2010 Year End Security Wrap

Peter Silva, 2010-15-12

Figured I'd write this now since many of you will be celebrating the holidays over the next couple weeks and who really wants to read a blog when you're reveling with family and friends. It's been an interesting year for information security, and for me too. I started the year with New Decade, Same Threats? and wondered if the 2010 predictions of: social media threats, smarter malware/botnets, using the cloud for crime, financial DDoS, rogue software, Mac and Mobile malware, more breaches and a whole host of others would come through. And boy did they.

Social media was a prime target for crooks with the top sites as top targets. Users were tricked to accepting and sharing friends that really weren't friendly and social networks became a new hotbed for malware distribution. As for malware, while many botnets and spam outfits got taken down this year, Stuxnet was certainly the most sophisticated piece of malware researches have seen in a while. Targeting industrial & utility systems along with the ability to reprogram itself, no longer was it my single laptop or a company's system that had a bull's-eye, although the initial infection is with those systems, it was nuclear facilities, oil refineries and chemical plants that were the ultimate objective. For Cloud Computing, was it Cloud 9 or Cloud Crime when it came to using the cloud for nefarious activities? Many people thought that with the cloud offering a slew of computing power, that it would be a prime way to initiate an attack. We really didn't see much pertaining to 'cloud breaches' even though almost every survey throughout the year indicated that security in the cloud was everyone's ichiban concern. I covered many of these surveys in my CloudFucius Series, now playing in a browser near you. This article talks about that, the reason we might not have seen much in the way of cloud specific breaches is that many of the data loss repositories do not differentiate between a cloud based and non-cloud attack. In addition, cloud providers are not that willing to spill vulnerabilities that have led to crimes. Share please.

Banks and financial institutions were certainly targets this year, why wouldn't they be, that's where all the money is. In one incident, about $3 million was stolen from various banks around the world using viruses and more than 100 crooks suspected of running the global cybercrime ring were arrested in the US and UK this September. A 16 year old Dutch kid was arrested last week for a Distributed Denial of Service attack on the MasterCard and Visa websites. And, merging malware, mobile and money stores, the ZeuS Trojan could infect a desktop, capture the user's bank credentials next time they logged in to their financial institution, popped a dialogue box for the user to 'include' their mobile phone for SMS payments, send the phone a fake message & certificate for acceptance and then installed another Trojan on the phone to monitor messages via SMS. Lots of trickery and luck to be successful but still a very scary exploit. And if you think those mobile banking apps are secure, think again. Just last month, a number of those apps were found to have serious vulnerabilities, flaws and holes. Many of those apps have been patched in light of the research but as with any 'new-ish' type technology, mobile banking must be locked down before the masses adopt. Too late now.

I wrote about corporate espionage both in Today's Target: Corporate Secrets (2010) and The Threat Behind the Firewall (2009) and this year did not disappoint. Social engineering or convincing someone to give up their info is alive and well but throughout 2010, employees stole secrets from the companies they worked for: Former Goldman Programmer Found Guilty of Code Theft, Greenback engineers guilty of corporate espionage, Ford secrets thief caught red handed with stolen blueprints, and SEC Bares Text of Inept Suspects As They Sold Disney Earnings Info To FBI Agents. These insider events can often be more costly than an external breach.

This is by no means an exhaustive list of the breaches, attacks, vulnerabilities, hijacks, frauds, or other cybercriminal activities from 2010. I'd probably be writing through the holidays to get them all. These were just some of the things I found interesting when looking back at my initial blog entry for the year. With 2011 being the Year of the Rabbit, just how much will cybercrimes multiply?

ps

Resources:

- Social Life's a 'breach'
- Security: Malware, Hacks and Leaks: The Top 10 Security Stories of 2010
- 2010: Looking back at a year in information security
- Surprising little information about Cloud Computing and Terrorism or Crime

- Accounts Raided in Global Bank Hack
- ZeuS attacks mobiles in bank SMS bypass scam
- Firm finds security holes in mobile bank apps
- The truth about Mac malware. It's a joke
- Study: No Hacking Needed when Modern Spies Steal Corporate Data
- Growth in Social Networking, Mobile and Infrastructure Attacks Threaten Corporate Security in 2011
- Ponemon Encryption Trends, 2010
- Personal Data For Sale – In time for the Holidays!
- Synthetic Identity Theft: The Silent Swindler
- Cybercrime, the Easy Way
- Dumpster Diving vs. The Bit Bucket

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com