Zombies

For Oklahoma Bankers Association – December issue

Rayleen M. Pirnie, AAP
RP Payments Risk Consulting Services

The Zombie Apocalypse: Fighting the Plague

It seems every decade we have a new ghoulie to obsess over; I think we can agree that today that's the zombie. As a culture we love to get scared; we even pay for it (think haunted houses). We know we can turn the television off and the ghoulie goes away. But few seem to realize that zombies go well beyond the TV, and there are some you can't turn off. In fact, you could have one lurking in your home right now and not know it, even when the coded-creature carries out its evil deed.

I'm not talking stumbling, slow, flesh eating "undead"; I'm talking about computer zombies. They are very real and very dangerous; yet few people even know what they are and worse, don't know how to protect themselves against one. So buckle up, we're heading for a crash course on why bankers need to fear THIS zombie apocalypse.

What is a computer Zombie?

A zombie is a computer that is connected to the Internet that has been compromised by a hacker, usually through a virus or Trojan horse. Doesn't sound TOO bad yet, right? Well, here's the other side of a zombified computer – that hacker can use the infected computer for malicious tasks, attacks, and a lot of other nasty stuff. Hackers often connect the infected computers together to become powerful threats.

Why should bankers care?

Your own customers' computers could be part of a Distributed Denial of Service (DDoS) attack against your bank, and they wouldn't know it. Criminal's string together compromised computers into what is known as a botnet (i.e. robot network). It's really just like it sounds; thousands or even hundreds of thousands of infected computers a hacker can control all pointed at, for example, your online banking site to take it down because it can't handle that much traffic. DDoS attacks hit a new record high in 2Q15 according to the latest State of the Internet report from Akamai.

The controlling hacker can also use the infected computers to spread spam and computer viruses to others. Security experts estimate as much as 80% of spam is sent by zombie computers.

Depending on the flavor of infection they caught, hackers could even capture information as the computer user accesses websites like their online banking or payroll service sites.

And computers aren't the only potential victims; in 2014, Network World explored how hackers could compromise iPads and iPhones on a large scale when connected to infected computers. The malicious app can steal passwords, personal information, and oh yes, PINs you text as part of out of band authentication.

All this happening every day, yet few seem to understand just how vulnerable they are. Even worse, zombie programs are very good at hiding on your computer, lying dormant until the hacker needs a boost in power to carry out their master plan.

Be afraid; be very afraid. Then, spread the word.

Setting up defenses
There are defenses to help decrease your computer's chances of becoming part of the cyber-undead. Powerful anti-malware packages, updating and patching regularly, properly configured firewalls and a huge dash of cynicism will help protect you and your coworkers.

I encourage you share the customer article, titled *The Zombie Apocalypse: Possibly Coming to a Computer Near You* with your customers so they understand what the threat is, and more importantly, defensive actions to fight this growing threat.

The Zombie Apocalypse: Possibly Coming to a Computer Near You

(customer perspective)
It seems every decade we have a new ghoulie to obsess over; I think we can agree that today that's the zombie. As a culture we love to get scared; we even pay for it (think haunted houses). We know we can turn the television off and the ghoulie goes away. But few seem to realize that zombies go well beyond the TV, and there are some you can't turn off. In fact, you could have one lurking in your home or business right now and not know it, even when the coded-creature carries out its evil deed.

I'm not talking stumbling, slow, flesh eating "undead"; I'm talking about computer zombies. They are very real and very dangerous. Yet few people even know what they are and worse, don't know how to protect themselves against one. So buckle up, we're heading for a crash course on what you need to know to survive the computer zombie apocalypse.

What is a computer zombie?
A zombie is a computer that is connected to the Internet that has been compromised by a hacker, usually through a virus or Trojan horse. The hacker can use the infected computer for malicious tasks, attacks, and a lot of other nasty stuff. Yes, you heard that right – they can use the infected computer, from wherever they are in the world. Oh, and did I mention you won't know it?

How can zombies affect my business or me personally?
Computers are often infected via Facebook and other social media sites where sharing videos is common. When you click on the video or video link, a devious program starts downloading.

Once infected, zombie computers are most frequently used to spread spam and viruses to other computers, without the knowledge of the infected party. So that means your computer is being used maliciously to infect others. Criminals prefer this method because using thousands of IP addresses (i.e. different computers) helps them get their spam and viruses past email filters, making their campaign more successful. And, there's more…

Infected computers are often tied together so a hacker has literally thousands of different IP addresses to commit what is known as a Distributed Denial of Service attack; a powerful attack that has taken down sites like Visa, MasterCard, Xbox, and many bank online banking sites. These types of attacks hit a new record high this year; what that means is hundreds of thousands of people's computers are already infected and used regularly in attacks against other businesses. The total number of zombie computers is unknown, but security experts have reason to believe it's a very high number.

And depending on what variety of zombie infection your computer picked up, the hackers may also have access to any personal information stored on the computer, collect data you type into forms (like online banking sites), harvest files (i.e. accounting programs, employee and client identifiers, etc.), and attach to your mobile phone or tablet when you sync it to an infected computer.

Playing hide and seek with zombies is no fun.
Zombies are very good at hiding in the shadows of your computer so you don't notice them. The programs that make your computer a zombie often have file names that are similar, or even

identical, to normal system file names so you wouldn't worry even if you do see them processing. Sneaky.

Kinda like a flu shot.
So now you know what cyber zombies are and I'm guessing that you really don't want to own one. So what do you do? Glad you asked! It's time to educate yourself on best practices that you can use at work and at home.

Anti-virus alone probably won't be much help. You need a sophisticated security package which comes with what is known as anti-malware too. Up-to-date anti-malware software can proactively protect PCs from most zombie infections. Set your security software to update automatically whenever a new patch is released. However, don't rely solely on software. There is always a lag between the time when hackers launch new attacks and when your security vendor can release an update to fight the new threat.

Use cynical judgement before playing videos or clicking on links. If it seems strange, contact the sender to inquire if they really sent you something. For example, you and I are business colleagues; one morning you receive an email from me with a link or video attachment. The email says "check out this video I found of you online! LOL" That should set off alarm bells. Don't click the link or open the video.

Considering giving your firewalls a fine tune as well. Firewalls won't protect you from everything, but they sure go a long way if they are set up correctly. And if your computer pops up a message, be sure to read it. You may think you're just grabbing a quick cute cat video on Facebook during lunch, but your computer may try to warn you that there's something more sinister lurking there.

Fortinet developed The Zombie Awareness Month Computer Survival Guide to help you learn how to defend yourself against the zombie invasion. The guide says "While you can't kill a zombie computer by shooting it in the head, the best way to disable it and then kill it is to quarantine it (and the best way to do that is to disconnect the suspected zombie from the network). Then run a virus scan, which, if your software's up to date, should find it and rub it out.

Thanks for helping keep zombies on the television and out of our computers.

About the Author

Rayleen is the owner of RP Payments Risk Consulting Services, based in Orrick, MO. She travels the country presenting at fraud, payments and security conferences on topics ranging from Mobile, fraud, risk management, and information security. Rayleen has been writing and presenting for 9 years. Previously she worked financial crimes investigations for a national bank.