Telos Corporation Ensures the Security Posture of Security Solutions from SCIT Labs

Overview

Founded in 2007, SCIT Labs offers next-generation server security products that are threat-independent and mission-resilient. SCIT's Moving Target Defense (MTD) technology continuously changes the attack surface, making it difficult for intruders to get in or have the time to continue and complete the attack. Acting as a "digital vaccine," their solutions restore servers to pristine uncontaminated state in minutes, thus increasing system availability and maintaining the reliability and reputation of the enterprise.

Because SCIT Labs develops solutions that provide information security, it's essential for them to have an independent security firm thoroughly test their solutions and development environment in order to discover vulnerabilities and make recommendations for remediating them. Thus SCIT Labs approached Telos Corporation's Computer Network Operations (CNO) Team to conduct an evaluation of their test environment and technology. The test was conducted using a Java web application.

Test Environment

The test environment consisted of the following configuration:

1. OS: Slackware 2.6.17.13

2. Web Server: Apache Tomcat 5.5.12

3. JDK: Jdk 1.5.0_13

4. Memory for the VM: 1 GB

5. Names of VM; Slack11-Apache00, Slack11-Apache01, Slack-Apache02

6. The SCIT gateway was in front of the 3 VM's running the web servers

7. SCIT controller, which was running on a standalone Windows 7 machine

Target/Objective:

The objective of the test was to steal a 3.2 GB file on the web servers.

Undisclosed Information

The version of the Tomcat server used was an older version with a known vulnerability (CVE 2007-0450), and had been running as "root."

Disclosed Information

The path to the file and the configuration of the various servers along with the exposure time of SCIT was disclosed to the testers ahead of the test.

Disabled Components

To focus the test on the Moving Target Defense with Restoration capability of SCIT Labs' technology, the following features were disabled:

1. Throttling of the outgoing messages
2. IT Early Warning
3. Randomize the exposure time

Testing Process

1. Using the previously mentioned Tomcat vulnerability, the test team obtained access and elevated privileged access to the file with little effort.
2. File download was initiated. However, the connection to the server was terminated every 90 seconds. It was not feasible to download the file with one access.
3. A script was developed utilizing the Range header of the HTTP protocol, automated through the cURL utility. The script was written to download the file in segments of 3.8 megabits. Attempts at downloading bigger chunks did not succeed – downloading of bigger chunks would be interrupted and the resulting downloaded file corrupted.
4. The test team concluded that the most reliable approach would be to download each chunk three times; compare the hashes; select the file with identical hashes; discard the download that did not match. This approach would take three times longer and was not considered feasible.
5. The connection between the attacker and the server was terminated at each rotation cycle, and the test team had to re-login using the script. In this experiment, several independent attempts were required.

Remediation

The Telos CNO Team recognized that had SCIT enabled additional features the attack vector would have made the target objective even more difficult. Those features include:

1. **SCIT has the ability to throttle the bandwidth when a particular user is making excessive demands.** For example, a user is expected to access X KBs per unit time. If more frequent downloads are attempted then the bandwidth is reduced – increasing the time taken to download files.

2. **The exposure time at each revolution can be randomized.** This makes it more difficult for the attack script to always start at the beginning of the exposure cycle. This results in reducing the size of the chunks that can be downloaded, once again increasing the time for file exfiltration.

3. **Diversity can be used to further confuse the attacker.** Often diversity is expensive. One of the least expensive diversity mechanisms is ASLR (Address Space Layout Randomization). ASLR can be defeated relatively easily. However, if the ASLR parameters are altered in each SCIT cycle, then the attacker has to waste time in determining ASLR parameters and defeating ASLR implementation. N-version programming is another way to confuse the attacker.

Conclusion and Recommendations

The Telos CNO Team concluded that this technology would provide useful benefits to implementations able to take advantage of it. The most obvious implementation of this type would be applications that operate in a clustered environment. This would ensure that the application is already designed to take into account the extra requirements that the technology would place on it. Any application that cannot be implemented in a clustered environment would possibly require reworking of the application.

On any application that can be adapted for the technology, however, several useful security benefits would be noticeable. Attackers would require more time to adapt to the technology and the constantly changing environment, giving more chances for their activities to be detected by other technologies, such as an intrusion detection system (IDS). Additionally, scanning techniques such as input fuzzing may give inaccurate or inconsistent reports on applications running on this technology, since the techniques may not properly account for the regular rotation of servers.

SCIT Labs used the recommendations of the Telos CNO Team to modify the test environment and make it more effective. The Telos recommendations were used to establish development priorities and modify the development road map.

About Telos Corporation

Telos Corporation empowers and protects the world's most security-conscious enterprises with solutions and services for continuous security assurance of individuals, systems, and information. Telos offerings include cyber security solutions and services for IT risk management and information assurance; secure mobility to protect globally connected enterprises; and identity management to establish trust in personnel and continuously monitor for insider threats. Please contact us for more information.

Telos Solutions that empower and protect the enterprise.™

info@telos.com | 800.70.TELOS (800.708.3567)
www.telos.com | twitter.com/telosnews
facebook.com/teloscorporation
linkedin.com/company/telos-corporation

Telos Corporation | 19886 Ashburn Road, Ashburn, VA 20147-2358 | 1.800.70.TELOS | 1.800.708.3567 | Fax 703.724.3865 | www.telos.com
© 2016 Telos Corporation. All rights reserved. SCIT CS 01-2016