Zero-Day Threats, Vulnerabilities, and Remediation

1. **Zero-Day Exploit – The CVE-2013-0422 and the related Trojan JAVA/CVE-2013-0422.C virus**

Description:

First described in the US-CERT Alert TA13-010A - Oracle Java 7 Security Manager Bypass Vulnerability, and another vulnerability affecting Java running in web browsers. These vulnerabilities are not applicable to Java running on servers, standalone Java desktop applications or embedded Java applications. They also do not affect Oracle server-based software.

CVE-2013-0422, which was identified as early as January 2, 2013, was a Java 7 vulnerability that allows attacks to bypass Java security checks and execute code on a target machine. Though it was designed specifically for MS Windows, the vulnerability also left other operating system platforms that run Java open to attack.

Attacks exploiting this flaw downloaded ransomware known as "Tobfy." This ransomware locked users out of their computer, displaying a full-screen message, purportedly from the FBI, accusing the user of a crime and demanding a payment to unlock the machine. "Tobfy" also disabled Windows Safe Mode and automatically terminated processes such as taskmgr.exe, msconfig.exe, regedit.exe, and cmd.exe to thwart users and technical personnel from trying to find or disable the malware.

Related Issues: Trojan JAVA/CVE-2013-0422.C virus Method of Transmission or Infection:

The Trojan JAVA/CVE-2013-0422.C virus is spread via web browsers that have Internet connections and exploits the CVE-2013-0422 vulnerability. The Trojan JAVA/CVE-2013-0422.C is one that is very commonly found, and spread through image files, more commonly through pornographic images that are shared or downloaded from massive file sharing porn sites. Once these images are clicked it automatically downloads the virus to the computer and begins to do its damage.

The JAVA/CVE-2013-0422.C virus is also known to be found throughout file download sites and also from attachments in spam email. Hackers love to target the file download sites since they know many people frequent these sites and look for free cracked versions of software rather than paying for them. This is because many times unsuspecting users will often click on anything that pops up on these sites in hopes of downloading a free version of the software they are seeking. The hackers know this and do a great job at making the user click to activate the virus in an unsuspecting manner.

The spam email attachments work based just on sheer numbers. They send

these emails to hundreds of millions of user e-mail accounts and there are always going to be some people that open the e-mail and then click to open the attachment.

Prevention of CVE-2013-0422.C virus infection:

Prevention of CVE-2013-0422.C virus infection includes all of the following:

- **Applying the updates provided by the Security Alert at http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html.**
- **A change to the default Java Security Level setting from "Medium" to "High". With the "High" setting, the user is always prompted before any unsigned Java applet or Java Web Start application is run.**
- **Avoidance.**
- **User education.**

Resolution or Remediation:

Since antivirus programs have failed to remove CVE-2013-0422.C virus, manual removal is required as it is a guaranteed complete removal.

Oracle strongly recommends that customers apply the updates provided by the Security Alert at http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html as soon as possible.

A change to the default Java Security Level setting from "Medium" to "High". With the "High" setting, the user is always prompted before any unsigned Java applet or Java Web Start application is run.

2. **Post-Infection Remediation**

- **When an infection of CVE-2013-0422.C virus infection is identified, manual removal is required as it a guaranteed complete removal.**
- **Apply the Oracle Java update that is required to fix the Java installation vulnerability.**
- **Change to the default Java Security Level setting from "Medium" to "High". With the "High" setting, the user is always prompted before any unsigned Java applet or Java Web Start application is run.**
- **Determine if further complications resulted from the download of the "Tobfy" program, such as user payment under the terms described in the**

Ransomware. Those situations should be remediated also, as discreetly as possible, including having the user contact their credit card company to invalidate the transaction(s).

- **Activate your Incident Response Plan if you have one and notify your management chain, if you have no Incident Response Plan, notify your management chain.**
- **Attempt to contact expert resources such as US CERT, the CVE Database, and FireEye to determine the nature of the Zero-Day Exploit.**
- **Create a "War Room" and notify affected stakeholders, and keep them updated on a regular basis.**
- **Determine as much as possible, the infection vectors, and the extent of the number of infections to understand how widespread the problem is.**
- **Work with the Network Manager and Administrators to quarantine infected areas and network segments.**
- **Keep a real-time timeline log of all activities from initial identification to final remediation.**
- **After the final remediation, write a final report of the remediation that includes impacts in terms of potential damages, data breaches, reputational damages, lessons learned, root cause(s), recommendation(s) to prevent or minimize the damage from future attacks, etc.**

3. General Proactive Prevention or Remediation for Zero-Day Exploits

- **Educate your users and all other Stakeholders about the dangers of malware, Advanced Persistent Threats, and Zero-Day Exploits, and ensure that they always engage in safe computing practices (i.e. not clicking on attachments, messages, dialog boxes, or links from unknown parties, not downloading or using unauthorized software, etc.).**
- **Segment your Networks and Keep your network documentation updated.**
- **Limit network and IT resource privileges based on least privilege and the need to know.**
- **Use application whitelisting.**
- **Have a current Incident Response Plan in place.**
- **Know your environment and if possible, have a current Configuration Management Data Base (CMDB) in place.**
- **Deploy a security platform environment that can identify known and unknown threats.**

- **Keep all systems patched with the most current patch updates and keep documentation about the patch level of each system.**
- **Use operating systems that support Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP), even though this is not 100% foolproof these days.**
- **Where it is possible and not restricted by policy or regulation, participate in security-related forums and professional organizations (i.e. ISACA, (ISC)2, FBI INFRAGARD, etc.) that promote best practices in IT security and facilitate sharing advanced threat knowledge and experience, sharing, lessons learned, and collaboration in remediation.**