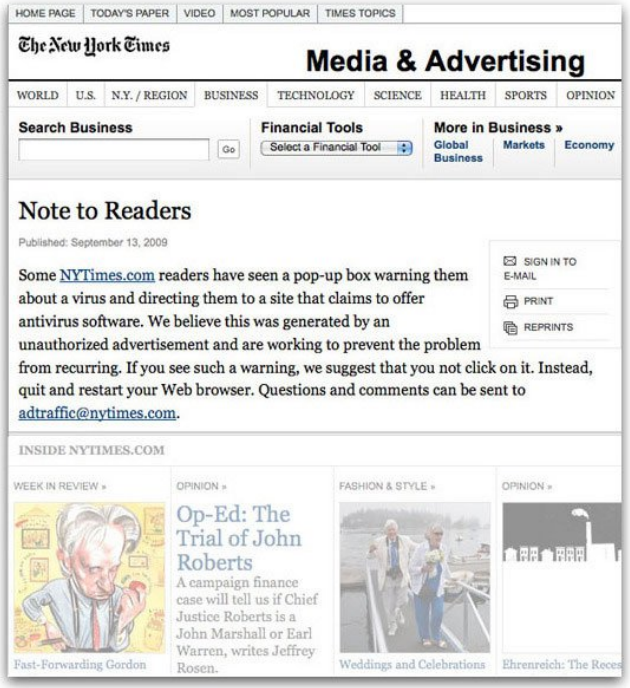
Malvertising

David Fowler – Dennis Dayman

New York Times

- On September 14, 2009 New York Times readers were automatically redirected to a site hosting malmare thanks to an ad containing malicious code.



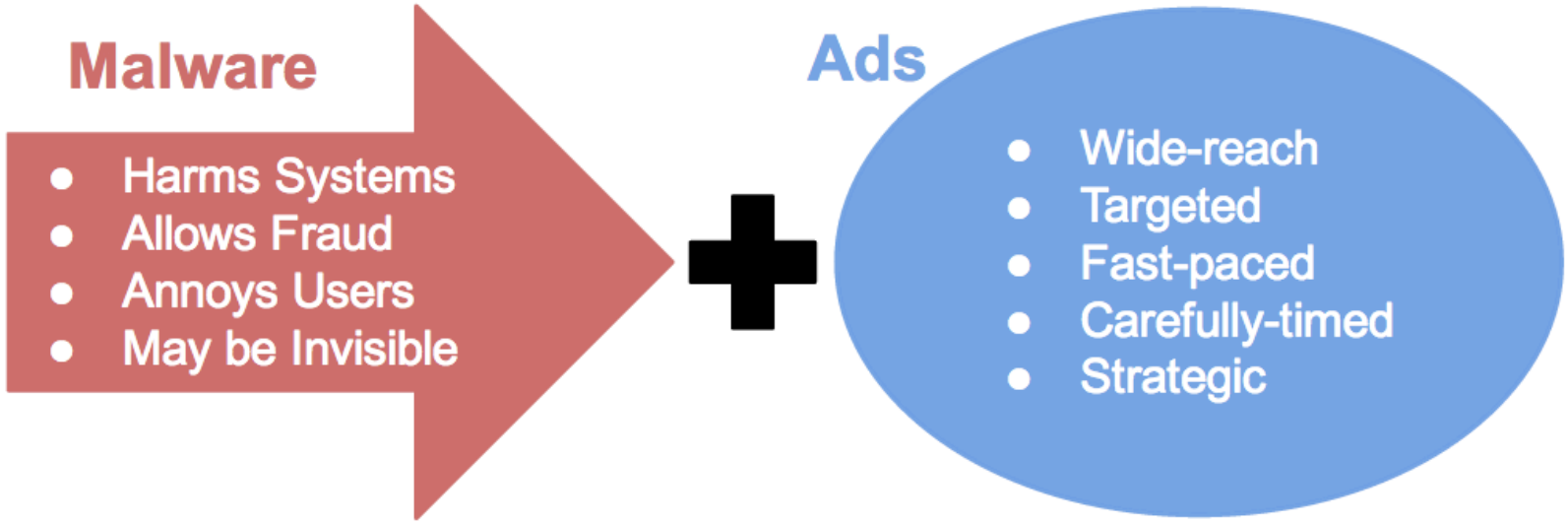
TweetMeme

- On July 15 2010, TweetMeme was the victim of a similar attack and began sending its users to a "scareware" site. These are just two examples of "malvertising," one of the fastest growing security threats…

Agenda:

- What is Malvertising?
- Complexity of the Ecosystem
- Proliferation & Impact
- Who are the Victims?
- Obstacles & Hurdles
- Types and Modes
- Tips for Everyone

What is Malvertising?



MALWARE: Malicious Software

MALVERTISING: MALWARE + ADVERTISING

Source: anti-malvertising.com

Complexity of the Ecosystem

Please direct any inquiries or comments on the landscape to Terence Kawaja at tkawaja@gcasavvian.com or (212) 999-7082

OTA Online Trust Alliance

Proliferation & Impact

Infected Ad Server

Infected Ad

Infected Site

1. User visits a trusted website via a link, typing the URL directly or going to their favorites
2. Ad tricks user / or auto downloads via a "driveby" a program that installs malware
3. Captures & forwards data back to creator, turns into bots, installs ransomware and other
4. Used for identity theft, ACH fraud, account take over, corporate espionage and other crimes

Impact

All site visitors *plus the reputation of Web Sites & Brands*

OTA Online Trust Alliance

Types and Modes

- By visiting websites that are affected by malvertising, users are at risk of infection. There are many different methods used for injecting malicious advertisements or programs into webpages:
  - Pop-up ads for deceptive downloads, such as fake anti-virus programs that install malicious software on the computer
  - In-text or in-content advertising
  - Drive-by downloads
  - Web widgets in which redirection can be co-opted into redirecting to a malicious site
  - Attackers embed hidden iframes that spread malware into websites
  - Content Delivery Networks (CDNs can be exploited to share malware)
  - Malicious banners on websites
  - Third-party advertisements on webpages
  - Third-party applications, such as forums, help desks, CRM and CMS

Source: wikipedia

Who are the Victims?

- Unsuspecting users who visit trusted sites
- Businesses who are compromised
  - Loss of proprietary data
  - Emerging driver of data breaches
  - Bots & DDoS attacks on critical infrastructure
- Web properties who unknowingly serve malicious ads
- The integrity of the interactive ad industry

Obstacles & Hurdles

- Perceived as not a significant issue by some trade groups
- Complexity of the ecosystem and supply chain
- Cybercriminals can remain hidden and anonymous
- Like spam, a very low cost and amplified effort
- Consumer education has little impact
- Inability of the site (publisher) to have a line of sight
- Compromised user /device has limited ability to identify the cause
- Perceived anti-trust and competitive roadblocks to share threat intelligence and work together

Why is this important to me?

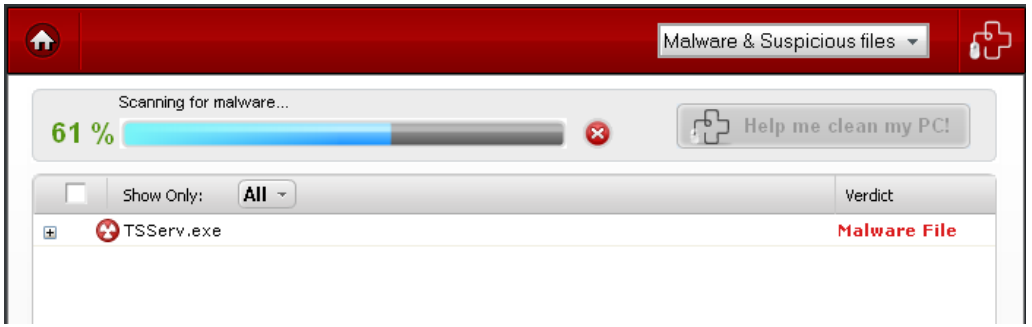
- Organizations around the world are quickly realizing that front end web security is important to their customers
  - PR issues
  - Loss of customer
  - Brand dilution
  - Loss of data
  - Legal liability

Who pays?

- The biggest question is whether to charge customers for privacy and security
  - No is simple the answer
- We as a community are offering inter-connectivity to the masses
  - We are a cause of this issue
- It's our responsibility to ensure our systems are protected

Inline and real-time

- Think about this?
  - When your customers uploads content, are you scanning it?
    - Not just for anti-spam reasons
      - FREE!, $$$, Discount, OFFER, Stock alert
- Are you checking for them:
  - Links
  - Images
  - Attachments
  - Domains
  - Reply to's



- Are you ready to stop and impact their campaigns for their and your safety?

So, what can my company do?

- Join coalitions/conferences
  - There are so many out there that you and your company and participate
    - Blackhat, M3AAWG, IAPP, etc
- Certify and educate
  - Make sure your staff is trained up
    - CIPP-IT or CISSP
- Share information
  - Many lists out there, even in coalitions
- Technology
  - Make use of and update regularly enterprise software
- Security by (re)-design
  - Make security a line item in your development process


FROM THE
INSIDE
OUT

Training

- How often are you training your employees?
- Are you giving new employee's security training?
- Are you training existing employee's annually?
- Testing them

Who has your back?

Ask yourself this question?

- Who is responsible for security in my company?
  - Is there a CSO/CISO?
    - Not just a CTO playing the role
  - Someone separate and involved
  - Responsible for going to jail when things go wrong
    - No, not really
  - Someone with the power to stop and begin things?

- If you don't have yes to these answers then its time to push the panic button

Tips for Everyone

- Use up-to date ant-virus software
- Ensure your browser and OS are update
- Watch what you download
- Help keep the web safe
- If you suspect a computer maybe infected use a reputable product to detect/remove it

Source: anti-malvertising.com