The Annoyance Of Memory Based Hacking

by Steve Brown

A recent article by Concur identified the biggest job related annoyances that have surfaced in the past 20Ys or so. They include: smartphone sounds, unnecessarily replying to all in an email, having awkward web conference calls, over sharing links, pressuring co-workers to share your creations with their personal networks, sending emails to colleagues on the weekends, slow computers, sharing critical information verbally instead of through email or otherwise documenting it, connection requests on social media from co-workers and old technology solutions.

In banking there are many other annoyances beyond bad employee habits and one of the spookiest relates to cyber risk. More specifically, consider that technology researchers find hackers are using a relatively new tool - malicious code that runs in memory, rather than in a software file.

Memory-based intrusions use existing, legitimate software, applications and protocols, to carry out their mission. As such, they can control computers without downloading viral files. Knowing this, community banks need to be sure to incorporate this new type of threat into current cybersecurity measures.

Traditional antivirus measures are designed to stop file-based intrusions. Given this new cyber hacking development, those same antiviral tools don't recognize file-free code as a potential attacker, so they can't identify and shut down file-free hacks.

Hackers and thieves have taken advantage of this loophole. Carbon Black, a software security company based in MA, says that in 2016 hackers targeted nearly all their customers using memory-based code. The company found that attackers primarily targeted customer data (62%), corporate intellectual property (53%), disrupted service (51%), credentials (42%), and financial data (41%). The company's research also indicates that banks are increasingly popular targets.

Community banks should already assume they are potential victims and understand how memory-based attacks differ from file-based invasions.

A standard, file-based malware attack arrives as an email with a tainted attachment. IT departments put these attachments in a sort of electronic sandbox that serves as a safe place to evaluate them, and use programs designed to detect and detonate them.

Memory-based attacks are invisible to these standard defenses. Their program logic lets them detect a sandbox and they won't run in one. They easily elude file-based anti-malware and detonation which are two common defenses against file-based malware.

To fight this new threat, IT departments can deploy a technology called content destruction and reconstruction (or regeneration). This strips suspect content out of an email and delivers just the safe piece.

Several cybersecurity companies make endpoint detection and response tools for memory-based attacks and more traditional anti-malware companies are also adjusting their software to detect incursions.

In addition to reviewing countermeasure technologies, banks can evaluate what scripting languages can operate on their endpoints. Then banks can use that information to dial in protective responses. This may sound a bit "techy", so be sure to ask your IT team as they will surely know what all of this means.

Deception technology and decoys can help, too. Some software puts deceptive documents that contain fake customer information on a bank's file share, then scans the web to see if that information has leaked. This is a way to check how robust your protection is.

Banks might perhaps also use an endpoint security program that looks for any code that's asking questions. Memory-based malware often asks if it's in a sandbox. A security program can lie to it, tricking it into opening up and revealing its true nature.

The technology used by hackers is advancing quickly, so bankers must respond. After all, no matter how annoying co-workers might be on any given day, they pale in comparison to the annoyance cyber thieves can cause.

BANK NEWS

Yield Pop

Dallas Fed President Kaplan said he thinks the 10Y Treasury yield needs to move higher for the Fed to keep on removing accommodation. Meanwhile, Fed Chicago President Evans said technology is changing business models that used to be successful, leading to an "undercurrent" that could be holding back inflation.

CU Shift

In an odd twist, the Canadian government said only banks can use words like bank, banker and banking to describe their business. The shift means credit unions, financial companies, federally regulated trust and loan companies and non-banks will no longer be allowed to do so.

Good News

Fed Chair Yellen said banking regulators have made improvements to the financial system making it so much safer, that another financial crisis will not occur "in our lifetimes."

Branch Pressure

The former CEO of Barclays informed CNBC in an interview that bank branches are being closed so rapidly that they will be "as common as a Blockbuster video store in a few years' time."

Favorites

The Fed reports checks account for only 13.4% of noncash payments now vs. 57.8% in 2000. Meanwhile, debit card purchases have soared to nearly 40%.

2017 EXECUTIVE MANAGEMENT ROAD TOUR

Join us in San Francisco or Chicago for this not-to-be-missed event where experts will discuss critical issues facing community bankers. Visit our website and register today!