zscaler Security Preview

Jul 17, 2018, 01:36 pm UTC

Summary

Security Assessment	Data Protection
C	High Risk
4 Failed 8 Passed	3 Failed 0 Passed
Apply to Threat Prevention and Access Control test	Apply to Data Protection test

Assessment

SECURITY

Threat Prevention	
✗ **Block an executable (.exe) download**	This tests if you can download .exe files from websites that use a content delivery network (CDN). A CDN makes you vulnerable to malware.
✗ **Prevent cookie stealing or session hijacking**	This test takes a cookie from one website and tries to post it to a second site, a clear sign of an attempt to hijack the web session.
✗ **Prevent cross-site scripting**	This tests if your browser can be compromised by a website that has been infected with malicious code.
✗ **Prevent a common virus from a known malicious site**	This test downloads a benign file containing an EICAR virus test file from the official EICAR site.
✓ **Block threats in known malicious websites**	This tests if you can download a benign object from a known malicious site. It does not attempt to download actual malware.
✓ **Detect a phishing attack**	This checks if you can access one of the latest validated phishing sites uncovered by Phishtank.com.
✓ **Stop a botnet callback**	This test tries to contact a known botnet command-and-control server and download a benign file. Real information is not sent out.
✓ **Stop older known viruses**	This test downloads just enough of the well-known Zbot virus in order to trigger your antivirus security, but not enough of it to cause harm.
✓ **Block a virus hidden in a zip file**	This test downloads a benign file containing an EICAR virus test file that is zipped multiple times.

Access Control	
✓ **Block access to anonymizing websites**	This test tries to connect to an anonymizing website. Failing this test means you can bypass company policy and access restricted content.
✓ **Block websites in embargoed countries**	This tests your ability to access websites in countries that are embargoed by the United States and the European Union, such as North Korea.
✓ **Block access to adult websites**	This test attempts to visit a known adult website and download a benign icon.

DATA PROTECTION

Data Protection	
✗ **Block credit card exfiltration**	This test attempts to exfiltrate numbers that match the format of valid credit card numbers.
✗ **Block Social Security number exfiltration**	This test attempts to exfiltrate numbers that match the format of U.S. Social Security numbers.
✗ **Block source code exfiltration**	This test attempts to exfiltrate typical patterns found in source code.

Assessment details

SECURITY

✗ Block an executable (.exe) download

This tests if you can download .exe files from websites that use a content delivery network (CDN). A CDN makes you vulnerable to malware.

How To fix this

Your security infrastructure should inspect all content, including CDN traffic. Security devices often bypass inspection of content from CDNs like Akami and AWS, because it is viewed as coming from a trusted source.

test description

This test tries to download an executable file from a website with a good reputation that uses a Content Distribution Network (CDN) like Akamai or AWS. It tests whether your security infrastructure can block the executable, limiting the possible introduction of malware and other threats.

Solution Recommendation

Many security solutions bypass scanning CDN content to improve their performance. While CDNs like Akamai and AWS might have better security, it is unwise to assume their content is malware free. All content should be assumed risky and therefore be scanned.

Prevent cookie stealing or session hijacking

This test takes a cookie from one website and tries to post it to a second site, a clear sign of an attempt to hijack the web session.

How To fix this

Your security solution should confirm that a website's cookies are being sent back to the correct originating website.

test description

This test takes a cookie from one website and tries to post it to a second one, a clear sign of an attempt to hijack the web session. To avoid a false positive, ensure that you are not blacklisting the Zscaler website.

Solution Recommendation

Criminals often try to steal browser cookies, so that they can impersonate you, hijack your web sessions, and possibly infiltrate your online accounts. To prevent hijacking of your web session, use a security solution that confirms that a website's cookies are being sent back to the correct originating website.

Prevent cross-site scripting

This tests if your browser can be compromised by a website that has been infected with malicious code.

How To fix this

Your security solution must scan the entire URL and website content for all users who access the Internet.

test description

This test visits a Zscaler CDN website that simulates a cross-site scripting (XSS) compromise by malicious code and checks to see if it would have been able to exploit your web browser. XSS attacks inject malicious code into otherwise legitimate sites in an attempt to exploit your browser and compromise your system.

Solution Recommendation

Your security solution should scan the entire URL and content to identify the source website. It should block the individual content responsible for the malicious script, without overblocking. For example, it should only block facebook.com when it's facebook.com/example that contains the vulnerability.

Prevent a common virus from a known malicious site

This test downloads a benign file containing an EICAR virus test file from the official EICAR site.

How To fix this

It is likely you have no threat prevention tools deployed or, if you do, your Internet traffic is not passing through them.

test description

This test downloads a benign file containing an EICAR virus test file from the official EICAR site. Most network defenses easily block the download either by scanning the file and detecting the test pattern, or by blocking the destination based on reputation.

Solution Recommendation

Make sure you have threat prevention tools deployed between you and your Internet connection, regardless of where and how you connect. While you might have protection on a corporate network, you might not have that same protection from home or other non-corporate connections.

Block threats in known malicious websites

This tests if you can download a benign object from a known malicious site. It does not attempt to download actual malware.

test description

This test checks to see if a benign object hosted on a known malicious site is blocked by your security solution. It uses a compromised site from a list published by Google. The test does not attempt to download actual malware.

Detect a phishing attack

This checks if you can access one of the latest validated phishing sites uncovered by Phishtank.com.

test description

This test tries to access one of the latest validated phishing sites uncovered by Phishtank.com. The test covers all infection vectors, including mobile traffic. Criminals take advantage of mobile traffic as a key weakness in many security solutions. The test does not attempt to download actual malware.

Stop a botnet callback

This test tries to contact a known botnet command-and-control server and download a benign file. Real information is not sent out.

test description

This test tries to contact a known botnet command and control server (call home) and download a benign file. The server is selected from Google's Safebrowsing list. The test does not send real information.

Stop older known viruses

This test downloads just enough of the well-known Zbot virus in order to trigger your antivirus security, but not enough of it to cause harm.

test description

This test downloads enough of the well-known Zbot virus to trigger your security; it stops the virus download before it can infect your system. All antivirus engines should detect and block this very common virus, whether delivered from a trusted or unknown CDN.

Block a virus hidden in a zip file

This test downloads a benign file containing an EICAR virus test file that is zipped multiple times.

test description

This test downloads a benign file containing an EICAR virus test file, which is zipped multiple times. The test file is zipped using standard archivers and contains multiple benign files combined with the EICAR virus. The download is terminated if the inline network security allows most of the file.

Access Control

Block access to anonymizing websites

This test tries to connect to an anonymizing website. Failing this test means you can bypass company policy and access restricted content.

test description

This test tries to connect to an anonymizing website. Employees often try to bypass company policy by using anonymizing proxies that allow them to visit blacklisted websites, view pornography, or access restricted content. These anonymizers can open a backdoor for malware, expose your company to litigation risk, and expose your data to untrusted third parties.

Block websites in embargoed countries

This tests your ability to access websites in countries that are embargoed by the United States and the European Union, such as North Korea.

test description

This test tries to connect to websites in countries under embargo by the Unites States and European Union, such as North Korea. Most companies want to prevent users from connecting to websites in countries that are under embargo in order to comply with trade laws. Additionally, compromised websites are often hosted in countries that are hostile to the United States and the European Union, and they place a low priority on Internet security.

Block access to adult websites

This test attempts to visit a known adult website and download a benign icon.

test description

This test tries to visit a known adult website and download a benign icon. Employees often violate company policy and try to visit blacklisted websites and view pornography. These sites act as common watering holes to propagate malware, and they might expose your company to litigation risk and your data to untrusted third parties.

DATA PROTECTION

Data Protection

Block credit card exfiltration

This test attempts to exfiltrate numbers that match the format of valid credit card numbers.

How To fix this

Consider a Data Loss Prevention (DLP) system that can find and block credit card pattern matches in outbound traffic.

test description

This test tries to exfiltrate numbers out of your network that match the format of credit card numbers. Your network security solution should easily identify this leakage.

Solution Recommendation

Many security solutions are deployed in TAP mode and detect, but do not block, the leakage of sensitive information outside the organization. Consider a Data Loss Prevention system that monitors outbound traffic and blocks exfiltration attempts based upon pattern matches to sensitive data, such as U.S. Social Security numbers, credit card numbers, or your company's intellectual property.

Block Social Security number exfiltration

This test attempts to exfiltrate numbers that match the format of U.S. Social Security numbers.

How To fix this

Consider a Data Loss Prevention (DLP) system that can find and block Social Security number pattern matches in outbound traffic.

test description

This test tries to exfiltrate numbers out of your network that match the format of U.S. Social Security numbers. Your network security solution should easily identify this leakage.

Solution Recommendation

Many security solutions are deployed in TAP mode and detect, but do not block, the leakage of sensitive information outside the organization. Consider a Data Loss Prevention system that monitors outbound traffic and blocks exfiltration attempts based upon pattern matches to sensitive data, such as U.S. Social Security numbers, credit card numbers, or your company's intellectual property.

Block source code exfiltration

This test attempts to exfiltrate typical patterns found in source code.

How To fix this

Consider a Data Loss Prevention (DLP) system that can find and block source code pattern matches in outbound traffic.

test description

This test tries to exfiltrate typical patterns found in source code. Stealing your intellectual property is the goal of some of the world's most dangerous hackers and state-sponsored actors seeking a competitive advantage. A leak of intellectual property can have profound consequences for your enterprise — from rewriting source code to re-issuing binaries.

Solution Recommendation

Many security solutions are deployed in TAP mode and detect, but do not block, the leakage of sensitive information outside the organization. Consider a Data Loss Prevention system that monitors outbound traffic and blocks exfiltration attempts based upon pattern matches to sensitive data, such as U.S. Social Security numbers, credit card numbers, or your company's intellectual property.