How to Avoid Malvertising Leading to Phishing and Other Problems

Gene Gusman, Experian Marketing Services

Agenda

- What is Malvertising?
- What forms does it take?
- What damage can it cause?
- What should responsible companies do to minimize the risk?
- What to do when there is a malvertising event?
- What is the future of malvertising?

What is Malvertising?

- Malicious Software (Malware) + Advertising
- Spreads malware through digital ads
- Malicious ads injected on legitimate sites
- Malicious ads sent via email
- Malware placed on visitor's computer

What is Malvertising?

- Malware
  - Steals/Destroys info
  - Compromises/Disrupts systems
  - Uses systems anonymously to attack others

LEVERAGES

- Advertising
  - Broad exposure of advertising
  - Sophisticated targeting technology

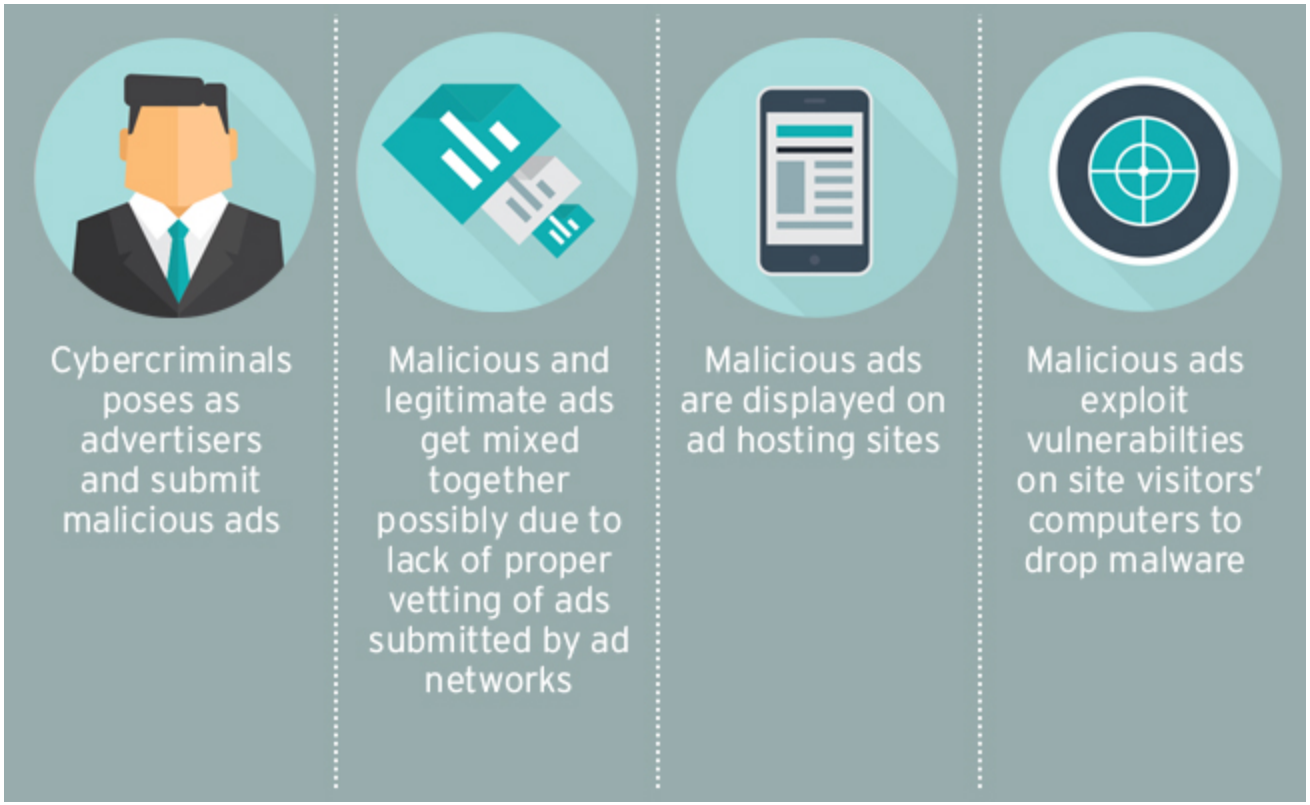
In the Beginning …

- 2007 – first recorded sighting of malvertising - based on a vulnerability in Adobe Flash (a product that continues to have vulnerabilities today)
- 2009 NY Times hit by malvertising – a pop-up posing as an anti-virus scanner.

What forms does it take?

- Paid Ads on Ad Networks
- Paid Ads using Google AdWords
- Drive-by downloads
- Hidden iframes
- Pop-up ads for deceptive downloads
- Pop-under ads (ad window behind the main window)
- Fake cancel buttons
- Malicious banners on websites
- Phishing

How does it work?



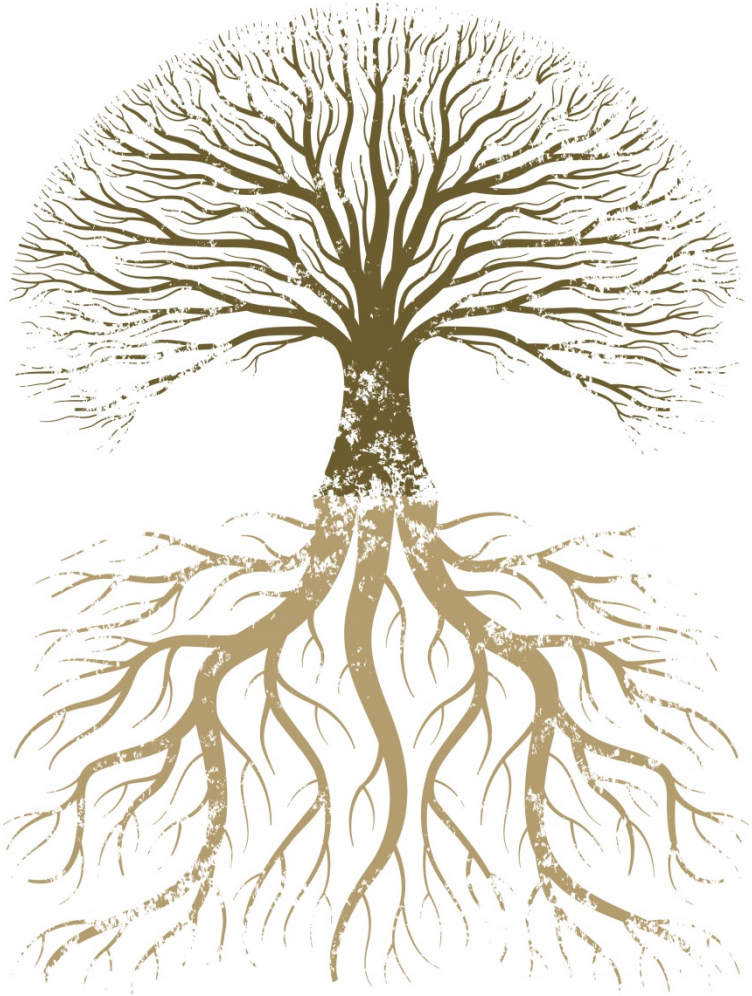
How does it work?

- Cybercriminals sign up to ad network
- Warm their reputation with good ads
- Upload malicious ads
- Site visitor unknowingly receives malware
  - Various techniques such as hidden iFrames – redirect to exploit site
  - Landing page code finds vulnerabilities and installs malware
- Bad things happen
  - Data stolen/destroyed
  - Use target for bot attacks
  - Phishing

Trojan Rabbits

Worms

Rootkits



Ransomware


PETYA
RANSOMWARE
Start
Payment
FAQ
Support
English
Your computer has been encrypted
The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.
The price will be doubled in:
6 days 13 hours 43 minutes 10 seconds
Start the decryption process

What are the types of malware?

- Trojan – tricks users into running it
- Worm – spreads through replication
- Rootkits – allows hidden functionality / backdoor
- Ransomware – demands payment to unlock system/files

What damage can it cause?

- Email attacks such as Phishing from infected machine
- Loss of information
- Loss of system access
- Corruption of data
- Stolen information
- Compromise of security credentials
- Loss of funds from bank accounts
- Use of company servers to attack other targets
- System/Data held at ransom
- Damage to brand

Ransomware – Voted most popular

- "*According to the FBI, ransomware attackers collected more than $209 million in ransom during the first three months of 2016 alone, with the volume of attacks 10 times higher than all of 2015. …*
- *Most ransomware spreads through phishing email, though mobile devices and infected websites are also vectors"*

(from the Proofpoint Ransomware Survival Guide)

Why has Ransomware Increased?

- Low cost to implement
- More channels for distribution
- Targets can be willing and able to pay large ransoms
- Collection is easy via Bitcoin or other digital currency.

What should responsible companies do to minimize the risk of malvertising?

Protect clients and their subscribers

- Protect clients from Phishing against their subscribers
  - Scan all attachments or simply do not permit them
  - Scan entire email content for dangerous URLs, script, images.
  - Check all domains in the email, including the header if you allow your clients to change any field other than friendly from
  - Have them use DMARC with a policy of reject
- Design your systems/software with security in mind

Protect Against Inbound Attacks

- Use email, mobile and social media security software
  - anti-virus , anti-malware software, etc.
  - Not foolproof, esp. for new/zero-day attacks
- Adjust browser/plug-in settings
- Create regular backups
- Run regular backup and restore drills
- Maintain up to date software: OS, security software and patches

Protect Against Inbound Attacks

- Train employees about social engineering attacks
  - What not to do
  - How to recognize phishing, malware, ransomware, etc.
- What to do
  - Disconnect your computer from the network (wired AND wireless)
  - Report attack immediately to the security team
- Ongoing
  - Refresher courses
  - New employees – part of staff onboarding

Stay Informed

- Participate in industry events
- Join industry coalitions
- Educate staff (internally or 3rd party programs)

What to do when there is a malvertising event?

- Analyze – automate data collection/analysis
- Contain – automate quarantine/containment
- Eradicate – remove and clean systems
- Recover – from backups

What is the Future of Malvertising?

- Advances in security systems
- Personalization – good for marketers – good for criminals
- Use of Artificial Intelligence for attacks and defense

Stay safe out there

Gene Gusman
gene.gusman@experian.com