Blog for MPA Networks

https://www.mpa.com/blog.aspx?p=seven-delivery-channels-ransomware

The “Seven Deadly Sins” of Ransomware

Posted June 29, 2016

Readers of our blog over the past few years know we were among the first in the Bay Area to warn our customers about the growing threats of ransomware—from the emergence of CryptoLocker and CryptoWall to our federal government's startling admission that they're virtually powerless to stop it.

Mostly originating from sophisticated cyber-gangs in Eastern Europe, ransomware may be the most profitable organized crime scheme in the world today.

We weren't exactly surprised, then, when we received “2016 Will Be the Year Ransomware Holds America Hostage,” a 40-page report from The Institute for Critical Infrastructure Technology (ICIT), a non-profit cybersecurity think tank. The ICIT report is a **comprehensive review of the ransomware landscape**—from its earliest origins to the major active strains "in the wild" to the likeliest targets (particularly American small businesses). Today we'd like to highlight the **seven delivery channels of ransomware and other malware infections**—what we refer to as "The Seven Deadly Sins."

1. Traffic Distribution Systems (TDS)

If you visit a website and suddenly see an annoying pop-up ad, it's because the website sold your "click" to a TDS vendor, who contracted with a third-party advertiser. Pop-up blockers have rendered most pop-up ads obsolete, but some of the shadiest TDS vendors contract directly with ransomware groups to spread exploit kits and “drive-by downloads.”

2. Malvertising

As we discussed last July, even trusted web pages can include third party ads embedded with malware-inducing code. One click on a bogus ad can wreak havoc.

3. Phishing Emails

From phony bills and résumés to bogus "unsubscribe" links in annoying spam, email recipients can be tricked into clicking a link allowing an instant viral download of ransomware. Research reveals that despite strong security training, up to 15% of employees still get duped by phishing schemes.

4. Gradual Downloaders

Exploit kits and ransomware can be discreetly downloaded in "segments" over time, evading detection by most anti-virus defenses.

5. Social Engineering

Also known as simple "human ignorance," a user can be tricked into downloading a phony software update or other trusted download link—even ignoring warning messages (as happened to a friend of ours) only to allow a costly malware infection.

6. Self-Propagation

Once inside a single computer, the most sophisticated ransomware strains can automatically replicate through an entire network via the victim's address book. ICIT expects that self-replicating ransomware will evolve to infect multiple devices within the Internet of Things.

7. Ransomware as a Service (RaaS)

ICIT predicts that the largest ransomware creators will syndicate "retail versions" of their products to less sophisticated criminals and lower-level hackers who'll perform the day-to-day grunt work of hunting down new victims around the world. The creator collects a percentage of every successful ransom payment. In the coming weeks, we'll continue to examine ransomware and other cyberthreats our customers need to defend against.
For more on how to protect your company, contact us.