The Anatomy of Tech Support Scams

How Tech Support Criminals Continue to Exploit Consumers and Businesses Without Getting Caught

October 18, 2016

Presented by:

Malwarebytes

Introduction

Each year, several million people fall for tech support scams. In 2015 alone, crooks walked away with an estimated $1.5 billion according to Microsoft. Once simply conducted by telemarketers through "cold calling," now scammers pay to have their tech support line number listed on websites or use pop-ups to get victims to call them. Instead of receiving help, the user finds their computer held ransom. These tech support scams aren't easy to spot. Their tactics have become so advanced (with real company logos, signatures of legitimate tech support offers and digital targeting); almost anyone could fall for their tricks.

The Origin of Tech Support Scams

Most people associate tech support scams (AKA fake Microsoft support cold calls) with technicians sitting in a crowded and buzzing boiler room somewhere offshore, and they are not wrong. The origin of tech support scams can be tracked to Mumbai, Kolkata or elsewhere in India. The first reports of these tech support scams (TSS) surfaced around 2008 and they have gradually gained momentum over the years.

Instances of TSS rose rapidly in 2013 when scammers began to use malvertising to push fake alerts. One year later, the Internet Crime Complaint Center, also known as IC3, issued a public service announcement about the new digital twist on tech support scams in order to educate Internet users and urge the public to file complaints and take precaution.

Not long after digital tech support scams hit the mainstream, giant tech companies began to fight back. In December 2014, Microsoft publicly sued several companies, including an Indian one, alleging they falsely claimed to be Microsoft-affiliated technical support. And in 2015, the FTC started to take some giant leaps in the fight to support and protect tech companies, as well as consumers. In November of that year they announced the shut down of several tech support scammers that impersonated Apple, Microsoft, Google Tech Support and stole nearly $17 million from consumers.

However, the fight has only just begun. Since the FTCs first major win, tech support scams continue to evolve and steal millions of dollars from consumers every year.

Tech Support Scams Today

Over time, tech support scams have evolved to become very advanced. Today, they remain effective against most average Internet users. The forces behind them have also shifted. Tech support scammers are no longer all sitting in a call center in Mumbai. They are right in our backyard and they are using all of the newest cyber tactics.

A New Home for TSS

Most tech support scams still originate from India due to a number of strategic factors, including pre-existing networks of locals with backgrounds in the tech support industry and low overhead costs. However, the state of Florida has also evolved into a hot spot for more digital variations of tech support scams. Many of the most lucrative tech support scam organizations are now run out of the U.S. Due to the sheer amount of tech support organizations based in Florida, it lends itself to being a hub for tech support scams. Cheaper labor, relaxed laws and resources make this a prime location and the industry continues to flourish in the sunshine state today.

Tactics Continue to Evolve

As cyber crime has evolved, so have the tactics of tech support scammers. In fact, tech support scammers are well aware of what is going on in cyber crime and often rip off ideas and concepts from other criminals. Below are a few of the most prevalent modern tactics.

- **Software Activation Scams:** Software activation scams convince individuals to purchase a program (for example, a PC optimizer) and purposely hide the license key. They are then forced to call the company that sold them the program for help and are social engineered over the phone about 'problems' with their PCs. This specific approach is highly targeted to elderly individuals who are not tech savvy.

- **Fake AV:** Some tech support scammers impersonate AV "security scanners." Screenshots of what appears to be real anti-virus software appear on a webpage, displaying made up infections.

- **ISP Targeting:** Recently, tech support scams have evolved to pose as legitimate Internet service providers (ISP). In this instance, a realistic pop-up interrupts a victim's normal browsing session with a message prompt to call a support number because their computer has been infected and, most importantly, it appears to be legitimate and seems to come from the victim's real ISP.

- **Domain switching:** Some browsers, like Google Chrome, may be able to detect and therefore block repeated attempts of tech support scam attacks. To circumvent this protection, some scammers today load a new URL each time you click on the "Leave Page" button. That URL points to a subdomain from the original scam page, which in turn repeats the process with another subdomain, in effect creating what looks like a never-ending situation, convincing many people that their only way out is to call the fake tech support number.

- **Scam lockers:** Most tech support scams today use malware-like techniques and extortion tactics to force targets to call TSS organizations. Because the scammers are using malware and ransomware, simply installing what appears to be a software update

or video codec can infect a victim's computer. They are then forced to call scammers in order to unlock their machines.

Impact is Growing along with the Targets

Tech support scams continue to impact thousands of consumers a year, causing the public to lose millions of dollars. Just from January 1, 2016, through April 30, 2016, the IC3 received 3,668 complaints with adjusted losses of $2,268,982 and these numbers are growing at an alarming rate. According to a recent report by Symantec, there was a 200 percent rise in fake tech support scams in 2015. Tech support scammers have not stopped using traditional cold calling tactics and are only using their newest digital tactics on top of their old techniques. The evolution of this scam is leading to more victims and much greater consequences for the general public.

Not surprisingly, most tech support scams heavily target a demographic that is not tech savvy – the elderly. In particular, fake alert TSS and software activation TSS target older individuals. However, with the emergence of tech support scam lockers this year, **anyone is now a potential victim**. This new tactic no longer just employs social engineering, and criminals are no longer solely targeting less tech savvy individuals.

A Look at Why Engineers Work for "Tech Support Scam" Operations

Tech support scams targets are not the only victims of the TSS industry. Recruitment for these organizations is conducted mostly through online networks with minimal checks and balances, such as Craigslist. The individuals targeted to operate the tech support scams, and even support their programming efforts, are mostly young and the prospect of these positions is increasingly appealing for a number of reasons. First and foremost, they are lucrative and easy to come by.

In fact, Malwarebytes researchers recently discovered a network of TSS companies whose operations appear shockingly legitimate and whose recruitment efforts have enabled them to hire real engineers for years. For example, Gowyn/Delwyn, which looked legitimate until further digging, appeared at a career fair in India alongside legitimate, recognizable multinational corporations. So how many companies at that same career fair were also running scams? Let's take a look at a few new ones that were uncovered.

- **Gowyn/Delwyn:** Based in India, Gowyn/Delwyn is a "tech support" company that treats their employees well, appears at legitimate career fairs, offers reasonable salaries in an affluent area (a recent graduate can expect to make an average income equivalent to USD $60,000 per year), and provides employees with technical challenges to work on. In the thriving and complicated tech market in India, a company such as this is naturally drawing quite a few candidates, despite the fact that their business model is centered around tech support scams and infecting individuals with potentially unwanted programs (PUPS).

- **Emobilize:** Emobilize tries very hard to present themselves as a UK based digital marketing firm. However, they maintain assets on their site relevant to tech support spam Quora, offering tech support services, and have so exceptionally upset their customers that the CEO felt it necessary to post a blog begging Malwarebytes to believe that his company is not a scam.

- **BENOVELLIENT TECHNOLOGIES Pvt. Ltd:** There's no overt history of scamming with this company – it has a fairly professional website, a public CEO, and no significant record of complaints. But digging a little yields some interesting results. The US contact number, 1 800 290 0592, also shows up on Cyberpcexperts.com, a site that does have an extensive list of scam complaints.

TSS companies are not only able to attract programmers and engineers with seemingly legitimate recruitment tactics; they also attract individuals who simply need a job. In the U.S. the standards for hiring have been found to be incredibly low. As a result, the TSS space has the potential to take advantage of individuals with criminal records or little to no work experience. These are individuals who will have difficulty getting jobs elsewhere, and they are exploited into doing the job without asking questions.

Fighting Back

The individuals behind most tech support scam organizations might surprise you. They are mostly big money scammers who have been involved in criminal activity elsewhere and hold significant financial power. And, while small attempts have been made to shut these criminals down, they remain very powerful today – both here in the U.S. and abroad.

An Uphill Battle

The legal case against tech support scams originating in the U.S. has proven to be difficult over the past few years, and prosecution has been limited. Courts are not tech savvy enough to understand the latest scam tactics, making it very easy for scammers to get away with certain technical intricacies. In a recent case againt ICE Tech Support, defense lawyers were able to argue that the techniques they were using were legitimate, despite the fact that any security researcher would be able to tell you that actual potential damage impact of what they were "warning" consumers about was negligible. For a court faced with a decision, an argument such as this, without further technical evidence, is enough for criminal tech support companies to claim their actions as legitimate.

Additionally, the social impact of putting an entire tech support company out of business, even if they are suspected of criminal activity, can be very concerning for a court. Most tech support companies have thousands of employees and millions of dollars of revenue. Shutting them down would put all of these individuals out of work.

These factors extremely complicate the battle against tech support scams today. Regardless, the impact that they are having on consumers is substantial and steps can be taken to improve the processes that are in place to eliminate them.

The Malwarebytes Mission

Malwarebytes researchers have been actively engaged in the fight against tech support scammers overseas but also here at home in the U.S. With a commitment to helping protect consumers from all dangerous cyber threats, they are working hand in hand with the Federal Trade Commission to help provide technical evidence in support of shutting tech support scammers down while simultaneously educating Internet users on how to protect against the latest TSS tactics.

In 2014, Malwarebytes worked with the Federal Trade Commission to shutdown OMG Tech Help, an American-based tech support company involved in deceptive tech support practices. The FTC alleges that "the defendants used software designed to trick consumers into thinking there were problems with their computers, and directed consumers to telemarketers who subjected those consumers to high-pressure deceptive sales pitches for tech support products and services." Malwarebytes researchers were able to testify in court with strong technical evidence against the defendants, including video evidence of their activities. **On June 20 2016, the FTC announced that the defendants had settled and have been required to surrender all of their assets to a court receiver.**

Malwarebytes remains committed to pursuing online scammers who often use its brand, products and reputation to defraud innocent people. The company now provides daily reports to hosting providers and the FTC, detailing activities that they suspect are malicious.

What Others Can Do to Help

Security companies can help join the fight by educating themselves and consumers on the latest scams, because they are evolving at a rapid pace. Security companies can also help join the fight by collecting and providing any evidence that they find on malicious tech support activities. The FTC continues to invest resources and time on battling those suspected of TSS activity, and could use any evidential help and support.

Consumers who are targeting or fall victim to tech support scams are urged to revoke remote access, scan their computers for malware, and quickly change all passwords to everything including your computer, email, and bank accounts.

Tech support scams can and should be reported to government agencies. In the U.S., consumers are urged to report any scam activity to the FTC. For consumers outside of the U.S., more information on who to contact can be found at https://blog.malwarebytes.com/tech-support-scams/.