INTERNET CRIME COMPLAINT CENTER'S (IC3) SCAM ALERTS
AUGUST 08, 2012

This report, which is based upon information from law enforcement and complaints submitted to the IC3, details recent cyber crime trends, new twists to previously-existing cyber scams.

FAKE POLITICAL SURVEY

The IC3 has been notified of a scam involving telephone calls conducting a multiple-choice "political survey." Following the survey, the recipients are told they won a free cruise to the Bahamas. After providing a website address for legitimacy, the caller requests the "winner's" email address for notification purposes and credit card information to cover port fees. The website has very limited information, but does contain a few photos, testimonials, and "Caribbean Line" banner, in an attempt to convince visitors it is legitimate.

ONLINE PHONEBOOK

The IC3 has received several complaints regarding a phonebook website. Complainants reported that anyone could post other individuals' information. Some reported being verbally bullied, had uncensored comments, or false accusations posted about them. Personal information that could be listed on the website included: full name, unlisted cell phone numbers, email addresses, direct links to a person's private Facebook account, and any other information or photos someone wants to add. The website also allows users to anonymously call anyone listed on the site directly from the web, as well as track them with GPS.

FREE CREDIT SERVICE WEBSITE

The IC3 has received over 2,000 complaints regarding a particular website that is claiming to offer "free" credit services such as credit scores and credit monitoring. Customers reported being charged a monthly service fee. However, the terms of the agreement advised that the "free" report only lasts for a limited time. At the end of the free term, the website used the customer's supplied financial information to charge a monthly membership service ranging from $19.95 to $29.95.

The terms and agreement from the website states the following:

"For Subscription Services which include a free-trial period, if you do not cancel your free trial within the free trial period, you will be charged at the monthly rate in effect at that time for the Subscription Services for which you enrolled. Your debit or credit card (including, if applicable, as automatically updated by your card provider following expiration or change in account number) will continue to be charged each month at the applicable monthly rate unless and until you cancel the Subscription Services."

The website, according to the Better Business Bureau (BBB), has been given an F rating by the BBB for the following reasons:

- 1037 complaints filed against the business.
- 8 complaints filed against the business that were not resolved.
- 17 serious complaints filed against business.
- Advertising issue(s) found by the BBB.

CITADEL MALWARE DELIVERS REVETON RANSOMWARE IN ATTEMPTS TO EXTORT MONEY

On May 30, 2012, the IC3 released the following PSA warning consumers about a new Citadel malware platform used to deliver ransomware, named Reveton:

The IC3 has been made aware of a new Citadel malware platform used to deliver ransomware, named Reveton. The ransomware lures the victim to a drive-by download website, at which time the ransomware is installed on the user's computer. Once installed, the computer freezes and a screen is displayed warning the user they have violated United States Federal Law. The message further declares the user's IP address was identified by the Computer Crime & Intellectual Property Section as visiting child pornography and other illegal content.

To unlock their computer the user is instructed to pay a $100 fine to the US Department of Justice, using prepaid money card services. The geographic location of the user's IP address determines what payment services are offered. In addition to the ransomware, the Citadel malware continues to operate on the compromised computer and can be used to commit online banking and credit card fraud. Below is a screenshot of the warning screen.

This is an attempt to extort money with the additional possibility of the victim's computer being used to participate in online bank fraud. If you have received this or something similar do not follow payment instructions.

It is suggested that you:

- File a complaint at www.IC3.gov.

The IC3 continues to see variations of the scheme and a rapidly growing number of complaints. The PSA is available at https://www.ic3.gov/media/2012/120530.aspx .

MALWARESURVIVAL.NET RELEASED THE FOLLOWING ARTICLE ON MAY 24, 2012:

Spoofed Microsoft Update Includes Malware

Our team reports of a Spoofed Microsoft Email that includes a Critical Patch. The Spam includes links to sites in Argentina that include the Fake Anti-virus Attacks!

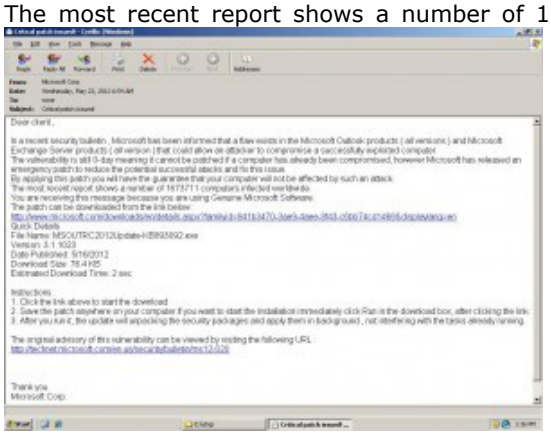
THE CYBER CRIMINALS WERE EVEN KIND ENOUGH TO INCLUDE INSTRUCTIONS ON DOWNLOADING THE MALWARE!

————————————<**Spam Sample**>————————————
From: "Microsoft Corp."<windowsupdate@microsoft.com>
Subject: Critical patch issued!
TO:<axxdaj@thgus.com>

Dear Client

- In a recent security bulletin, Microsoft has been informed that a flaw exists in the Microsoft Outlook products (all versions) and Microsoft Exchange Server products (all versions) that could allow an attacker to compromise a successfully exploited computer.
- The vulnerability is still 0-day meaning it cannot be patched if a computer has already been compromised, however Microsoft has released an emergency patch to reduce the potential successful attacks and fix this issue.
- By applying this patch you will have the guarantee that your computer will not be affected by such an attack.

- The most recent report shows a number of 1673711 computers infected worldwide.



EMBEDDED LINKS:

- href="hxxp://smatarosario.com.ar//administracion/includes/mail/MSOUTRC2012Update-KB893092.exe"
- The patch can be downloaded from the link below hxxp://yostarquitectura.com//imagenes/microsoft.html

————————————<End Sample>————————————

MALWARE PAYLOAD IDENTIFIED AS RANSOMWARE /FAKE AV:

- SHA256: 05ed7b9f30fb46c52a1913bf6b50144edd1d01cab3a18509b691d0347c891baf
- File name: MSOUTRC2012Update-KB893092.exe

MALWARE FOUND:

- BackDoor.Andromeda.22
- Trojan-Ransom.Win32.Birele.nml
- TR/Rogue.kdv.630542.1

MALWARE SITE1:

- hxxp://smatarosario.com.ar//administracion/includes/mail/MSOUTRC2012Update-B893092.exe
- IP:201.212.135.13
- Origin: Argentina

MALWARE SITE2:

- hxxp://yostarquitectura.com//imagenes/microsoft.html
- IP: 200.110.135.136
- Origin: Argentina

ADDITIONAL MALWARE FOUND:

- JS:Redirector-NH [Trj]
- PUA.Script.Packed-2
- EXP/JS.Blackhole.E=

THE US-CERT RELEASED THE FOLLOWING REVISED ALERT ON JUNE 25, 2012 :

VULNERABILITY NOTE VU#649219

SYSRET 64-BIT OPERATING SYSTEM PRIVILEGE ESCALATION VULNERABILITY ON INTEL CPU HARDWARE

Some 64-bit operating systems and virtualization software running on Intel CPU hardware are vulnerable to a local privilege escalation attack. The vulnerability may be exploited for local privilege escalation or a guest-to-host virtual machine escape.

Intel claims that this vulnerability is a software implementation issue, as their processors are functioning as per their documented specifications. However, software that fails to take the Intel-specific SYSRET behavior into account may be vulnerable.

DESCRIPTION

A ring3 attacker may be able to specifically craft a stack frame to be executed by ring0 (kernel) after a general protection exception (#GP). The fault will be handled before the stack switch, which means the exception handler will be run at ring0 with an attacker's chosen RSP causing a privilege escalation.

DETAILS FROM XEN

CVE-2012-0217 / XSA-7 - 64-bit PV guest privilege escalation vulnerability

A vulnerability which can allow a 64-bit PV guest kernel running on a 64-bit hypervisor to escalate privileges to that of the host by arranging for a system call to return via sysret to a non-canonical RIP. Intel CPUs deliver the resulting exception in an undesirable processor state.

DETAILS FROM FREEBSD

FreeBSD-SA-12:04.sysret: Privilege escalation when returning from kernel

FreeBSD/amd64 runs on CPUs from different vendors. Due to varying behaviour of CPUs in 64 bit mode a sanity check of the kernel may be insufficient when returning from a system call. Successful exploitation of the problem can lead to local kernel privilege escalation, kernel data corruption and/or crash.

DETAILS FROM MICROSOFT

User Mode Scheduler Memory Corruption Vulnerability - MS12-042 - Important

An elevation of privilege vulnerability exists in the way that the Windows User Mode Scheduler handles system requests. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

Mitigating Factors for User Mode Scheduler Memory Corruption Vulnerability

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state that could reduce the severity of exploitation of vulnerability. The following mitigating factors may be helpful in your situation:

- *An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users.*
- *This vulnerability only affects Intel x64-based versions of Windows 7 and Windows Server 2008 R2.*
- *Systems with AMD or ARM-based CPUs are not affected by this vulnerability.*

DETAILS FROM RED HAT

RHSA-2012:0720-1 & RHSA-2012:0721-1: It was found that the Xen hypervisor implementation as shipped with Red Hat Enterprise Linux 5 did not properly restrict the syscall return addresses in the sysret return path to canonical addresses. An unprivileged user in a 64-bit para-virtualized guest, that is running on a 64-bit host that has an Intel CPU, could use this flaw to crash the host or, potentially, escalate their privileges, allowing them to execute arbitrary code at the hypervisor level. (CVE-2012-0217, Important)

Details from some affected vendors were not available at the time of publication.

Vendor	Status	Date Notified	Date Updated
Citrix	Affected	-	18 Jun 2012
FreeBSD Project	Affected	01 May 2012	12 Jun 2012
Intel Corporation	Affected	01 May 2012	13 Jun 2012
Joyent	Affected	-	14 Jun 2012

Microsoft Corporation	Affected	01 May 2012	18 Jun 2012
NetBSD	Affected	01 May 2012	08 Jun 2012
Oracle Corporation	Affected	01 May 2012	08 Jun 2012
Red Hat, Inc.	Affected	01 May 2012	12 Jun 2012
SUSE Linux	Affected	02 May 2012	12 Jun 2012
Xen	Affected	02 May 2012	12 Jun 2012
AMD	Not Affected	-	13 Jun 2012
Apple Inc.	Not Affected	01 May 2012	08 Jun 2012
OpenBSD	Not Affected	-	25 Jun 2012
VMware	Not Affected	01 May 2012	08 Jun 2012
Debian GNU/Linux	Unknown	02 May 2012	02 May 2012

Impact - A local authenticated attacker may exploit this vulnerability for operating system privilege escalation or for a guest-to-host virtual machine escape.

Solution - Apply an Update

TRENDMICRO POSTED THE FOLLOWING ARTICLE ON JUNE 4, 2012:

Malicious PowerPoint File Contains Exploit, Drops Backdoor

We discovered a malicious ***MS PowerPoint*** document that arrives via an attached file attached to specific email messages. The file contains an embedded Flash file, which exploits a software bug found in specific versions of ***Flash Player*** (CVE-2011-0611) to drop a backdoor onto users' systems.

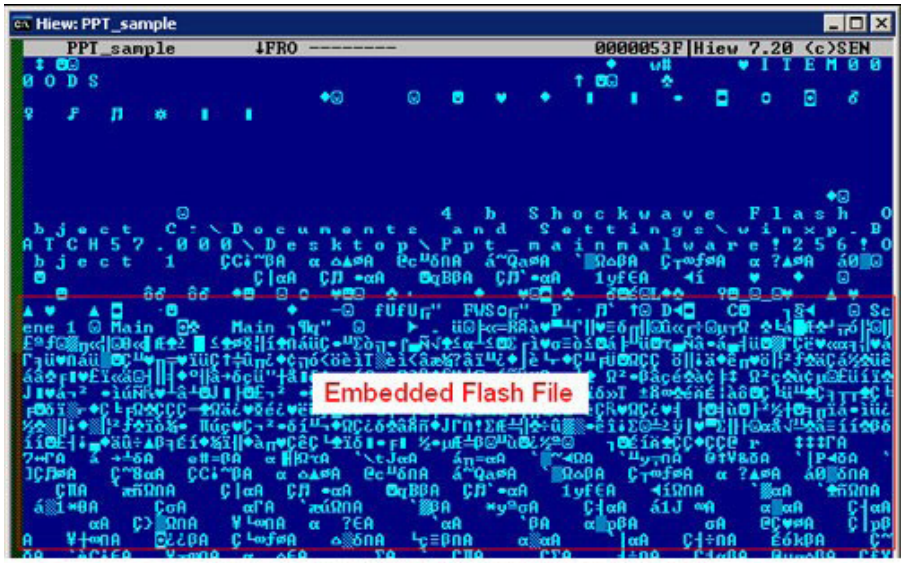


Figure 1. Embedded Flash file in TROJ_PPDROP.EVL

Users who open the malicious .PPT file triggers the shellcode within the Flash file that exploits CVE-2011-0611, and then drops "Winword.tmp" in the Temp folder. Simultaneously, it also drops a non-malicious ***PowerPoint*** presentation file "Powerpoint.pps", tricking users into thinking that the malicious file is just your average presentation file. Based on our analysis, "Winword.tmp" is a backdoor that connects to remote sites to communicate with a possible malicious user. It is also capable of downloading and executing other malware leaving infected systems susceptible to other, more menacing threats such as data stealing malware.

Trend Micro detects the malicious PowerPoint file as TROJ_PPDROP.EVL and the dropped backdoor file as BKDR_SIMBOT.EVL. Reports, as well as our own analysis, confirmed that this kind of malware has been used for targeted attacks in the past.

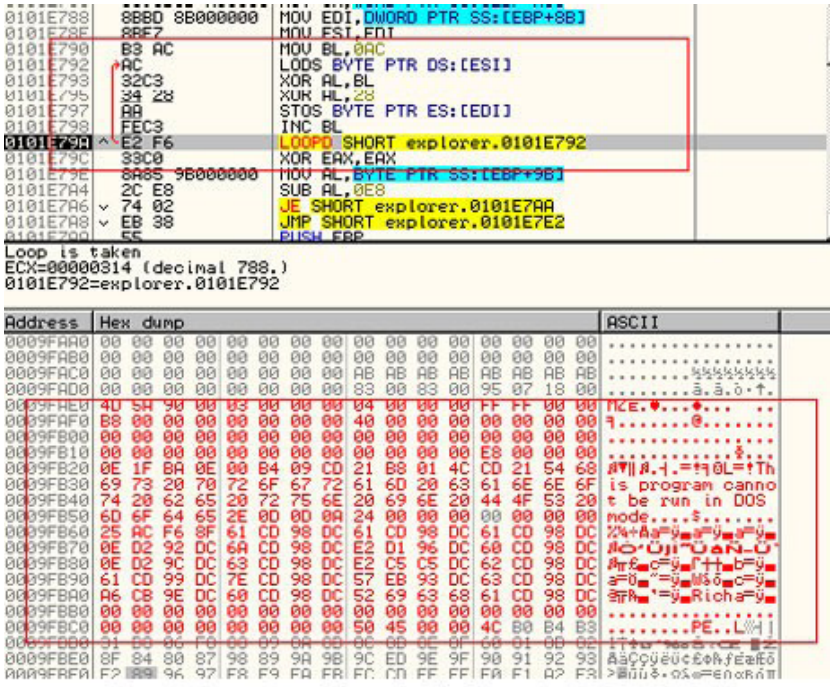


Figure 2. Decryption of the embedded binary in TROJ_PPDROP.EVL

Recent threats are no longer limited to malicious files disguised as ordinary binaries (such as .EXE file) attached to emails. These specially crafted files can be embedded in commonly used files such as PDF, DOC, PPT or XLS files. In this particular scenario, users are unaware of the attack since TROJ_PPDROP.EVL also displays a non-malicious ***PowerPoint*** file to serve as a decoy.

RELIABLE VULNERABILITIES: EFFECTIVE INFECTION GATEWAYS

This case also shows that cybercriminals are continuously taking advantage of previously reported vulnerabilities in popular software such as MS Office applications, Flash etc. In a previous blog entry, we uncovered that old and reported software bugs such as CVE-2010-3333 and CVE-2012-0158 are still being exploited by attackers. This finding highlights two things. First, exploits created for reliable vulnerabilities remain effective cybercriminal tools. Second, most users do not regularly update their systems' with the latest security patch, which explains why attackers are continuously exploiting these bugs.

For more information regarding online scams visit our Press Room page for the most current Public Service Announcements. https://www.ic3.gov/media/default.aspx