TECH SCAMS: IT’S TIME TO RELEASE THE HOUNDS

Erik C. Wahlstrom
Sr. Program Manager
Microsoft – Windows Active Defense (WiAD)
A social engineering attack designed to trick users into believing that their devices are compromised or broken. Victims are directed to a “call center” where they are scared and coerced into purchasing fake tech support services.
The tech support ecosystem

- Cold Calls
- Browser lock ups
- Unsolicited email
- Fake Anti-virus /Security software
- Fraudulent
- Destructive

Helpful

Official support channels

e.g. https://support.microsoft.com

Legitimate

Your cousin that used to work in “Tech”

Our Focus
Why should we care?

- 2 in 3 surveyed consumers report being impacted
- $250-$450 average loss
- Among Microsoft’s top customer support call types
- ~13,000 reports monthly
- 300+ identified targets
- 46 law enforcement actions
- 87% think companies like Microsoft are responsible
CASE STUDY: JEN

Abusing the Browser
Case Study: Jen

- Jen opened an internal home page: [http://msw](http://msw)
- Something had changed since yesterday
The server warning-abv59.stream is asking for your user name and password. The server reports that it is from This URL has been blocked under instructions of a competent US Government Authority or in compliance with the orders of a Court of competent jurisdiction. Infringing or abetting infringement of copyright-protected content including under this URL is an offence in law. Ss. 63, 63-A, 65 and 65-A of the Copyright Act, 1957, read with Section 51, prescribe penalties of a prison term of upto 3 years and a fine of upto 3000 USD. CALL (Toll Free).

Warning: Your user name and password will be sent using basic authentication on a connection that isn’t secure.

User name

Password

OK  Cancel
This site says...

**Microsoft Warning Alert**

Malicious Pornographic Spyware/Riskware Detected

Error # 0x80072ee7

Please call us immediately at (888) 440-6107
Do not ignore this critical alert.

If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a Pornographic Spyware and riskware. The following information is being stolen...

- Financial Data
- Facebook Logins
- Credit Card Details
- Email Account Logins
- Photos stored on this computer

You must contact us immediately so that our expert engineers can walk you through the removal process over the phone.

OK Cancel
WARNING!

The last website you visited has infected your computer with a virus.

Click OK to begin the repair process.

**If you leave this site your computer will remain damaged and vulnerable**

Close
CASE STUDY: JIM

How the calls unfold
Hi Erik,

I was having trouble with Outlook, so I called MS support at 800-237-6964 to my machine and said that it's infected, and that someone has a the IP address. He brought up a box on the screen that showed some kind of foreign address that had access to my machine. This scared the shit out of me. Then he offered to fix everything for a support fee of $129. At that point, I said I'd have to think about it, and we hung up. I've turned the machine off.

This is scarier the shit out of me because I've used that machine to access our investment accounts at Vanguard. I didn't understand most of what this person was saying. I'm going to leave the machine off until we can figure out what to do.

Is this as bad as it sounds?

Jim

I'm sending this from Colleen's old Apple.
Disclaimer: MicrosoftWindowsSupport.com is just an online lead generating website. We strongly deny any affiliation with any of online/offline independent/direct remote tech support services providers except that we're generating potential computer issue related leads for them. We strongly condemn any potential misuse/online scam or unlawful handling of the leads generated by us. Our verbal guidelines to the clients are pretty clear & any misuse or aforesaid act will be the sole responsibility of the client handling the lead. We've no affiliation with any of these third-party companies unless such relationship is expressly specified. For permitted use and specific warranties associated with the software, hardware, and peripherals, please contact the relevant third party. All the brand names, logos and trademarks used herein remain the property of their respective owners. Use of any company name or their logos or images is not intended to imply any endorsement or direct affiliation with MicrosoftWindowsSupport.com. You agree that you will not rely on and are solely responsible for determining the appropriateness of using the information provided on this website and assume any risks associated with doing so.
CASE STUDY: GAIL

Payment
I am a nursing instructor and I have to have an operational and secure computer to use for two jobs. . . . I purchased a Lifetime Warranty for my computer and technical services good for my lifetime on any device, which also included any new Microsoft/Windows updated programs e.g. Windows 11. The cost for these was $1249.99. . . .

When I initially tried to use my credit card to pay MS Infotech on their site, it “mysteriously” would not take my card number. The technician suggested I could do a . . . . one-time bill pay. He assured me he could not see my codes or numbers and that the bank was secure. . . . I believe they trick you into having to use your bank account bill pay as opposed to a credit card so you can’t block the charges when you discover they are a scam.
THE FULL ATTACK CHAIN
The Full Attack Chain

- Search Engine
- Online Ad
- Phishing Mail
- Web Site
- Malware
- Cold Call
- Call Center

Make the "sale"

Payment

Scammers returning for a second helping
Windows Defender SmartScreen™ currently uses many of these signals as ML features.

The latest version of Windows 10 moves these models inline to address new classes of threats.
The Full Attack Chain

- Search Engine
- Online Ad
- Phishing Mail

- Ranking/Relevance
- Fraud Detection
- Scanning / Detonation
- Anti-Virus

- Call Center

- Make the sale

- Payment
The Common Pattern

Establish the call
Install RAT tools
Display “threats”
Complete the “sale”
Payment

Potentially detectable
Highly detectable
Potentially detectable
Highly detectable
Machine Learning to detect cold calls

- Many of these events are currently detected today
- We are currently tuning ML detection models based on these signals (and others)
Now what?

- Behavior modification is difficult
- People don’t *want* to be informed
- Ramping up notifications is exactly the wrong thing to do
- We *can* block but should we?
A Gentle Reminder?

Jim Philipps would like to install “Im-A-Scam Remote Access Tools” on “Jim’s Desktop”. Would you like to authorize this?

- Allow
- Deny

Your security software detected a malicious actor using a trusted application. This connection has been rejected and closed. The application hosting this threat will be disabled for 72 hours to protect you.
DISRUPTING THE CALL CENTER
Disrupting the Call Center

- Search Engine
- Online Ad
- Phishing Mail
- Cold Call
- Web Site
- Malware
- Call Center
- Make the sale
- Payment
Affiliate Programs

Cold Call Detection
(888) 595-4323
(xxx) xxx-xxxx
(866) 649-2816
(xxx) xxx-xxxx
(855) 784-2431
(xxx) xxx-xxxx

Browser Detection
(888) 595-4323
(xxx) xxx-xxxx
(866) 649-2816
(xxx) xxx-xxxx
(855) 784-2431
(xxx) xxx-xxxx

Customer Submission
(888) 595-4323
(xxx) xxx-xxxx
(866) 649-2816
(xxx) xxx-xxxx
(855) 784-2431
(xxx) xxx-xxxx

Totally Legit
(888) 595-4323
(xxx) xxx-xxxx
(866) 649-2816
(xxx) xxx-xxxx
(855) 784-2431
(xxx) xxx-xxxx

Remote call forwarding

Call Center
"Virus Total for Phone Numbers"

1(888) 595-4323 has received reports of suspicious activity in the past 72 hours.

3rd party dialer app

3 reports in Last 72 hours

Phone Reputation Service

Law Enforcement

Edge/IE

Telecom

Other Browser
What’s next?

- **Educate**: “Microsoft does not make unsolicited phone calls to fix your computer”.

- **Technology**: Use strong web filtering technologies and other blocking technologies to avoid scams.
  - Most modern browsers ship with these installed. Use them. And provide feedback!

- **Partner**: With Microsoft, other platform vendors, search engines, telecoms, and governmental organizations to address Tech Scams and social engineering attacks.