



The Hidden Enemy: Malvertising and Ransomware

Brian Henger
Regional Vice President

 Malwarebytes

 HIMSS[®]

CENTRAL & SOUTHERN OHIO *Chapter*

Overview

This session will provide a better understanding of the impact of malvertising and ransomware. It will also tackle some of the biggest misconceptions, latest tactics/incidents, how these attacks are delivered, and why your organization may be at risk without you even knowing it.

Key takeaways include:

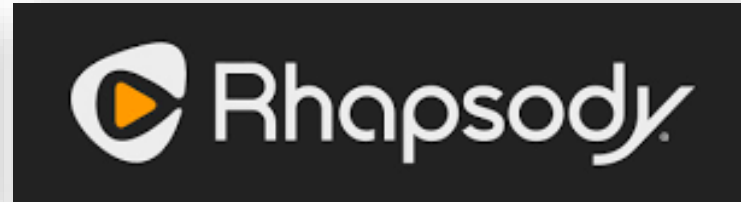
- The growth in malvertising and malvertising-based ransomware
- A better understanding of the tactics and techniques cybercriminals use to deliver and cover up their malvertising campaigns
- Tools and solutions to help detect, eliminate, and protect your business



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**

2007





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.

2012



The image shows the classic Yahoo! logo, which consists of the word "YAHOO!" in a white, bold, sans-serif font with a slight shadow effect, set against a solid purple rectangular background.

A campaign targeting **Yahoo** infected machines with **Banker Trojans**

2013

2007

2009

2011

2012

2013

2014

2015

2015

himss

CENTRAL & SOUTHERN OHIO Chapter



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 Google, in 2015 they disabled more than **780 million ads**, an almost **50% increase** from 2014.

2015



Some Examples

VIRTUAL DJ

VIRTUAL DJ

An excellent tool for DJ-mixing by newbies

HIM

CENTRAL & SOUTHERN O

AdChoices

lost.fm

Music search

Metallica

thrash metal metal heavy

xHamster

just porn, no bullshit

Search

Video Login

Video Live Cams Pictures Dating Stories Premium

Recommended Videos Categories HD Videos Top Rated Mobile Videos Upload Your

Sophia - Hot Blonde Want A Rough Ride

Malwarebytes Anti-Exploit

Malwarebytes Anti-Exploit blocked an exploit attempt

Application:	Internet Explorer (and add-ons)
Protection Layer:	Protection Against OS Security Bypass
Protection Technique:	Exploit Stack Pivoting attempt blocked
File/Process Blocked:	N/A
Attacking URL:	N/A

Malwarebytes ANTI-EXPLOIT

HERMÈS PARIS

> ON YOUR MARKS...

Malwarebytes Anti-Exploit

Malwarebytes Anti-Exploit has blocked an exploit attempt

Application:	Internet Explorer (and add-ons)
Protection Layer:	Protection Against OS Security Bypass
Protection Technique:	Exploit ROP gadget attack blocked
File/Process Blocked:	N/A
Attacking URL:	N/A

Malwarebytes ANTI-EXPLOIT

Close

WORK LESS MAKE MORE

Malvertising Attacks Can Also Lead to Scams

Google youtube

Web Videos News Images Books More Search tools

About 7,760,000,000 results (0.41 seconds)

AdWords

Youtube Channel
Ad www.youtube.com/
Watch Youtube Television Channel Browse News Channel on Youtube

YouTube.com - Youtube Channel
Ad www.youtube.com/
Watch Youtube Channel 360Videos Browse Hundreds Of Youtube Videos

YouTube
www.youtube.com/
Share your videos with friends, family, and the world.

Results from youtube.com

Youtube subscriptions
One account. All of Google. Sign in to continue to YouTube. Email ...

Music
YouTube's music destination featuring top tracks and popular ...

You Tube

Movies
YouTube Movies (United States).

PopularOnYouTube
The pulse of what's popular on YouTube. Check out the latest ...

History
Watch history. Search history. Clear

Parent organization: Google
Founders: Chad Hurley, Steve Chen, Jawed Karim

Profiles
Facebook Twitter Google+ Instagram LinkedIn

Feedback

0x000000CE DRIVER_UNLOADED_WITHOUT_CANCELLING_PENDING_OPERATIONS

WINDOWS HEALTH IS CRITICAL
DO NOT RESTART

PLEASE CONTACT MICROSOFT TECHNICIANS

BSOD : Error 333 Registry Failure of Operating system - Host : BLUE SCREEN ERROR 0x000000CE

Please contact Microsoft Technicians At Toll Free :
1-844-396-3227

To Immediately Rectify issue to prevent Data Loss

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



Pro's

Advertisers love this stuff:

- Ads are displayed in real time
- Ads are targeted to user profiles
- Billions of impressions every day
- 3rd-party advertisers can play

Con's

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 then 10 minutes!

Popcash
The Popunder Network

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

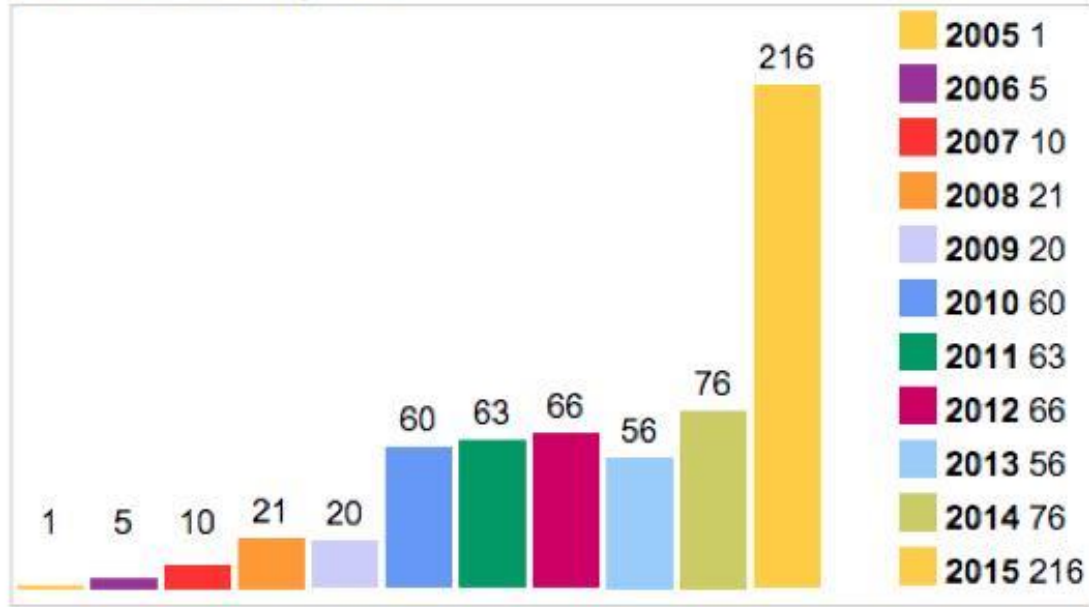
Using Adobe's Flash to Deliver Exploits



- 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 Ad Can Give Us Lots of Data

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

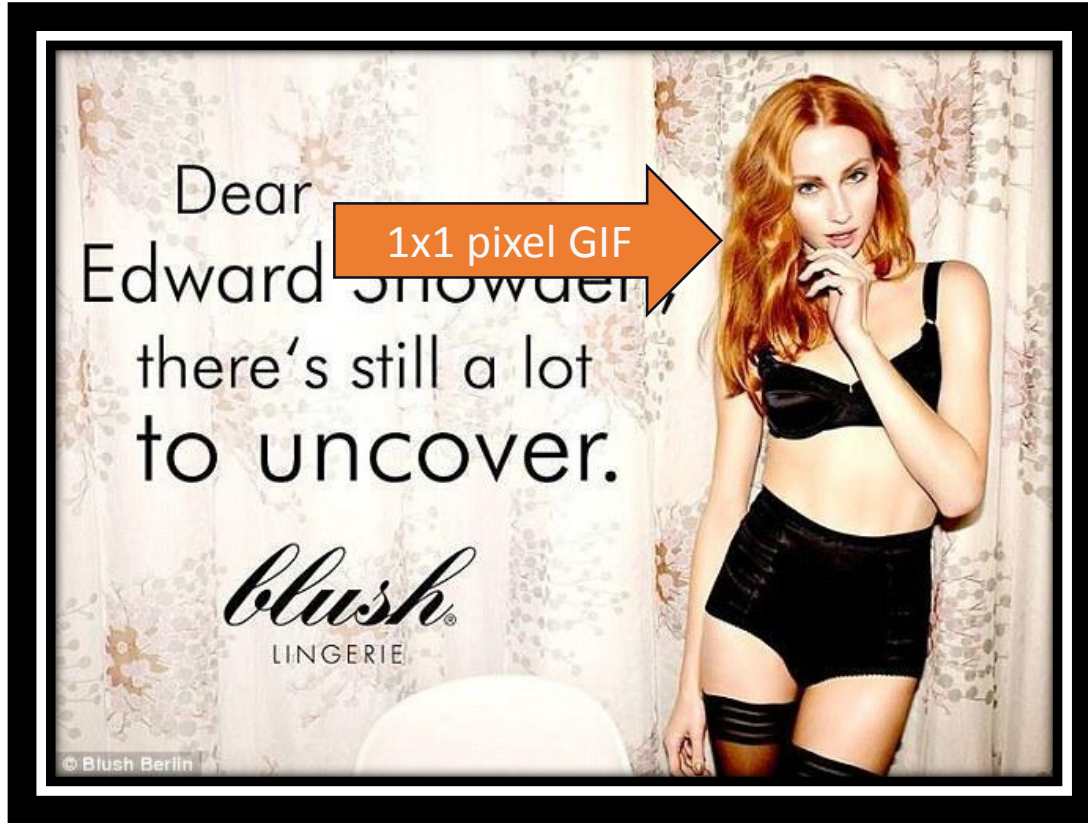


How Malware Uses “Fingerprinting”



- 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?





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

<http://3A%2F%2Fcon.texto-meta.com%2Fcivis%2Fviewforum.php%3F>

Will malvertising affect me?



CENTRAL & SOUTHERN OHIO *Chapter*

Do Your People Go To These Sites?

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

Publisher	Traffic (monthly)*
msn.com	1.3B
nytimes.com	313.1M
bbc.com	290.6M
aol.com	218.6M
my.xfinity.com	102.8M
nfl.com	60.7M
realtor.com	51.1M
theweathernetwork.com	43M
thehill.com	31.4M
newsweek.com	9.9M

** Numbers pulled from SimilarWeb.com.*

Security

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



157



265

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.



CBCnews | Technology & Science

Home

World

Canada

Politics

Business

Health

Arts & Entertainment

Technology & Science

Trending

Video

Technology & Science

Quirks & Quarks Blog

Spark

Photo Galleries

Hollywood hospital hit with ransomware only the latest in trend of monetizing cyberattacks

Hospitals vulnerable to malware attacks, as budgets typically prioritize medical equipment over IT

By Jonathan Ore, CBC News Posted: Feb 26, 2016 9:00 AM ET | Last Updated: Feb 26, 2016 9:56 AM ET



What recently happened to Hollywood Presbyterian Medical Center in Los Angeles may be part of a larger trend predicted for 2016: ransomware being used to target the medical sector, where lives can be put at risk. (Hollywood Presbyterian Medical Center/Facebook)

Related Stories

- Hollywood hospital

It sounds like the plot of a bad episode of *CSI*: hackers shutting down a hospital's computer network, locking down its ability to treat patients until a sky-high ransom is paid.

ADVERTISEMENT

Stay Connected with CBC News



Mobile



Facebook



Podcasts



Twitter



Alerts



Newsletter

Top News Headlines



- Canada's bill to legalize pot coming for spring 2017, minister tells UN

- Criminal charges laid against 3 officials in Flint's lead-tainted water crisis

- Fight over LGBT rights moves to the bathrooms of a nation: Neil Macdonald

- Star Fox Zero reboots classic franchise, but awkward controls cause turbulence

- First she took Manhattan, then Bernie's base? Clinton's goal after New York



[Home](#) > [Leadership and Management](#) > [Security](#)



SALTED HASH- TOP SECURITY NEWS

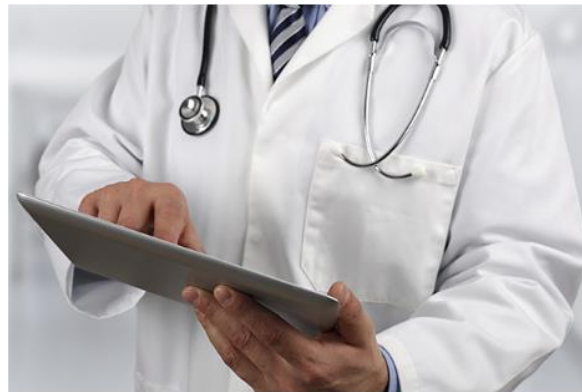
By [Steve Regan](#) | [Follow](#)

About

Fundamental security insight to help you minimize risk and protect your organization

NEWS

Ransomware attack hits MedStar Health, network offline



Credit: Thinkstock

Medical group forced to use paper and pen after suspected Ransomware attack

CSO | Mar 28, 2016 4:56 PM PT

MORE LIKE THIS



The FBI isn't wrong; sometimes you will have to pay the ransom



Ransomware: Pay it or fight it?

CryptoLocker's success will fuel future copycats

on IDG Answers

How to switch Samsung Galaxy from Sprint to AT&T?

Cryptolocker

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.

Private key will be destroyed on
10/9/2013
4:25 PM

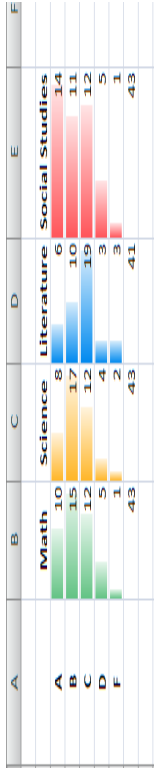
Time left
95 : 56 : 35

Next >>



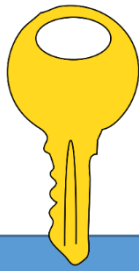
Modern Ransomware

- 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...



Original File

AES Symmetric Key
(different for each file)



Encrypt the File



Encrypted File

Encrypt the File's Key



RSA Public Key from Master
(Asymmetric Key)



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

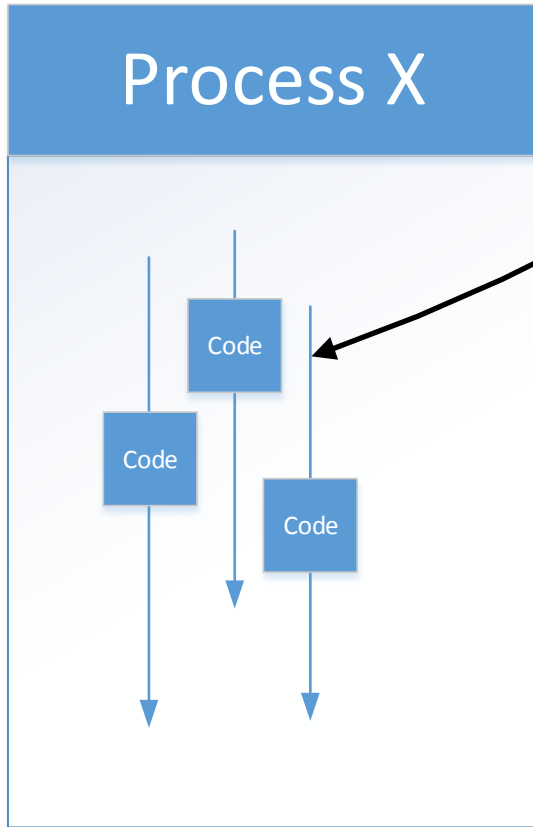
- Track down the ransomware and delete it, then...

Step 4: Remediate

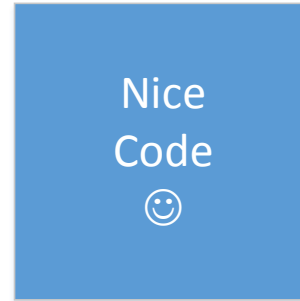
- Restore any encrypted files (usually a manual process)

Step 1: Detecting Ransomware

A Primer on Processes and Threads



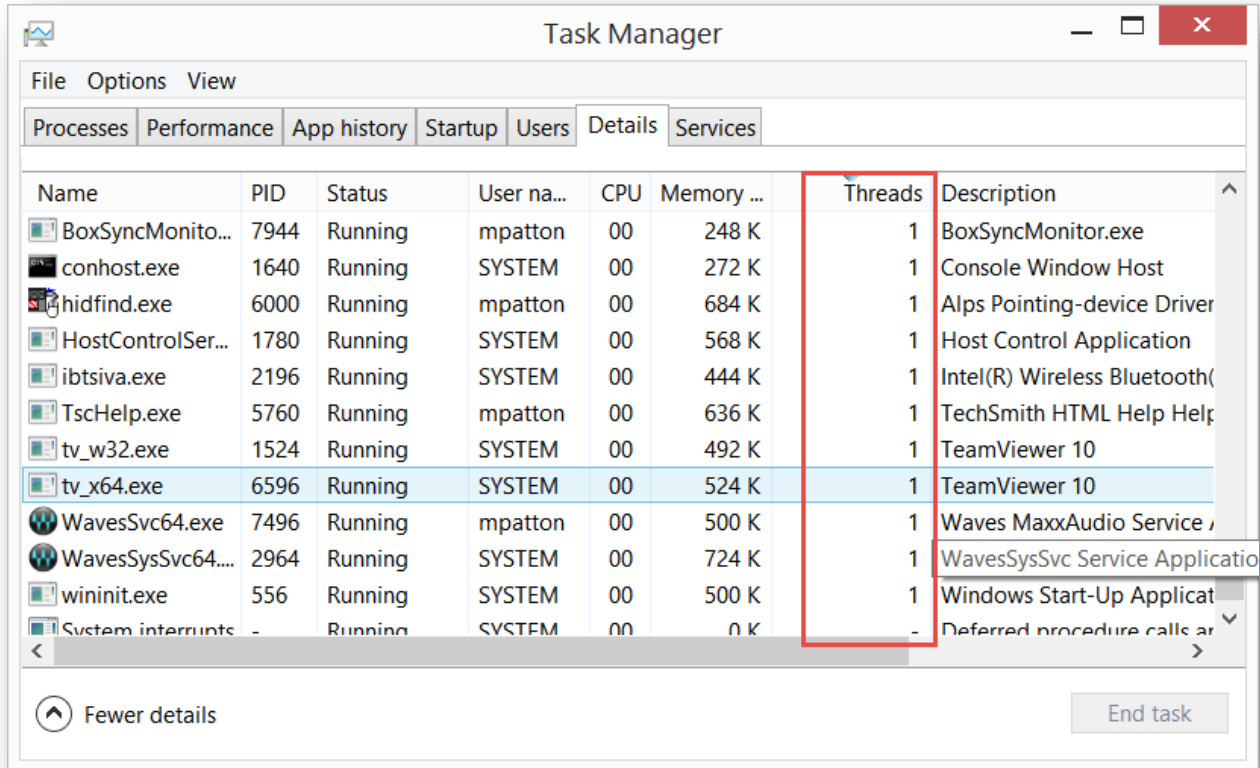
Thread



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

...
...
...

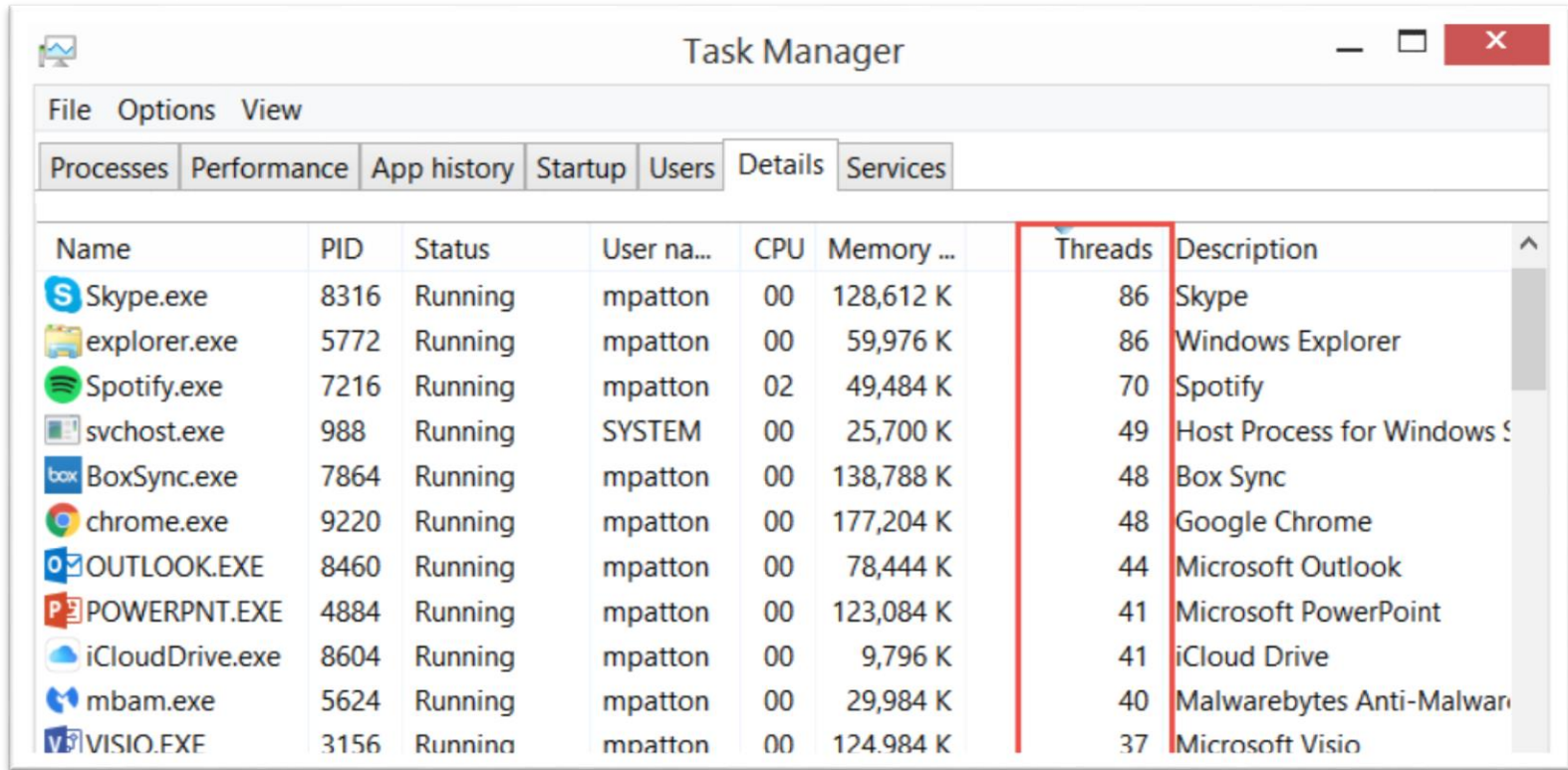
Some Processes Have Only a Few Threads



The screenshot shows the Windows Task Manager window with the 'Details' tab selected. A red rectangular box highlights the 'Threads' column in the process list. The list shows various running processes, including BoxSyncMonitor.exe, conhost.exe, hidfind.exe, HostControlSer..., ibtsiva.exe, TscHelp.exe, tv_w32.exe, tv_x64.exe, WavesSvc64.exe, WavesSysSvc64..., wininit.exe, and System interrupts. The 'Threads' column shows that most of these processes have only 1 thread, while 'System interrupts' has 0 threads.

Name	PID	Status	User na...	CPU	Memory ...	Threads	Description
BoxSyncMonito...	7944	Running	mpatton	00	248 K	1	BoxSyncMonitor.exe
conhost.exe	1640	Running	SYSTEM	00	272 K	1	Console Window Host
hidfind.exe	6000	Running	mpatton	00	684 K	1	Alps Pointing-device Driver
HostControlSer...	1780	Running	SYSTEM	00	568 K	1	Host Control Application
ibtsiva.exe	2196	Running	SYSTEM	00	444 K	1	Intel(R) Wireless Bluetooth(
TscHelp.exe	5760	Running	mpatton	00	636 K	1	TechSmith HTML Help Help
tv_w32.exe	1524	Running	SYSTEM	00	492 K	1	TeamViewer 10
tv_x64.exe	6596	Running	SYSTEM	00	524 K	1	TeamViewer 10
WavesSvc64.exe	7496	Running	mpatton	00	500 K	1	Waves MaxxAudio Service
WavesSysSvc64...	2964	Running	SYSTEM	00	724 K	1	WavesSysSvc Service Applicatio
wininit.exe	556	Running	SYSTEM	00	500 K	1	Windows Start-Up Applicat
System interrupts	-	Running	SYSTEM	00	0 K	-	Deferred procedure calls ar

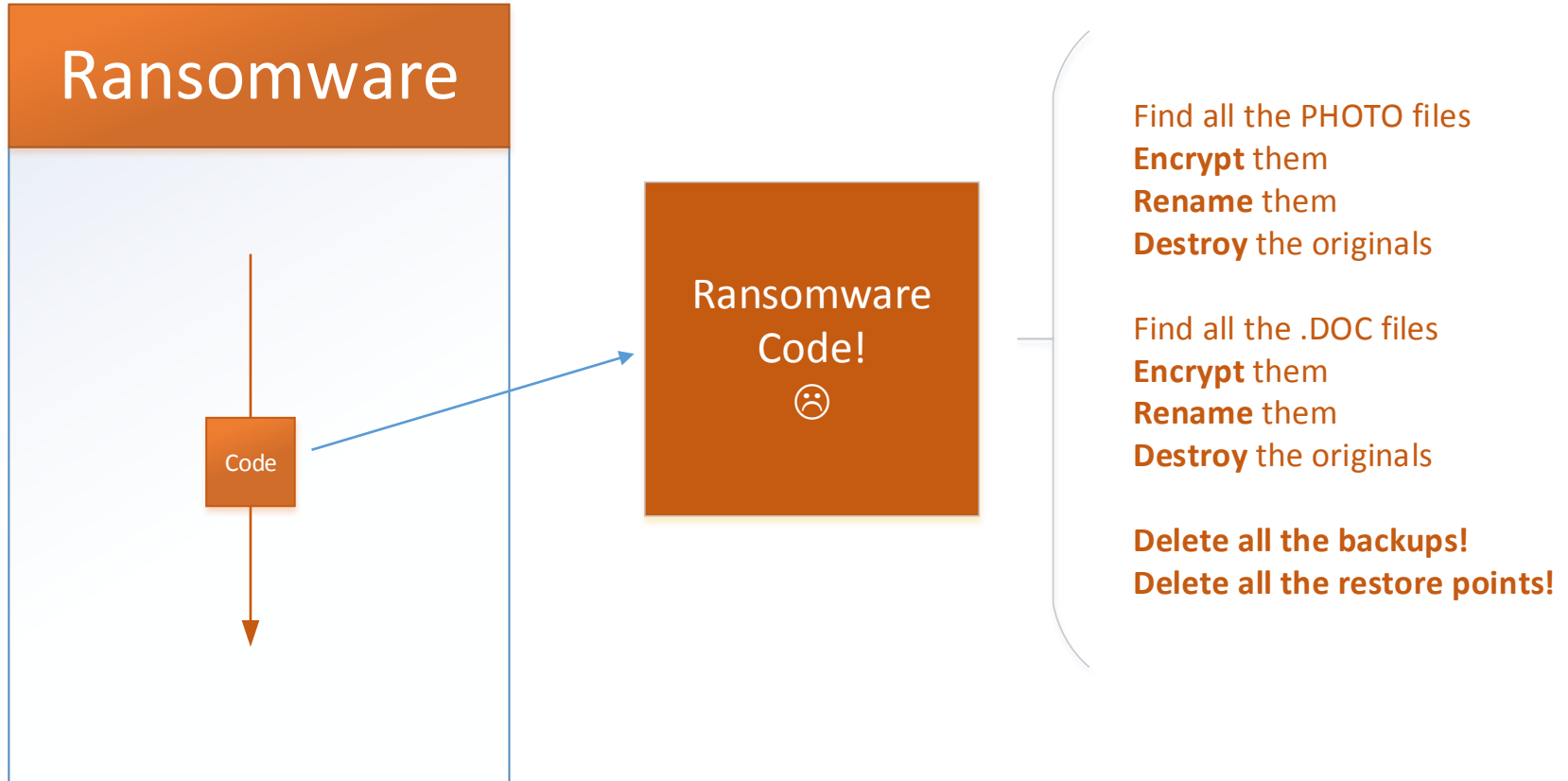
Some Windows Programs Use LOTS of Threads



The screenshot shows the Windows Task Manager window with the 'Details' tab selected. A red box highlights the 'Threads' column, which shows the number of threads for each process. The processes listed are: Skype.exe (86 threads), explorer.exe (86 threads), Spotify.exe (70 threads), svchost.exe (49 threads), BoxSync.exe (48 threads), chrome.exe (48 threads), OUTLOOK.EXE (44 threads), POWERPNT.EXE (41 threads), iCloudDrive.exe (41 threads), mbam.exe (40 threads), and VISIO.EXE (37 threads).

Name	PID	Status	User na...	CPU	Memory ...	Threads	Description
Skype.exe	8316	Running	mpatton	00	128,612 K	86	Skype
explorer.exe	5772	Running	mpatton	00	59,976 K	86	Windows Explorer
Spotify.exe	7216	Running	mpatton	02	49,484 K	70	Spotify
svchost.exe	988	Running	SYSTEM	00	25,700 K	49	Host Process for Windows S
BoxSync.exe	7864	Running	mpatton	00	138,788 K	48	Box Sync
chrome.exe	9220	Running	mpatton	00	177,204 K	48	Google Chrome
OUTLOOK.EXE	8460	Running	mpatton	00	78,444 K	44	Microsoft Outlook
POWERPNT.EXE	4884	Running	mpatton	00	123,084 K	41	Microsoft PowerPoint
iCloudDrive.exe	8604	Running	mpatton	00	9,796 K	41	iCloud Drive
mbam.exe	5624	Running	mpatton	00	29,984 K	40	Malwarebytes Anti-Malwar
VISIO.EXE	3156	Running	mpatton	00	124.984 K	37	Microsoft Visio

What a Ransomware Process and Thread Does



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

Suspicious Behaviors

- Deleting a file
- Writing new data to a file
- Renaming a file

Bad Behaviors

- Deleting the “Volume Shadows”
- Stopping the Volume Shadow Service
- Deleting Restore Points
- Using a “File Wipe” utility
- Supersede a file (e.g. change from .XLS to something else)

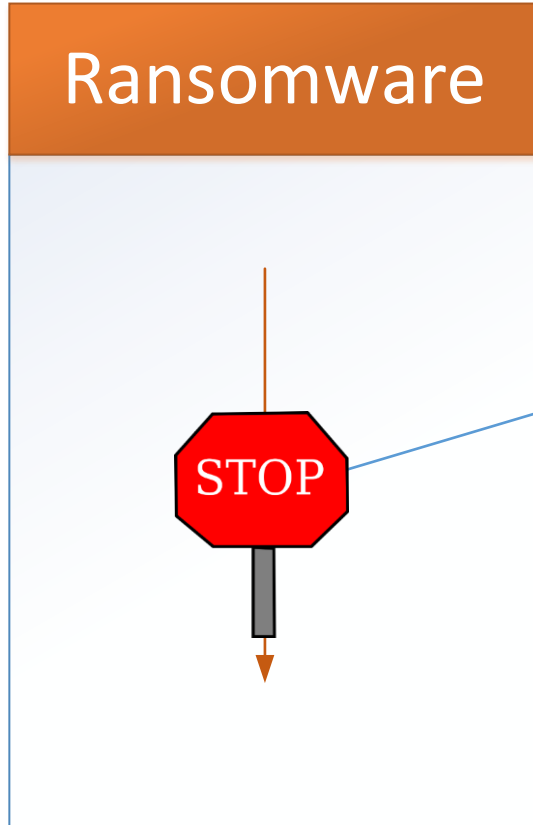
Really Bad Behaviors!!

- Looking for encryption keys
- Runs encryption command line
- Registry operations that indicate encryption
- **Encrypting a file!**

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!

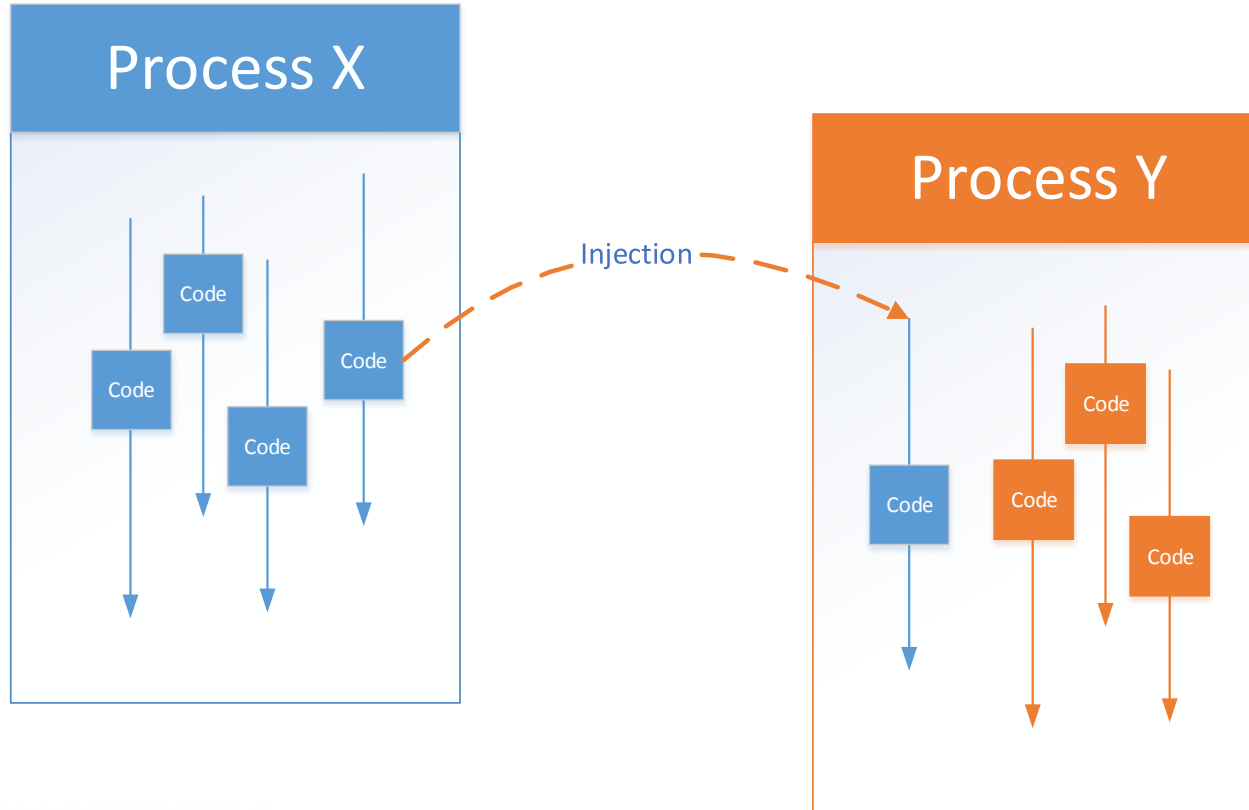
Step 3:

Removing the Ransomware, and why that is harder than it looks.

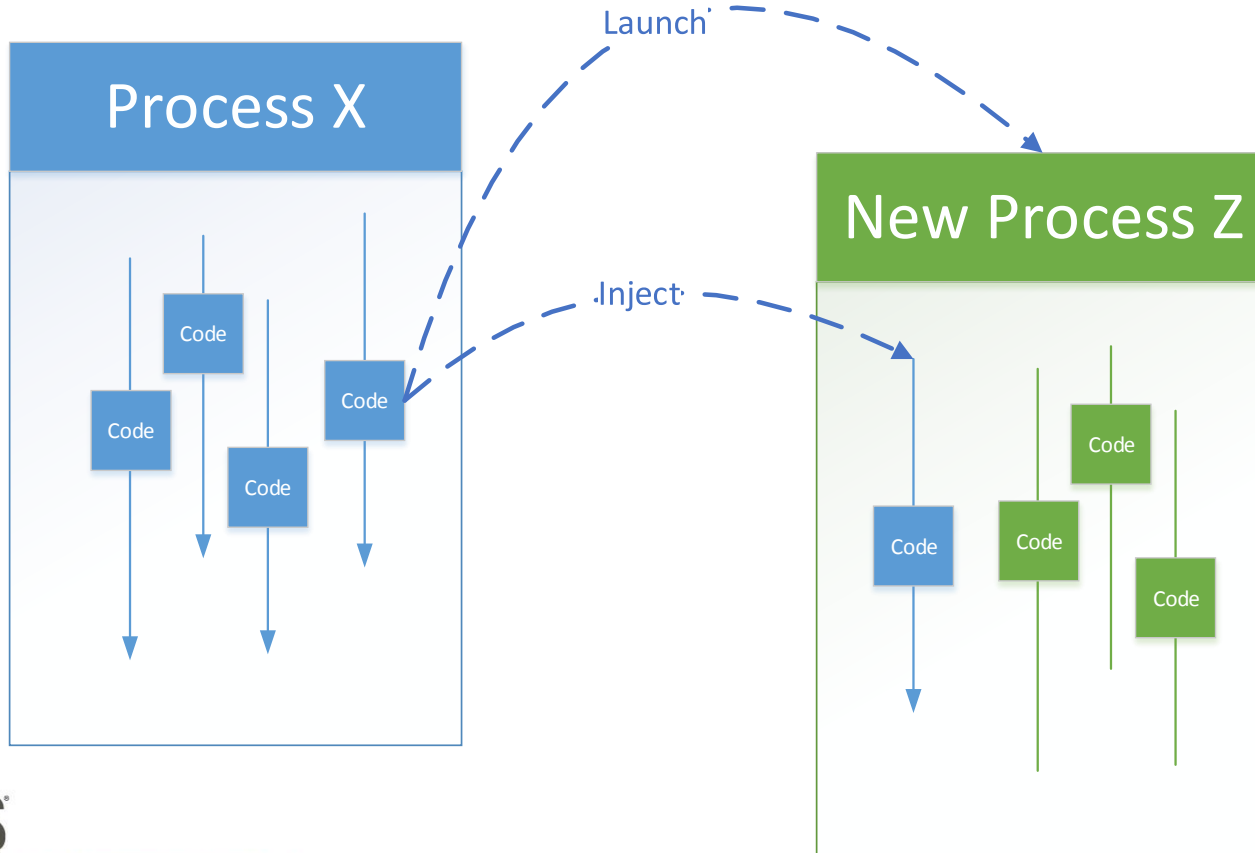
(but first, a short lesson)



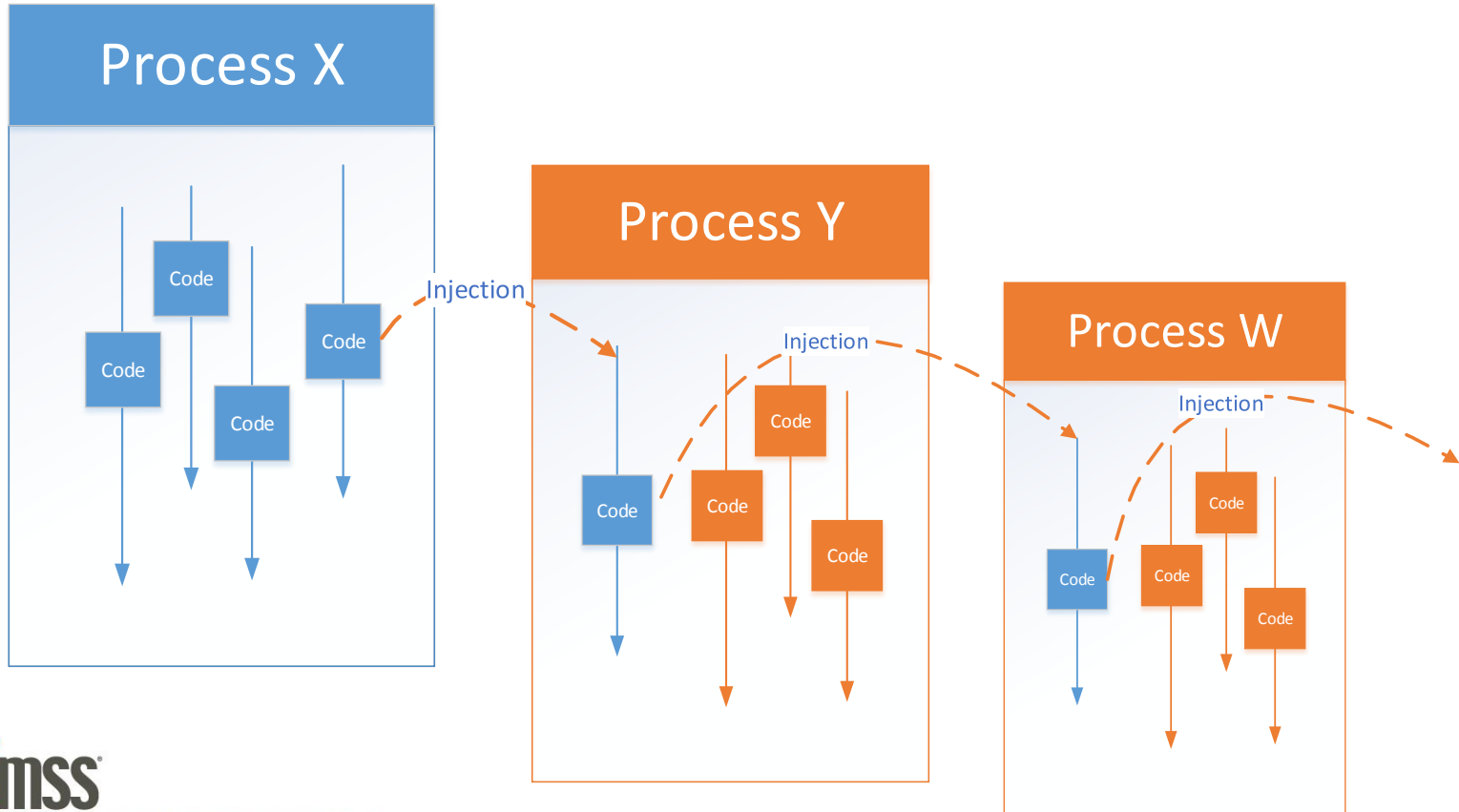
Threads Can “Inject” Threads into Other Processes? What?!!



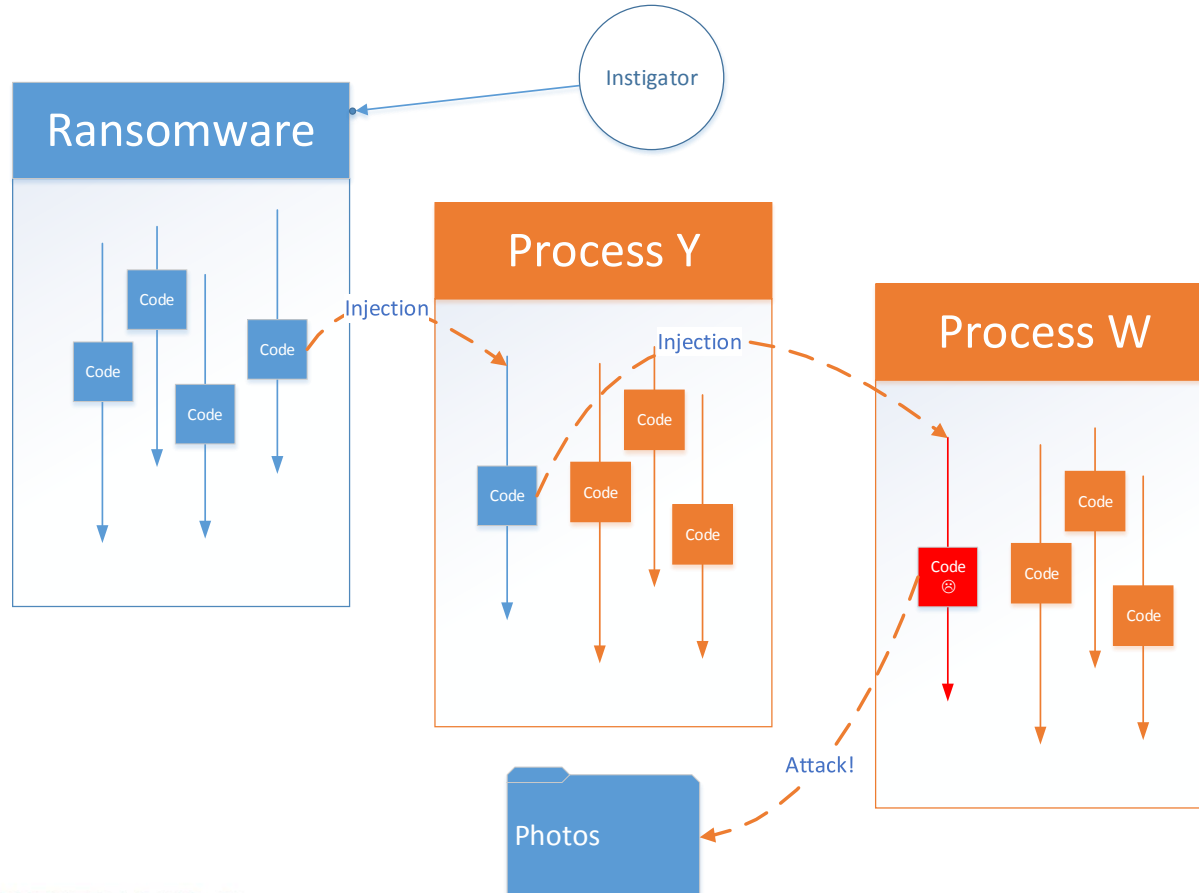
Threads Can Start Processes and THEN "Inject" Threads?



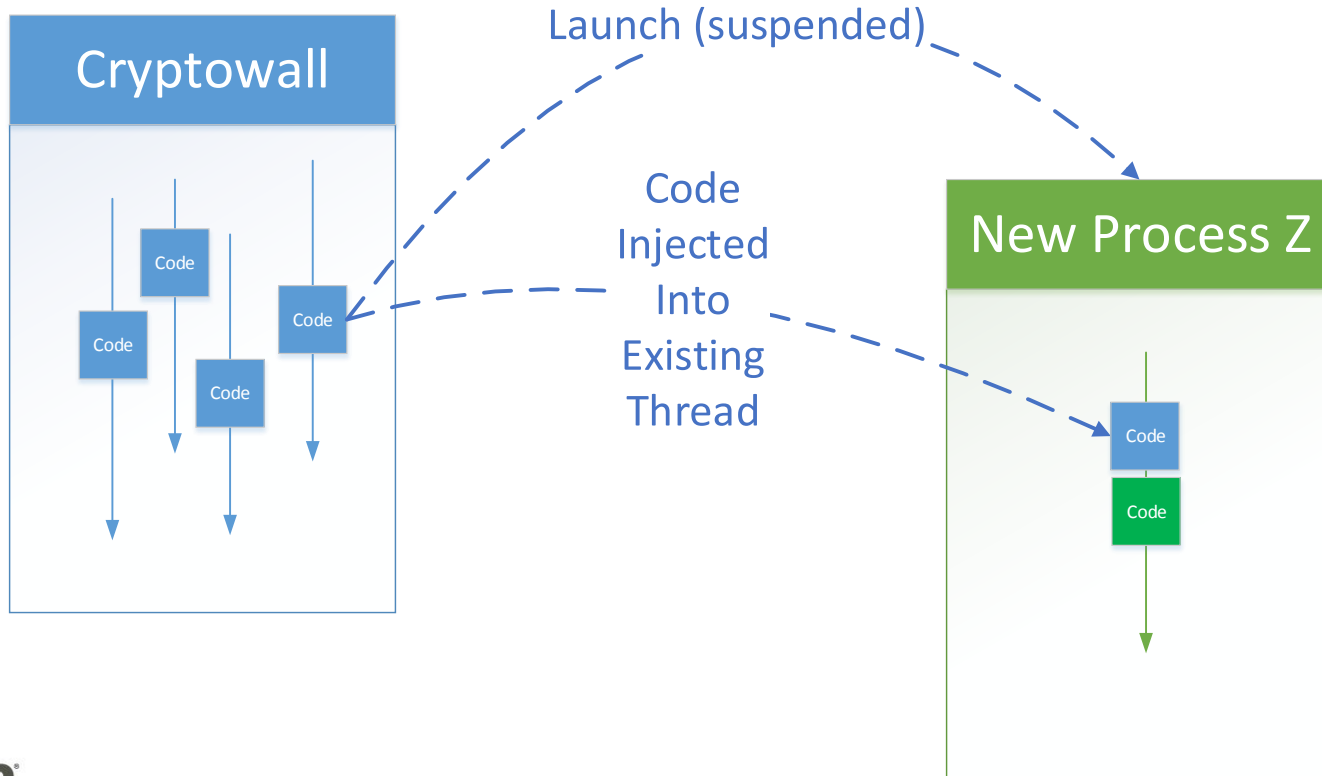
An "Injection Chain"



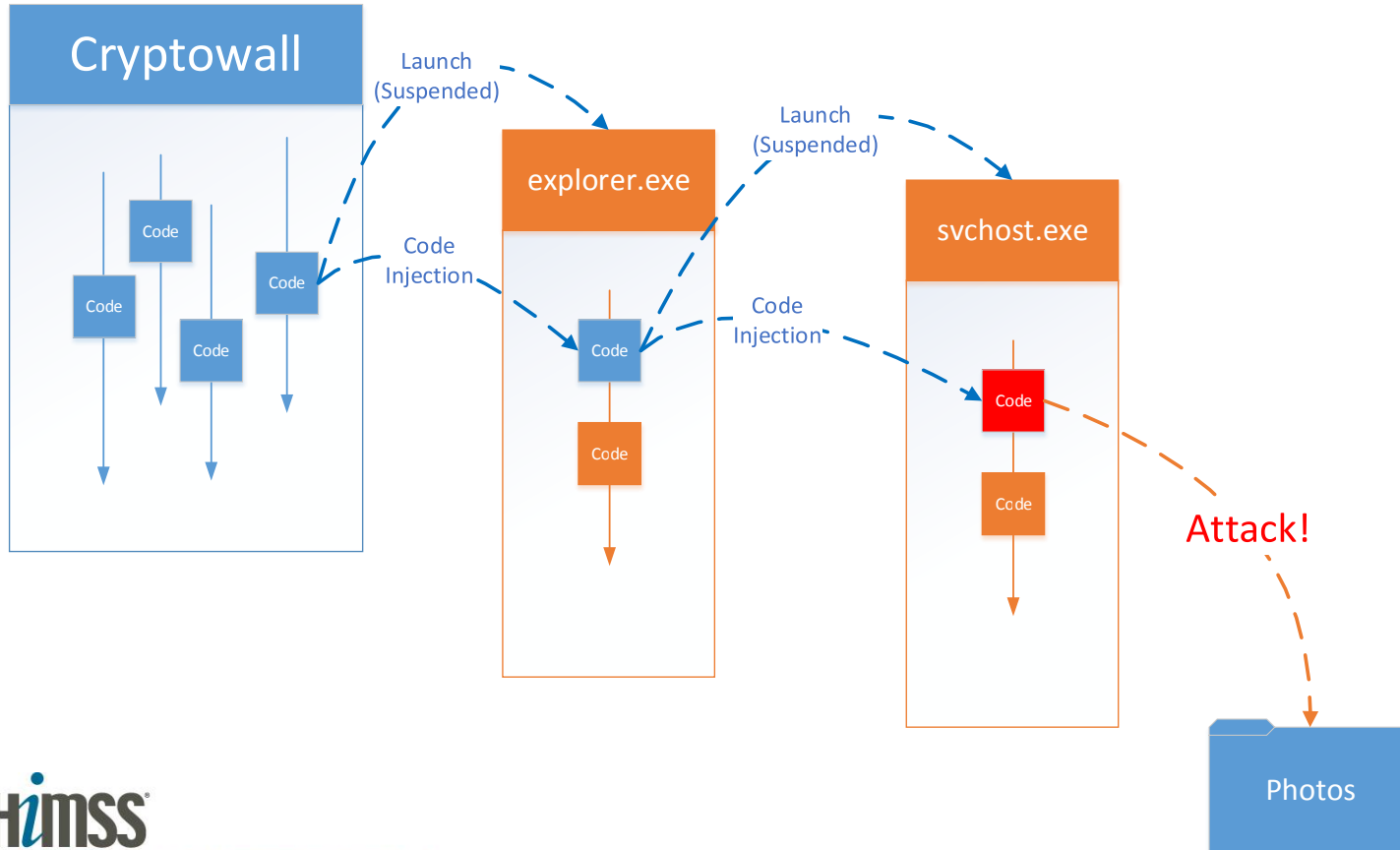
Ransomware Uses "Injection Chains" to Hide Itself from Detection



The Even Harder Part: CryptoWall 4 Techniques for Evasion – Code Injection



The Even Harder Part: CryptoWall Injection Chain



To **track down** and **remove** the
actual **instigator**,
anti-ransomware programs must
keep records of all the
processes, threads and
injections.

Step 4: Remediate



CENTRAL & SOUTHERN OHIO *Chapter*

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

About Malwarebytes

Crushes Malware. Restores Confidence.



Founded in 2008,
440+ 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.



CENTRAL & SOUTHERN OHIO Chapter

Trusted by Millions



10,000+

Businesses
protected



750,000,000

IT hours saved



605,000

Threats blocked
every hour



28,000,000+

Endpoints
protected

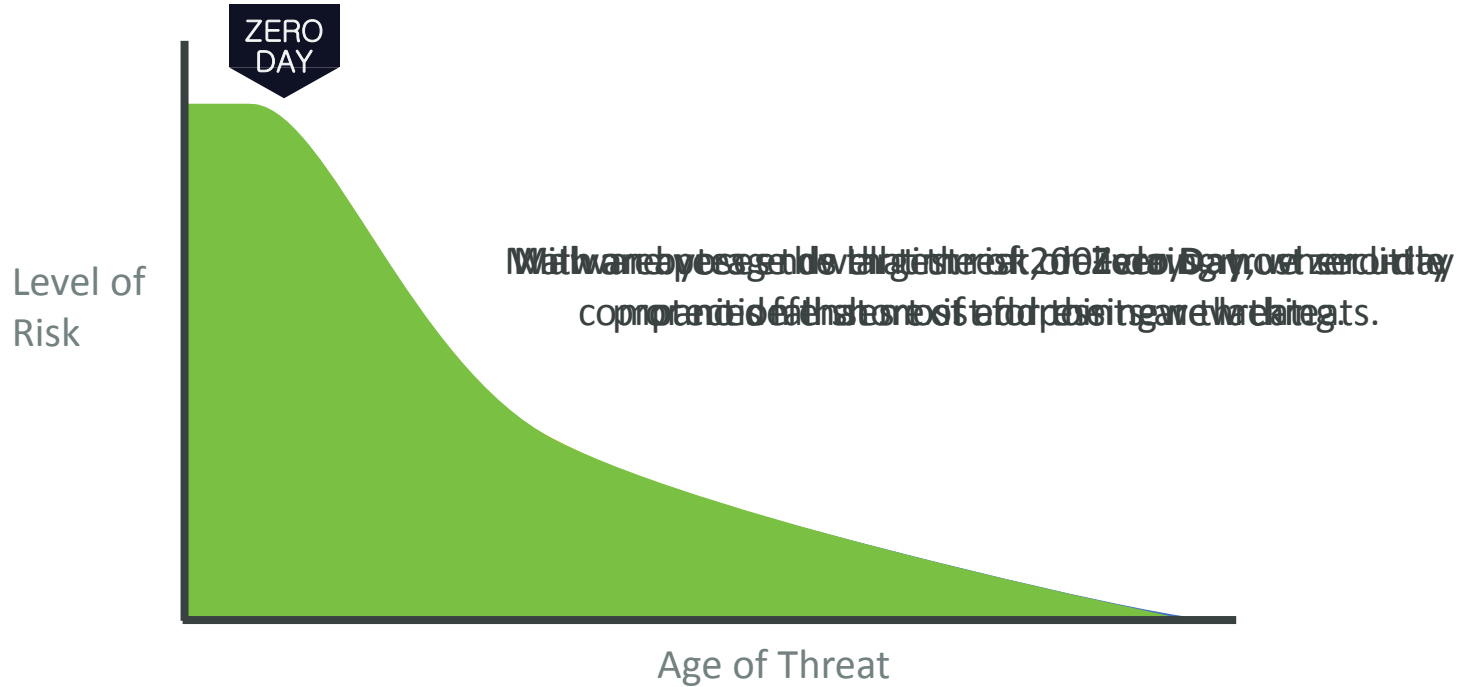


SAMSUNG



CENTRAL & SOUTHERN OHIO Chapter

Why Now? Why Us?



How Malwarebytes Can Help:

Multi-layered protection against malware, including ransomware



Malwarebytes

ENDPOINT SECURITY

Detecting and stopping advanced threats at every stage of the attack chain:

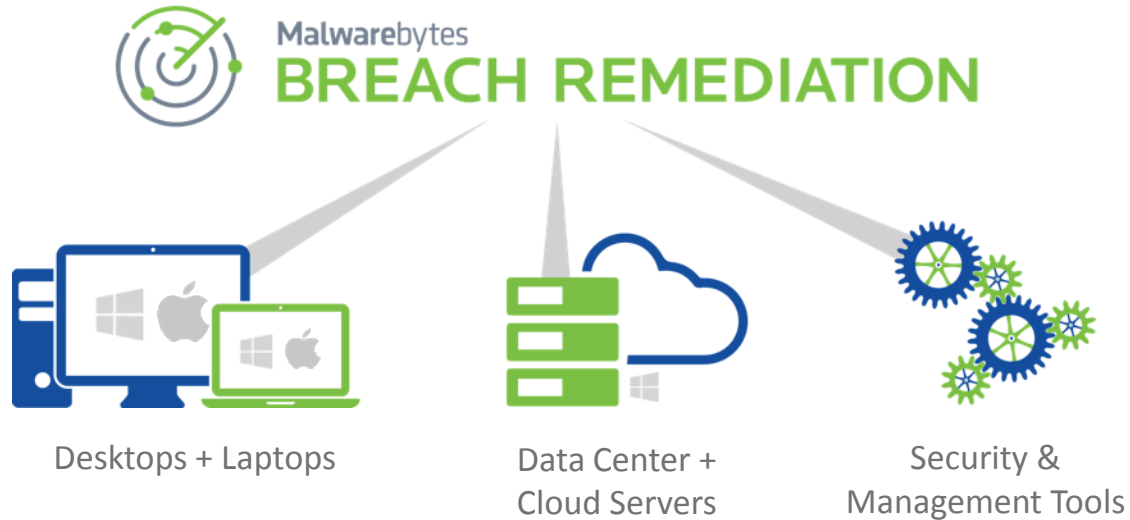
- ✓ **Profiling** – signature-less application hardening with fingerprinting detection
- ✓ **Delivery** – web protection prevents access to phishing and malicious websites
- ✓ **Exploitation** – signature-less exploit mitigations and application behavior protection
- ✓ **Payload Execution** – advanced payload analysis
- ✓ **Malicious Behavior** – signature-less ransomware behavior blocking, callback protection, remediation engine



CENTRAL & SOUTHERN OHIO Chapter

How Malwarebytes Can Help: Advanced threat removal

Detects and remediates advanced threats via an extensible platform:



Let's Take Your Questions

Learn More: malwarebytes.com/business

Latest News: blog.malwarebytes.com

Request a Trial: <https://www.malwarebytes.com/mwb-signup/trial/>

Thank You!



CENTRAL & SOUTHERN OHIO *Chapter*