The Hidden Enemy: Malvertising and Ransomware

Brian Henger – Regional Vice President
Dear Employees,

Don’t click that!

Warm Regards,

The Security Team
Malvertising (n)

Malicious advertising is the use of online advertising to distribute malware (or scams) with little or no user interaction required.

And now a Short History Lesson...
First noticed on Myspace and Rhapsody using Adobe Flash
Click-fraud scam on the **NY Times** website

|------|------|------|------|------|------|------|------|

2009
2.5x increase from previous year
Ads from Spotify serve malware that DOES NOT NEED THE USER TO CLICK!

2011
LA Times was hit by a massive malvertising attack which used the Blackhole exploit kit to infect users.
A campaign targeting **Yahoo** infected machines with **Banker Trojans**
In its effort to battle malvertising, Google disabled more than **524 million bad ads** and banned **thousands of advertisers**

2014
Comparing the first half of 2015 to ALL of 2014 malvertising increased by 260%*

450,000 compared to 250,000*

First Half of 2015

*according to RiskIQ
According to Google, in 2015 they disabled more than 780 million ads, an almost 50% increase from 2014.
Some Examples
Malvertising attacks can also lead to Scams
How Does It Work?

• Advertisers sign up with an advertising network
• Advertisers bid in real time to get their ads selected
• Bad Actors will serve out good ads for a while before they switch to malverts
• Ads and advertising space is increasingly being transacted programmatically
• Billions of ads are displayed to users in real-time
- Ads are displayed in real time
- Ads are targeted to user profiles
- Billions of impressions every day
- 3rd-party advertisers can play

Advertisers love this stuff:

But it opens the door for:
- Real-time brings opportunistic attacks
- The Malware can “target” too
- Bad actors can hide in the complexity
- Difficulty in tracking down offenders
How Bad Actors Get Onto Good Websites:

- Not all ad networks have strict criteria for advertisers
- An “impression” can go through many intermediaries
- Sellers don’t always know the buyers
- Some ad platforms allow newcomers in cheap!
Some Ad Platforms Allow Newcomers in Cheap!

Very quick campaign approval
Your campaign can be on air in less than 10 minutes!

Guaranteed Success  Daily Payments  Full Control  Refferal System  Quick Approval

I want to advertise through PopCash.Net. What is the minimum deposit?

The minimum deposit is only $5, but we don't have any set minimum budget limits for individual campaigns. With $5 you can create multiple campaigns.
Some Technical Stuff
Using Adobe’s Flash to Deliver Exploits

- Flash is a ubiquitous plugin that renders graphics and animations
- Heavily used by the ad industry
- Flash has zero-day vulnerabilities that can be exploited
- When the ad loads, so does the exploit!!!
Vulnerabilities By Year

The graph shows the number of vulnerabilities by year:
- 2005: 1 vulnerability
- 2006: 5 vulnerabilities
- 2007: 10 vulnerabilities
- 2008: 21 vulnerabilities
- 2009: 20 vulnerabilities
- 2010: 60 vulnerabilities
- 2011: 63 vulnerabilities
- 2012: 66 vulnerabilities
- 2013: 56 vulnerabilities
- 2014: 76 vulnerabilities
- 2015: 314 vulnerabilities
- 2016: 105 vulnerabilities

The chart indicates a significant increase in vulnerabilities in 2015 and 2016 compared to previous years.
The Ad Can Give Us Lots of Data

- Domain
- Campaign ID
- Affiliate ID
- Real-time-buy info
- Actual ad content

SSL obfuscates all that good data!
How Malware uses “fingerprinting”

• Malware authors want to target victims of interest, and foil research labs

• Fingerprinting code prevents malware from running on machines that are:
  • Virtual Machines
  • Connected to a VPN
  • Running certain advanced security products

• Some security products can detect when they are being fingerprinted (and use this as a “suspicious indicator”)

• So now malvertising is changing to camouflaged its fingerprinting!
POP QUIZ: Where is the fingerprinting code?

Dear Edward Snowden,

there’s still a lot
to uncover.

blush®
LINGERIE

© Blush Berlin
vaea = 'malwar~1/',
clh = arguments[0],
trm = 'kasper~1/',
oft = 'trendm~1/',

http://3A2F%2Fcon.texto-meta.com%2Fcivil%2Fviewforum.php%3F
Will malvertising affect me?
Do Your People Go To These Sites?

- There was a huge malvert attack recently
- Malvert ads were served to many high-profile sites
- These ads were delivering ransomware!

<table>
<thead>
<tr>
<th>Publisher</th>
<th>Traffic (monthly)*</th>
</tr>
</thead>
<tbody>
<tr>
<td>msn.com</td>
<td>1.3B</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>313.1M</td>
</tr>
<tr>
<td>bbc.com</td>
<td>290.6M</td>
</tr>
<tr>
<td>aol.com</td>
<td>218.6M</td>
</tr>
<tr>
<td>my.xfinity.com</td>
<td>102.8M</td>
</tr>
<tr>
<td>nfl.com</td>
<td>60.7M</td>
</tr>
<tr>
<td>realtor.com</td>
<td>51.1M</td>
</tr>
<tr>
<td>theweathernetwork.com</td>
<td>43M</td>
</tr>
<tr>
<td>thehill.com</td>
<td>31.4M</td>
</tr>
<tr>
<td>newsweek.com</td>
<td>9.9M</td>
</tr>
</tbody>
</table>

* Numbers pulled from SimilarWeb.com.
Millions menaced as ransomware-smuggling ads pollute top websites

msn.com, nytimes.com, aol.com et al. hit by malware-injecting banners

15 Mar 2016 at 17:19, John Leyden

Top-flight US online publishers are serving up adverts that attempt to install ransomware and other malware on victims' PCs.
What can I do?

- Keep your software patched
- Remove software you don’t use
- Run the latest browsers
- Keep your anti-malware software up to date
- Run an effective anti-exploit technology
- Train your staff on good security practices
Delivering The Payload: Ransomware
Ransomware (n)

Malware that will encrypt or lock all personal files, and then demand payment of the “ransom” to decrypt or unlock them.
Hi Rebecca!

I left you a voicemail earlier but I thought I would reach out and give you a little more information to what I was thinking about how we could work together...

I work for CSLFR which is the fastest growing team in the NASCAR Sprint Cup Series... Recently last week our crew chief of our team was hit with a ransom virus and his computer which holds tens of millions of dollars worth of data was corrupted and we were forced to pay the ransom... Our team was fully exposed and this was a very scary time to say the least!
Ransomware Landscape

- 96% of US companies aren’t very confident in their defenses for stopping ransomware
- 80% of orgs were victims of a cyberattack in last year, 50% were victims of ransomware attacks
- Most heavily targeted industries for ransomware are healthcare and financial services
- 1 in 4 ransomware attacks targeted senior executives and the C-Suite
- 50% of corporate decision makers consider ransomware to be a “concern” or “extreme concern”
- Globally, nearly 40% of ransomware victims paid the ransom

Source: Osterman Research, July 2016
Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay $300 USD / 300 EUR / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Ransom: $500 to $1,000

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)
2. Purchasing Bitcoins - Although it’s not yet easy to buy bitcoins, it’s getting simpler every day. Here are our recommendations:
   - LocalBitcoins.com - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
Modern Ransomware

- The encryption is **nearly impossible to crack**
- If you don’t have **backups**, the **only** way of getting your files back is to **pay the ransom**
- Are there **decryptors**? Not anymore...
AES Symmetric Key (different for each file)

Encrypt the File

Encrypt the File’s Key

RSA Public Key from Master (Asymmetric Key)

Original File

Encrypted File

Encrypted Key + File
Ransomware Detection: A behavioral approach
The 4-step process

Step 1: Detect
- Constantly look for ransomware behaviors. When detected...

Step 2: Arrest
- Immediately halt the encryption process, and then...

Step 3: Remove
- Track down the ransomware and delete it, then...

Step 4: Remediate
- Restore any encrypted files (usually a manual process)
Step 1: Detecting Ransomware
A Primer on Processes and Threads

Open file
Read the file
Close the file
Download something
Update the screen
Wait for a keystroke
...
...
...

Process X

Thread

Code

Code

Code

Code

Nice Code 😊
Some Processes Have Only a Few Threads
Some Windows Programs Use LOTS of Threads

<table>
<thead>
<tr>
<th>Name</th>
<th>PID</th>
<th>Status</th>
<th>User Name</th>
<th>CPU</th>
<th>Memory</th>
<th>Threads</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skype.exe</td>
<td>8316</td>
<td>Running</td>
<td>mpatton</td>
<td>00</td>
<td>128,612 K</td>
<td>86</td>
<td>Skype</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>5772</td>
<td>Running</td>
<td>mpatton</td>
<td>00</td>
<td>59,976 K</td>
<td>86</td>
<td>Windows Explorer</td>
</tr>
<tr>
<td>Spotify.exe</td>
<td>7216</td>
<td>Running</td>
<td>mpatton</td>
<td>02</td>
<td>49,484 K</td>
<td>70</td>
<td>Spotify</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>988</td>
<td>Running</td>
<td>SYSTEM</td>
<td>00</td>
<td>25,700 K</td>
<td>49</td>
<td>Host Process for Windows S</td>
</tr>
<tr>
<td>BoxSync.exe</td>
<td>7864</td>
<td>Running</td>
<td>mpatton</td>
<td>00</td>
<td>138,788 K</td>
<td>48</td>
<td>Box Sync</td>
</tr>
<tr>
<td>chrome.exe</td>
<td>9220</td>
<td>Running</td>
<td>mpatton</td>
<td>00</td>
<td>177,204 K</td>
<td>48</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>OUTLOOK.EXE</td>
<td>8460</td>
<td>Running</td>
<td>mpatton</td>
<td>00</td>
<td>78,444 K</td>
<td>44</td>
<td>Microsoft Outlook</td>
</tr>
<tr>
<td>PowerPoint.exe</td>
<td>4884</td>
<td>Running</td>
<td>mpatton</td>
<td>00</td>
<td>123,084 K</td>
<td>41</td>
<td>Microsoft PowerPoint</td>
</tr>
<tr>
<td>iCloudDrive.exe</td>
<td>8604</td>
<td>Running</td>
<td>mpatton</td>
<td>00</td>
<td>9,796 K</td>
<td>41</td>
<td>iCloud Drive</td>
</tr>
<tr>
<td>mbam.exe</td>
<td>5624</td>
<td>Running</td>
<td>mpatton</td>
<td>00</td>
<td>29,984 K</td>
<td>40</td>
<td>Malwarebytes Anti-Malware</td>
</tr>
<tr>
<td>VISIO.FXF</td>
<td>3156</td>
<td>Running</td>
<td>mpatton</td>
<td>00</td>
<td>124,984 K</td>
<td>37</td>
<td>Microsoft Visio</td>
</tr>
</tbody>
</table>
What a Ransomware Process and Thread Does

Find all the PHOTO files
Encrypt them
Rename them
Destroy the originals

Find all the .DOC files
Encrypt them
Rename them
Destroy the originals

Delete all the backups!
Delete all the restore points!
Using “Behavior” to Look For Ransomware

- Watch all the threads in every process, looking for ransomware behaviors
- Some behaviors are more “suspicious” than others
- If too many of these happen, triggers a detection!
## Detecting Ransomware by its Behavior

<table>
<thead>
<tr>
<th>Suspicious Behaviors</th>
<th>Bad Behaviors</th>
<th>Really Bad Behaviors!!</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Deleting a file</td>
<td>• Deleting the “Volume Shadows”</td>
<td>• Looking for encryption keys</td>
</tr>
<tr>
<td>• Writing new data to a file</td>
<td>• Stopping the Volume Shadow Service</td>
<td>• Runs encryption command line</td>
</tr>
<tr>
<td>• Renaming a file</td>
<td>• Deleting Restore Points</td>
<td>• Registry operations that indicate encryption</td>
</tr>
<tr>
<td></td>
<td>• Using a “File Wipe” utility</td>
<td>• Encrypting a file!</td>
</tr>
<tr>
<td></td>
<td>• Supersede a file (e.g. change from .XLS to something else)</td>
<td></td>
</tr>
</tbody>
</table>
Step 2: Arresting the Encryption Process
Arresting the Encryption Process (The easiest step!)

Find all the PHOTO files
- Encrypt them
- Rename them
- Destroy the originals

Find all the .DOC files
- Encrypt them
- Rename them
- Destroy the originals

Delete all the backups!
Delete all the restore points!
Step 3:
Removing the Ransomware, and why that is harder than it looks.

(but first, a short lesson)
Threads can “inject” threads into other processes? What?!!
Threads can start processes and THEN “inject” threads?
An “Injection Chain”
Ransomware uses “Injection Chains” to hide itself from detection
The Even Harder Part: CryptoWall 4 Techniques for Evasion – Code Injection
The Even Harder Part: CryptoWall Injection Chain

Cryptowall

Launch (Suspended)

Code Injection

explorer.exe

Launch (Suspended)

Code Injection

svchost.exe

Attack!

Photos
To track down and remove the actual instigator, anti-ransomware programs must keep records of all the processes, threads and injections.
Step 4: Remediate
Remediation and the Aftermath

• Restore from Backup

• Delete the encrypted files from the Backup History
  • And BTW, make sure you have History enabled!

• Root-cause analysis

• Review file and server read/write permissions

• Review security technology (esp. Firewall)

• Train your staff
The Villain of the Piece:

Vulnerabilities
Vulnerability (n):

A flaw or weakness in software that could be exploited to violate the system's security policy.
Malware delivered through vulnerabilities (Malwarebytes Labs)

- 2013: 35%
- 2014: 65%
- 2015: 80%
From a study done by the ICT institute in The Netherlands, based on CVE data.
Where do all these Vulnerabilities come from?

The people who wrote the code!
Vulnerabilities by Vendor (2015, from CVE)
About Malwarebytes
Crushes Malware. Restores Confidence.

Founded in 2008, 400+ employees focused on the “Infection Landscape.”

Malwarebytes is the global standard for complete malware removal.

Malwarebytes’ agile research team keep our customers in the fight against malware.

We don’t just remove threats, we prevent them—stopping data breaches before they happen.
Trusted by Millions

70,000+
Businesses protected

750,000,000
IT hours saved

605,000
Threats blocked every hour

280,000,000+
Endpoints protected

Disney
Dole
Samsung
Vermeer

Malwarebytes
Malware poses the largest risk on Zero Day, when little or no defenses exist for the new threat. With an average dwell time of 200+ days, most security companies fall short of addressing new threats. Malwarebytes ends that threat, delivering true zero-day protection that most endpoints are lacking.

Why Now? Why Us?

Malwarebytes reduces the level of risk, not by competing with the services of other parties, but by leading the answer.
How Malwarebytes Can Help:

**Multi-layered protection against malware, including ransomware**

Detecting and stopping advanced threats throughout the attack chain:

- **Profiling** – fingerprinting detection and application hardening
- **Delivery** – web blocking prevents access to phishing and malicious websites
- **Exploitation** – signature-less exploit mitigation prevents shellcode execution
- **Payload Execution** – signature-less app behavior protection, advanced heuristics
- **Malicious Behavior** – signature-less ransomware behavior monitoring, C&C blocking, remediation engine
How Malwarebytes Can Help: Advanced threat removal

Malwarebytes BREACH REMEDIATION

Desktops + Laptops

Data Center + Cloud Servers

Security & Management Tools
Let’s Take Your Questions

Learn More: malwarebytes.com/business

Latest News: blog.malwarebytes.com

Request a Trial: malwarebytes.com/business/licensing
Thank You!