Security Preview

Test Plan

Prepare for the Security Preview without the Zscaler service	Ensure that: • You are logged out of the Zscaler Service • You do not have a PAC file installed (verify at ip.zscaler.com) • You have cleared your cache
Take the Zscaler Security Preview without Zscaler	• Navigate to http://securitypreview.zscaler.com/, and click Check Your Security Now. • Note your score • Click to have the results e-mailed to you
Prepare for the Security Preview with the Zscaler service	Ensure that: • You have installed the SSL PAC file and are going through the Zscaler Service (verify at ip.zscaler.com) • You have logged in to the service • You have cleared your cache
Take the Zscaler Security Preview with Zscaler	• Navigate to http://securitypreview.zscaler.com/, and click Check Your Security Now. • Note your score • Click to have the results e-mailed to you

Security Test Plan

Test Plan

- *Please install the SSL PAC file.*
- *Navigate to http://securitytest.acmemodern.com*
- *Upon redirect, please log in with your administrator credentials*
- *Once going through Zscaler, you will have to log in again to enter the security portal*
- *Username: acmemodern* *Password: securitytest*

PLEASE NOTE: You must install the Zscaler SSL PAC file before beginning these tests. This is real live malware, and it can cause real live problems.

Tests include:	
EICAR Test Virus, zipped 5 times	Eicar is a well-known virus test file, created by the European Institute for Computer Antivirus Research. Any virus scanner should be able to detect this test. To elude detection, this version of the virus is zipped 5 times.
Powerpoint with embedded macro virus	Microsoft Office applications have support for Visual Basic for Applications (VBA), a macro language. VBA greatly extends the functionality and automation of Microsoft Office applications, however it can also be used for malicious purposes and is a common vector for infections. This Powerpoint presentation has an embedded macro virus.
Malicious Android APK	Though most users will install applications and games directly from the Google Play Store, some will download APKs (Android Package Kits). A common practice is to get a legitimate APK and repackage it with a virus or trojan. Users that install the modified version will have the desired app or game, but are also infected. This Android APK contains a virus.
Packer Virus	Packer viruses include their own compression algorithm, similar to ZIP, RAR etc. However by using their own algorithm, which is unknown to scanners, the packer virus tries to circumvent virus scanners. Because the virus actually needs to be unpacked to be able to infect a device, packer viruses are usually executables with the malicious payload packed. When run, they will unpack the payload. By executing the file in Zscaler's Cloud Sandbox, Zscaler is able to detect any malicious behavior and classify the packer viruses correctly.
Tescrypt Ransomeware	Ransomware is a type of malware that is rapidly gaining popularity. Once executed, ransomware holds the user's data "hostage;" typically by encrypting files. Users will be redirected to a webpage with instructions on how to make a payment to unlock their files. Payment is often required in a digital currency such as Bitcoins. Tescrypt is an example of this kind of ransomware.
HTTP Remote Access Trojan	A Remote Access Trojan (RAT) is a popular form of malware, as it allows attackers to remotely control the target. It's often used as an entry point to a network to gain access to other systems that are otherwise externally unreachable. This specific RAT runs a webserver that is used as the remote access console.

Malicious PDF	Similar to Microsoft Office documents, PDFs also have support for macros. Macros can be very helpful, but can be used maliciously. PDFs are a popular method for infecting victims because they are used frequently and seen as harmless to most users. This method is frequently used for targeted spear phishing attacks, in which the malicious content could be disguised as a resume that seems to be from the HR department, or an invoice that looks as if it comes from Finance.
Vulnerable ActiveX Controls	ActiveX is a framework designed by Microsoft, mostly to enhance the capabilities of Internet Explorer. ActiveX was a popular method to infect victims, as it had a lot of security issues. Though ActiveX has been deprecated now, many organizations still have legacy web apps that require ActiveX.
Botnet Command and Control Traffic	Infected computers that are part of a botnet need a way to receive commands. To circumvent firewalls, botnets are often designed to have the infected computers "call out" instead of waiting to receive a call in from the remote controller. This link is an example of an infected computer downloading new instructions from a Command and Control server that requires ActiveX.

Admin View

Log in to the Zscaler admin portal

Admin Tests:	
Top users for Adware	Starting from the Security Dashboard, locate the top department for Adware in the last month. See if you can identify the top user!
Types of traffic blocked	From Analytics, go to Web Insights, and filter on Web actions that have been blocked. View logs on the results, and see what you can spot, including types of blocked traffic and reasons for that action.