

Web Based Attacks

A Symantec White Paper

MSIT 458 – Information Security

The Locals

IN THE RACE TO INFECT USERS WITH MALCODE...



VIRUSES & WORMS



WEB ATTACKS

Why Web Sites?

* Increasing Complexity

- * Content aggregation
- * Database driven
- * Plugins, media, scripting

The screenshot shows the homepage of The New York Times. At the top left is a black box with the text "MARC JACOBS" and a red arrow pointing to it. The main header features the "The New York Times" logo in a large, black, serif font. Below the logo, the date "Sunday, October 31, 2010" and "Last Update: 4:21 PM ET" are displayed. To the right of the logo is a black box with the text "WELCOME TO MARCJACOBS.COM". Below the header is a search bar with the text "Search" and a "ING DIRECT" logo. To the right of the search bar is a small icon of a newspaper and the text "Get Home Delivery in Chicago | Personalize Your Weather". On the left side, there is a vertical menu with the text "Switch to Global Edition" and a list of categories: JOBS, REAL ESTATE, AUTOS, ALL CLASSIFIEDS, WORLD, U.S., POLITICS, N.Y./REGION, BUSINESS, TECHNOLOGY, SPORTS, SCIENCE, and HEALTH. The main content area features a large article titled "Bombs Were Designed to Destroy Planes, U.S. Believes" by JOSEPH BERGER and ROBERT F. WORTH, with a sub-headline "Officials believe the two bombs in last week's plot, one of which had traveled on passenger planes, were intended to blow up the aircraft carrying them." To the right of the article is a photograph of two men sitting at a desk in a room with large windows. Below the photograph is an "OPINION" section with a "VIDEO" icon and the title "'Memento Mickey'" by Jeff Scher, with a sub-headline "Jeff Scher's short film evoking death, or perhaps life, for Halloween." To the right of the "OPINION" section is a "Log In With Facebook" button and a "WHAT'S POPULAR NOW" section with a list of articles: "Give Obama a Break", "The Grand Old Plot Against the Tea Party", "Dowd: Can the Dude Abide?", "Rich: The Grand Old Plot Against the Tea Party", and "Friedman: India's Morning". A red arrow points to the "Log In With Facebook" button, and another red arrow points to the "WHAT'S POPULAR NOW" section.

Why limit your target?



Why limit your target?



- * Use mainstream sites
- * Targets more users
 - * 2008 = web attacks from 808,000 unique domains
- * Targets less suspecting users



How do Websites get infected?

- * SQL Injection
- * Malicious Advertisements
- * Search Engine Result Redirection
- * Attacks on the backend virtual hosting companies
- * Vulnerabilities in the Web server or forum hosting software
- * Cross-site scripting (XSS) attacks



What's the big deal?

The Bredolab example

- * Bredolab: “a large family of complicated, polymorphic trojans.”
- * Machines became infected through drive-by-downloads and email. It instructed users to purchase fake anti-virus software (Antivirusplus).
- * It grew to become a botnet with 30 million computers and 150 C&C servers.
- * Pay-per-install malware: rent a block of 1,000 bots at a time.

The Drive-By Download

- * Attacks from mainstream websites occur thousands of times every day
- * Leverages vulnerabilities on unpatched computer
- * Entire attack is invisible to victim
- * It is automatic
- * No user interaction required

The Drive-By Download



Through Open Doors

- * Drive-by downloads exploit software vulnerabilities on computer
- * Count on the user not applying the software updates that close open doors
- * Began by exploiting holes in operating systems like Windows (MS-RPC DCOM and LSASS components)
- * Progressed to exploiting...
 - * Web browsers, browser plug-ins
 - * ActiveX controls, multimedia
 - * Third-party applications
- * All it takes is one open door to breach the fortress

The Usual Suspects?

- * Exploit creation no longer limited to techies
- * Off-the-shelf Web toolkits
 - * Bring a DIY dimension to malware creation
 - * Little expertise required
 - * Comes with simple user interface
 - * Anyone can create an exploit



Measures of a successful exploit

- * Remaining Undetected
 - * Timing the Attack
 - * Playing the Odds
 - * Obfuscating Attacks
 - * Dynamically changing URL and Malware Variants
- * Being Efficient
 - * Profiling the Victim
 - * Using Brute Force
- * Increasing Sophistication
 - * Clickjacking





WHO'S THIS GUY?

HINT: 1994 WORLD CUP

Andre Escobar

- * Famous for: unintentionally helping the opposing team by scoring an own goal at the 1994 World Cup.
- * The Goal = your computer
- * The Ball = malware
- * The Kick = hitting **Enter** on your keyboard or mouse



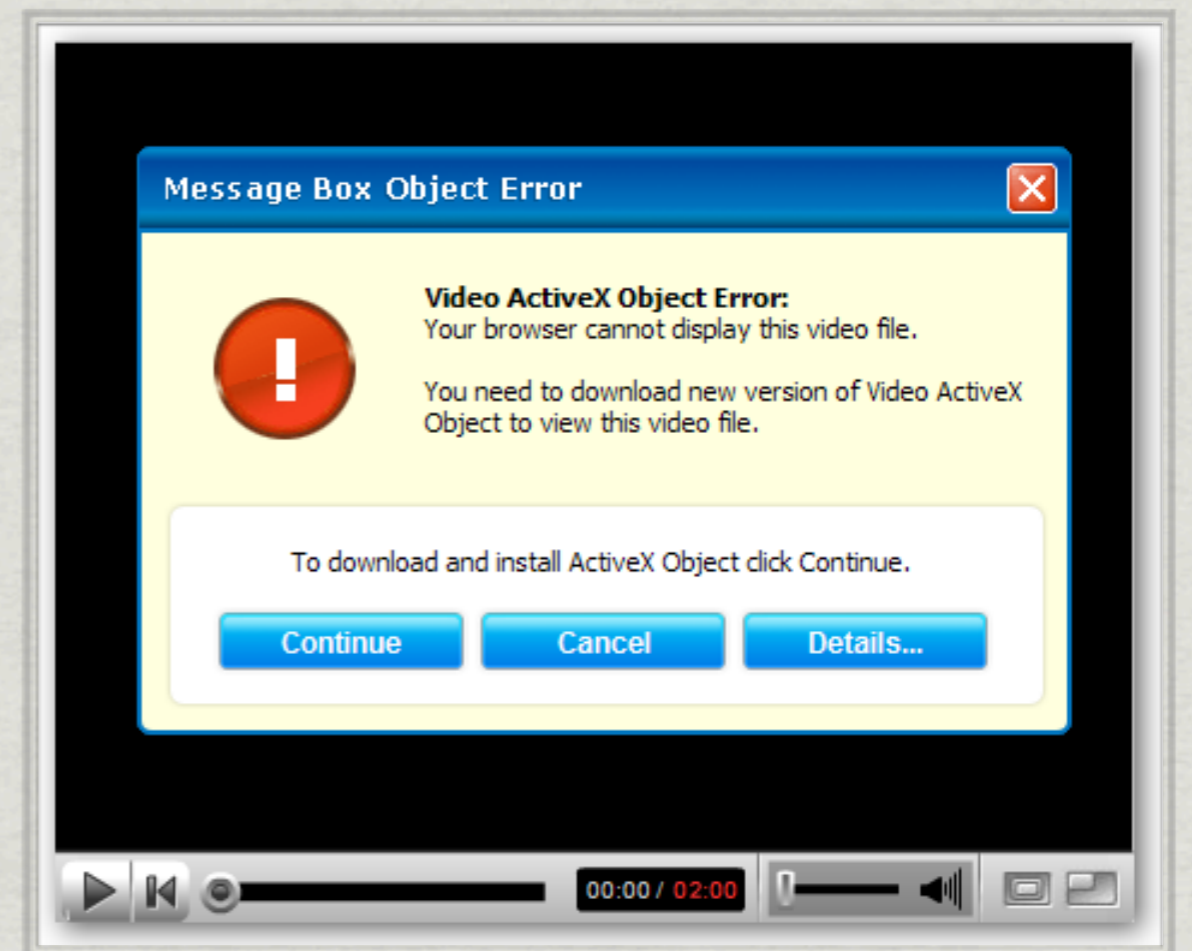
DON'T BE THIS GUY!

Getting onto a user's computer with help from the user

- * **Fake codec**
- * Malicious peer-to-peer files
- * **Malicious advertisements**
- * **Fake scanner Web page**
- * Blog spam
- * Other attack vectors

Fake Codec

- * Takes advantage of users understanding that downloads are needed for new media or browser plug-in
- * Malware authors establish sites that hosts tempting content and prompts users to install a new codec, but really authorizing users to install malware into their computers
- * Icons and logos from trusted video and multimedia players may be used



Malicious Advertisements

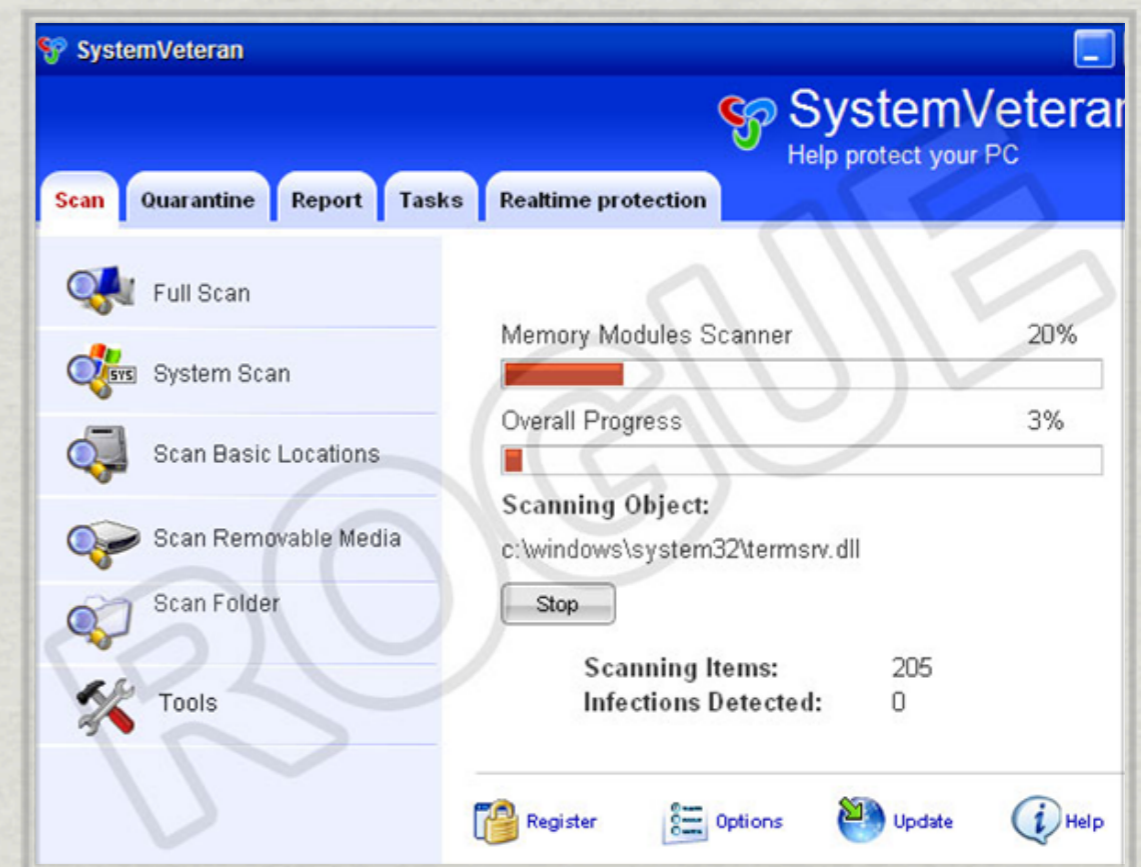
- * Mimics the techniques of legitimate businesses by turning on ads
- * Ads may lead users to a fake scanner page
- * Plays off of “free” copies of coveted games and software
- * Interesting 2010 study* results:
 - * 1.3 million malicious ads are viewed per day
 - * The probability of getting infected is 2x as likely on a weekend



*"Q1'10 web-based malware data and trends," blog.dasient.com, 5/10/10.

Fake Scanner Webpage

- * Creates a pop up with a legitimate-looking operation system alert notification
- * Uses scare tactics to convince users that their computers are infected, often in conjunction with malicious advertisements
- * Prompts users to download a fake removal tool to remove infections
- * Interesting study* results:
 - * Forums and blogs are common areas to place fake scanners
 - * Some are even advertised on TV, like FinallyFast.com.au



*"Beware of Rogue Programs: Fake Malware Scanners and Registry Cleaners," brighthub.com, 5/4/10.

What happens on
the user's computer?



What happens on the user's computer?

- * Fake antivirus software convinces the user to pay to remove fictitious viruses.
- * Steal your personal information
- * Use your computer to attack other computers

What can you do to protect yourself?

- * Keep software up to date
- * Deploy a comprehensive end point security product
 - * Heuristic file protection
 - * Intrusion Prevention System (IPS)
 - * Behavioral Monitoring
- * Keep your security protection subscription current
- * Be suspicious
- * Adopt a password policy
- * Prevention is the best cure!

Be vigilant. (Buy a Symantec product.)