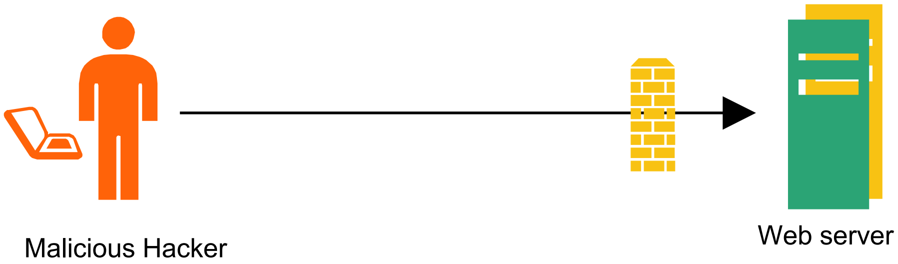
Scob Outbreak

The Scob outbreak enabled a hacker to steal customer data such as username and password information by secretly installing an application that captures all key strokes on a computer and sending the information to a data collection server.

SONICWALL

Anatomy of an Outbreak - Scob



The hacker targets unpatched Microsoft IIS Web servers.

Over 100 Web sites were exploited by this attack.

SonicWALL Intrusion Prevention prevents the exploit of the SSL-PCT vulnerability on the Microsoft IIS Server

Web page

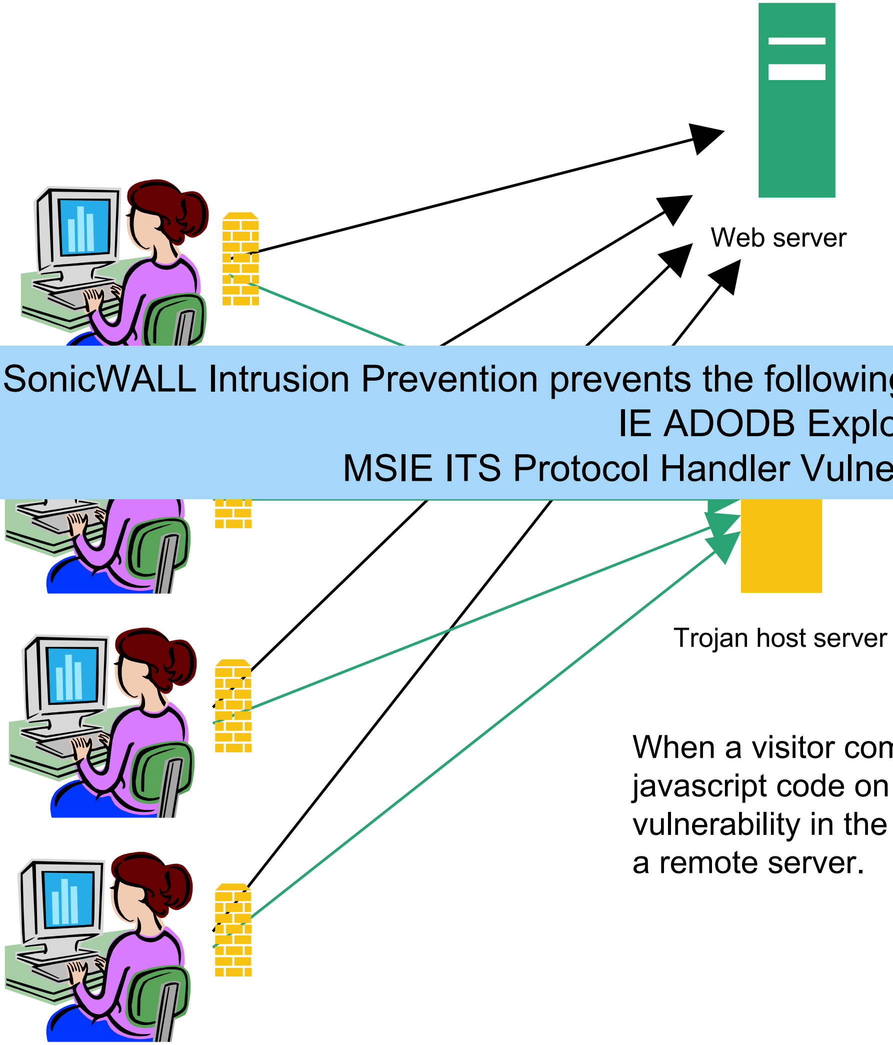
<META name="keywords" content="Security Topic Center White Papers Analysis
News Reviews Opinion Commentary Virus VPN Hacking Worm Hackers RADIUS
Enterprise Security Wireless Networking (LAN/WAN/PAN)" lang="en-us">
<META name="title" content="Security News, Product Reviews, Trends and
Analysis - eWEEK.com Security Center" lang="en-us">
<META name="description" content="Security Topic Center White Papers Analysis
News Reviews Opinion Commentary Virus VPN Hacking Worm Hackers RADIUS"
lang="en-us">

<META name="keywords" content="Security Topic Center White Papers Analysis
News Reviews Opinion Commentary Virus VPN Hacking Worm Hackers RADIUS
Enterprise Security Wireless Networking (LAN/WAN/PAN)" lang="en-us">
<META name="title" content="Security News, Product Reviews, Trends and
Analysis - eWEEK.com Security Center" lang="en-us">
<META name="description" content="Security Topic Center White Papers Analysis
News Reviews Opinion Commentary Virus VPN Hacking Worm Hackers RADIUS"
lang="en-us">

Microsoft IIS servers were exploited to insert Javascript into HTML of Web pages.

Insert Javascript

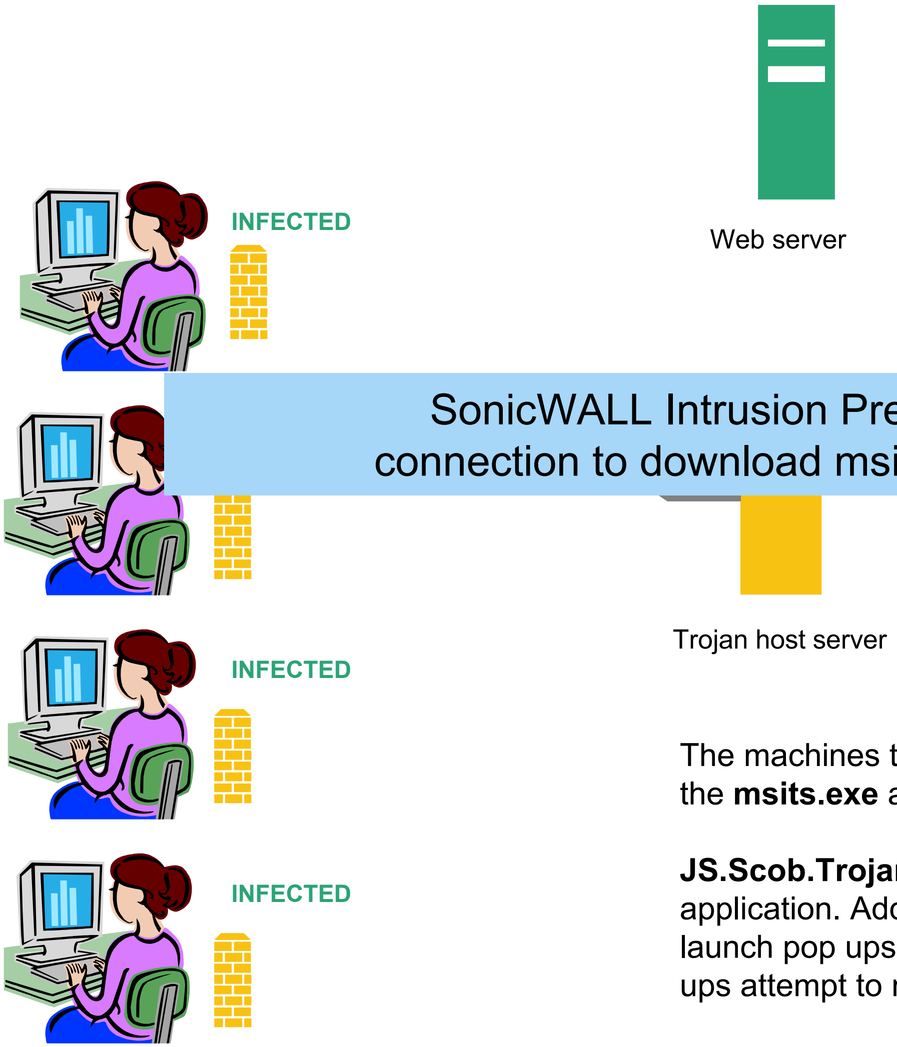
Anatomy of an Outbreak - Scob



SonicWALL Intrusion Prevention prevents the following exploits of Microsoft Internet Explorer
IE ADODB Exploit
MSIE ITS Protocol Handler Vulnerability over HTTP

When a visitor comes to the compromised Web site, the malicious javascript code on the Web server exploits an Internet Explorer vulnerability in the visitor's browser, redirecting the visitor's machine to a remote server.

Anatomy of an Outbreak - Scob



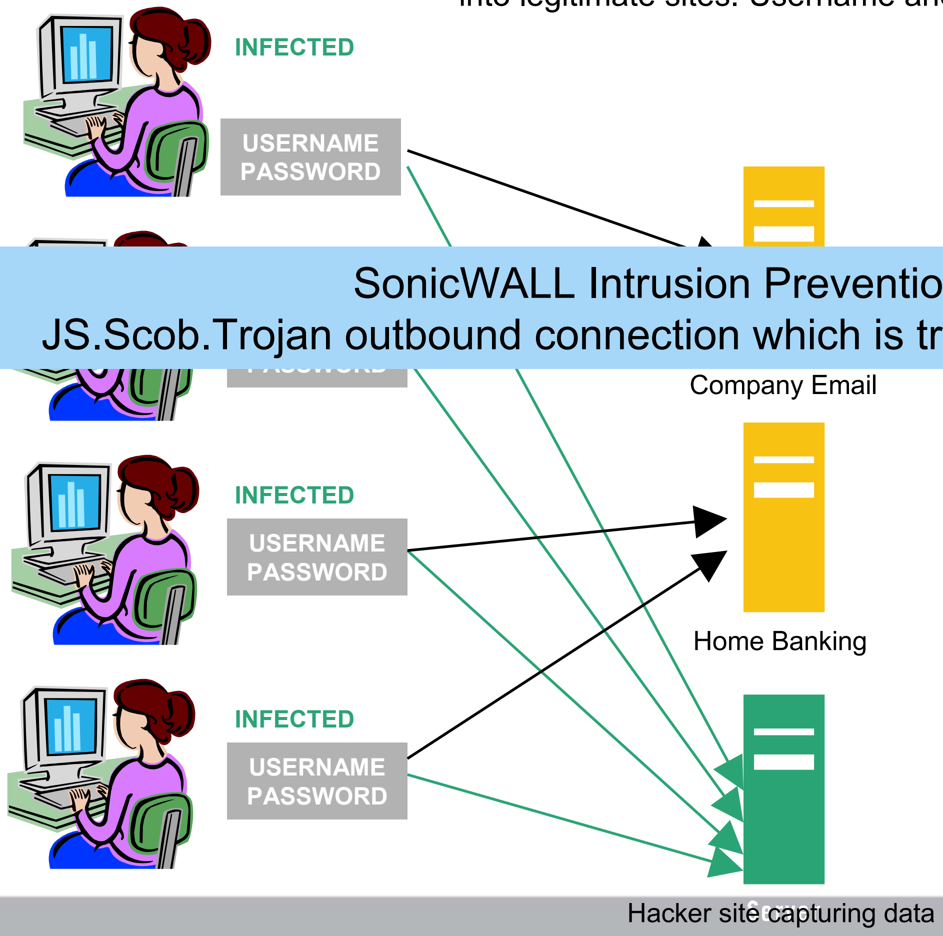
SonicWALL Intrusion Prevention prevents the connection to download msits.exe (JS.Scob.Trojan)

The machines then contacts the Trojan host server and downloads the **msits.exe** application which installs the **JS.Scob.Trojan**.

JS.Scob.Trojan is a key logger and information collection application. Additionally, the Trojan injects code into DLLs to launch pop ups while the visitor is using the Web browser. The pop ups attempt to mislead the user into entering confidential data.

Anatomy of an Outbreak - Scob

The key logger application captures user name and password data as it is entered into legitimate sites. Username and password data is then sent to the hacker site.



SonicWALL Intrusion Prevention prevents the JS.Scob.Trojan outbound connection which is transferring the confidential data

Signatures Updated Daily/Weekly

Description	Type	Severity
Sasser FTP Server connection attempt	BACKDOOR	High
Sasser ftp script to transfer up.exe using open shell	BACKDOOR	High
Agobot/Phatbot Infection Successful	BACKDOOR	High
Phatbot P2P Control Connection	BACKDOOR	High
Beast v2.05 Outbound Connection Attempt	BACKDOOR	High
Autoproxy Trojan control connection	BACKDOOR	High
IIS5 SSLBomb	DOS	High
ASN.1 generic overflow	NETBIOS	High
ASN.1 netbios generic overflow	NETBIOS	High
Sasser Worm exploit attempt type 1	NETBIOS	High
Sasser Worm exploit attempt type 2	NETBIOS	High
Sasser shellcode generic	NETBIOS	High
Sasser shellcode (Win2k)	NETBIOS	High
Sasser shellcode (WinXP)	NETBIOS	High
Sasser worm buffer overflow attempt	NETBIOS	High
Agobot/Variant Connection Attempt	RPC	High
RPCSS Stack Overflow	RPC	High
RPC DCOM Vulnerability Scan -- Blaster	RPC	High
Blaster Connection Attempt	RPC	High
Bagle.Q-eml	VIRUS	High
Zafi over SMTP	VIRUS	High
MacOS X Safari Help.app Runscript Traversal and Execution Attempt	WEB-CLIENT	High
MacOS X Safari Help.app Runscript Execution Attempt	WEB-CLIENT	High
Microsoft MHTML URL Redirection Attempt 5	WEB-CLIENT	High
IE6 Object Tag Improper Execution	WEB-CLIENT	High
IE6 Object Tag Improper Command	WEB-CLIENT	High
IE Object Tag -- Improper Script Execution Attempt	WEB-CLIENT	High
Microsoft MHTML URL Redirection Attempt 1	WEB-CLIENT	High
Microsoft IE ms-its Protocol Handler Improper File Processing	WEB-CLIENT	High
Microsoft MHTML URL Redirection Attempt 3	WEB-CLIENT	High
Microsoft MHTML URL Redirection Attempt 4	WEB-CLIENT	High
MSIE ITS Protocol Handler Vulnerability over HTTP	WEB-CLIENT	High
MSIE ITS Protocol Handler Vulnerability over SMTP	WEB-CLIENT	High
Internet Explorer BMP Processing Overflow	WEB-CLIENT	High

Monthly Average

- **30-40 Signatures Per Month**
- **25% High**
- **35% Medium**
- **40% Low**

IPS Signatures Added in May and June

Exploit Signatures

- Microsoft MHTL URL Redirection Attempt (June)
- IE ADODB Exploit Javascript detected (June)
- ASN.1 netbios generic overflow (May)
- Secure LDAP SSL-PCT exploit (May)
- Multiple SQL and MSSQL Injection exploits (May)
- Multiple MacOS X Safari Help.app Runscript exploits (May)
- RealServer exploit on Windows and Linux (May)

Virus, Worm and Trojan Signatures

- Scob trojan download and connection attempt (June)
- IE msits.exe download detected (June)
- Beast trojan connection attempt (June)
- Zafi over SMTP (June)
- ISS Witty worm (June)
- Multiple Sasser, Slammer and Blaster variants (May/June)
- Kibuv worm exploit (May)

Application Signatures

- iTunes (May)
- GoToMyPC (May)
- MusicMatch (May)