49\x63\x66\x6e” when decoded = “getIcon”

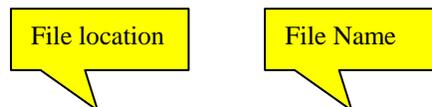
“\x5f\x4e\x2e\x62\x75\x63\x64\x6c\x65” when decoded = “\_N.bundle”

9. The whole line combined tells the administrator: “Collab.getIcon\_N.bundle”. The administrator researches and finds the code in Common Vulnerabilities and Exposures ID as CVE-2009-0927 (“Stack-based buffer overflow in Adobe Reader and Adobe Acrobat 9 before 9.1, 8 before 8.1.3 , and 7 before 7.1.1 allows remote attackers to execute arbitrary code via a crafted argument to the getIcon method of a Collab object.”) The administrator has now discovered what vulnerability this PDF is attempting to exploit, and that it is a buffer overflow attempt.
10. The administrator, to confirm that hosts on the LAN are not vulnerable to CVE-2009-0927, launches a FoundStone scan<sup>3</sup> to search for this weakness. This particular vulnerability was patched on March 18, 2009 by Adobe.<sup>4</sup>

Now it is time for the administrator to discover what all of this code is attempting to do aside from “Heap spraying” the memory. Heap spraying works by allocating multiple objects containing the attacker's exploit code in the program's heap, the area of memory used for dynamic memory allocation. Heap spraying circumvents this challenge by allocating, or “spraying” multiple copies of exploit code to increase the odds of finding a copy in the heap. The attacker can allocate hundreds of thousands of copies of exploit code into the heap. All that is needed is for one random program jump to land on one copy of such code, and a successful attack begins.<sup>5</sup>

To discover more about the malicious code:

1. The administrator runs a script named “jsunpackn.py”. jsunpackn.py is a JavaScript unpacker which will shed more light upon what the JavaScript and shellcode is attempting to do. To run the script, the administrator enters:



**./jsunpack.py ~/jsunpack-n/samples/newbenefits.pdf**

Note: This script may take a little while to run depending on the amount of code nested in the document. If the script can identify the exploit being used, the CVE will be identified here along with some other interesting information:

---

<sup>3</sup> Source:

[http://jnet.ao.dcn/Information\\_Technology/Computer\\_Security/Alerts/JASIRC\\_Notices/JASIRC\\_Notices\\_2011/Alert\\_04\\_04\\_11.html#article2](http://jnet.ao.dcn/Information_Technology/Computer_Security/Alerts/JASIRC_Notices/JASIRC_Notices_2011/Alert_04_04_11.html#article2)

<sup>4</sup> Source:

<http://www.adobe.com/support/security/bulletins/apsb09-04.html>

<sup>5</sup> Source

<http://www.darkreading.com/security/vulnerabilities/221901428/index.html>

```

remnux@remnux:~/jsunpack-n$ ./jsunpackn.py ~/jsunpack-n/samples/pdf.file.out
[malicious:10] /home/remnux/jsunpack-n/samples/pdf.file.out
  suspicious: Warning detected //warning CVE-NO-MATCH Shellcode NOP len 99
99 //warning CVE-NO-MATCH Shellcode NOP len 261283 //warning CVE-NO-MATCH Shellc
ode NOP len 847 //warning CVE-NO-MATCH Shellcode Engine Length 129358 //warning
CVE-NO-MATCH Shellcode NOP len 121 //warning CVE-NO-MATCH Shellcode NOP len 1023
  suspicious: shellcode of length 1451/847
  malicious: XOR key [shellcode]: 33
  malicious: shellcode [xor] URL=b35.info/w/who.exe
  file: decoding_92253c630dcc31a81f81a8234429a9a9c1cd716b: 5037 bytes
  file: shellcode_9e91c6f7ac43d4b404c9793f64e7617a2f257cba: 1451 bytes
  file: original_0c2b24bcbd8417022c0c3e2aaba0fac462b9110c: 8228 bytes
[not analyzed] (shellcode) b35.info/w/who.exe

```

2. The administrator sees that the script could not identify the CVE, but did list the file as being malicious with a grade of 10/10. The output also states that the amount of shellcode in the document is suspicious as well as the shellcode being XORED<sup>6</sup>.
3. Halfway down we see the output of the shellcode XOR. It is a URL leading to a malicious executable. After performing the buffer overflow, the shellcode is launched (from one of the memory addresses that were Heap sprayed) and attempts to access a file called “who.exe.” The administrator should then analyze the the “who.exe” file in an effort to determine its maliciousness. In a previous JASIRC Notice, we discussed online tools available to analyze executable files to determine whether they are safe<sup>7</sup>.

This article showed one of many ways to analyze a PDF document; there are other tools available including: Malzilla, Didier Stevens’ PDF Tools, and more. NOTE: Didier Stevens’ PDF Tools now come bundled with BackTrack 5 and are also available for download to Windows systems. *AM*

Note: This article is strictly informational in nature. The presence of a commercial product in the article above does not imply a recommendation or endorsement by the AO, nor does it imply that the mentioned product or service is the best available for its purpose.

<sup>6</sup> Source

[http://www.pcmag.com/encyclopedia\\_term/0,2542,t=XOR&i=55074,00.asp](http://www.pcmag.com/encyclopedia_term/0,2542,t=XOR&i=55074,00.asp)

<sup>7</sup> Source:

[http://jnet.ao.dcn/Information\\_Technology/Computer\\_Security/Alerts/JASIRC\\_Notices/JASIRC\\_Notices\\_2010/Alert\\_11\\_08\\_10.html#bullet2](http://jnet.ao.dcn/Information_Technology/Computer_Security/Alerts/JASIRC_Notices/JASIRC_Notices_2010/Alert_11_08_10.html#bullet2)

## Vulnerability Notification Services

### **Summary of Significant National Gateway Security Events**

The AO's Intrusion Detection team publishes reports of viruses stopped, firewall issues, intrusions attempted and other interesting external threats to the DCN. Weekly reports can be found on the RSS feeds at <http://soc.ao.dcn>.

### **Archives of JASIRC Notices**

This JASIRC Notice will be added to the JASIRC Security Alerts and News Page on the J-Net at the URL address [http://jnet.ao.dcn/Information\\_Technology/Computer\\_Security/Alerts.html](http://jnet.ao.dcn/Information_Technology/Computer_Security/Alerts.html)

### **Contacting the Judiciary Automated Systems Incident Response Capability**

For this JASIRC Notice, send questions and comments by internal electronic mail to SOC or to the Internet address of [SOC@ao.uscourts.gov](mailto:SOC@ao.uscourts.gov). Please continue to contact the Security Operations Center at (202) 502-4370 to report security incidents.