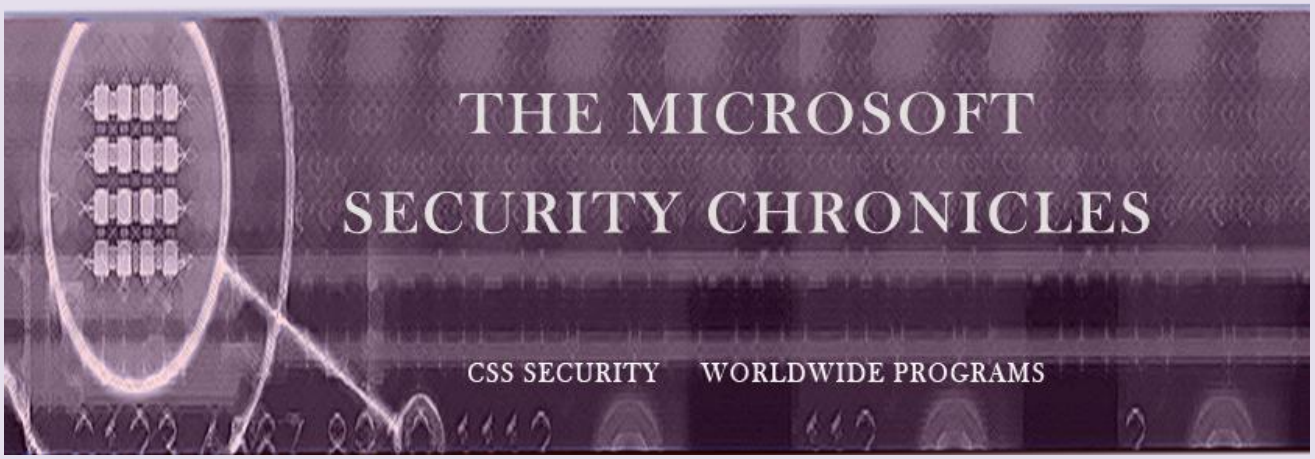


December 20, 2012

INSIDE THIS ISSUE

MICROSOFT RESOURCES

Microsoft Security Home

Microsoft Trustworthy Computing

Microsoft Security Sites Worldwide

Top 13 Security Predictions for 2013

The Channel

The year 2012 was a big year for security.

The Flame and Gauss viruses demonstrated the potentially devastating, threat of cyber warfare, Anonymous showed the world just how powerful hacktivists can be, and the first ever virus found in the iTunes app store made us realise that not even Apple is safe from cyberattack.

Analysis:

It seemed only right for our last article of the year to be one that not only spoke of what happened in the world of security for 2012 but also looked ahead to 2013. It was a busy year in terms of attacks where one of the main topics seemed to be around spear phishing. The crooks are getting better at targeting certain people in various companies that give them access to the data they need to steal intellectual properties.

Apple made the news this year having the first virus found in the iTunes app store and made us realize that the mobile malware was going to be huge (and it was!). Here is a great chart showing the growth of Android malware:

SECURITY CALENDAR

December 2012

10 WorldToor - Antarctica

27 29th Chaos Communication Congress - Hamburg

January 2013

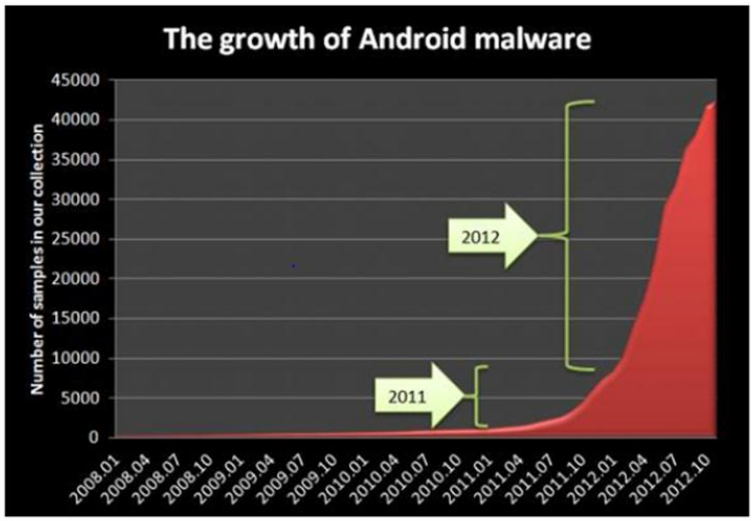
03 Microsoft Bulletin Advance Notification

07 FloCon 2013

08 Microsoft Security Bulletin Release

22 National Cyber Security Centre (NCSC) Symposium 2012 – The Hague

30 IT-Defense - Germany



Source: ZDNet

Cyber threats were also a hot topic in 2012. From threats to our infrastructure to denial-of-service attacks — speculations took shape through the year. Some say cyberthreats are just hype and a way to get us to feel threatened and be okay with losing some of our rights. Others say some firms, particularly utilities, are ignoring the risk. The author of the story says that "utilities should also avail themselves of other entities who are actively engaged in gathering and distributing information about cyber threats, including the United States Computer Emergency Readiness Team (US CERT) and the NERC Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."

We definitely saw a lot of targeted attacks to the financial sector. That probably won't go away any time soon since we are aware of shady operations that pay people to attack financial institutions. Just in one week in December 2012, there was news of a new attack against many financial institutions (including PayPal, Wells Fargo, Capital One, and many others). Obviously, since this is the biggest shopping time of year there is a lot of money to be made by accessing other's accounts. Well said from the Bank Systems & Technology article – "it's easy to forget that banks are under a near-constant attack from cybercriminals."

Spear phishing was also in the news this year as attackers looked to steal intellectual properties. Here are some great tips to keep spear phishers out of your inbox (both at work and home):

- Realize you are a target.
- Know your adversary's tricks.
- Take control of your online presence.
- Just don't click it.
- Ask for stronger security.

We found the last one to be interesting as most people wouldn't think of asking a company to add stronger security but why not? If your doctor's office has all of your private records – why can't you ask them to ensure they are taking all the right precautions? If enough patients ask for the doctor to add stronger security, we believe they would do the right thing.

Anonymous was pretty active in 2012 and not expected to go away quietly. They have been at the forefront of hacktivism in the world and are not afraid to go after anyone or any corporation that is doing what they consider to be wrong. PCWorld ran an article on How Hacktivism Affects Us All that explains why we all should be paying attention because it does affect all of us. Some highlights:

- Online vigilantes — any public presence is susceptible to attack and it is revealing how some companies are not securing their data.
- Collateral damage — high level of embarrassment whether it is on the personal or corporate level.
- Political impact — some politically motivated data breaches have inspired full-blown revolutions.

As we look ahead to 2013, there are some interesting trends based on an article by Help Net Security. They list social engineering, advanced persistent threats (APTs), internal threats, bring your own device (BYOD), cloud security, HTML5, botnets, and precision targeted malware. Security is definitely one New Year's resolution to try and keep!

Here are the top 13 issues to look out for in 2013 according to Kaspersky Labs:

- Critical Infrastructure – Flame, Gauss, and miniFlame.
- Exploit Kits – weapons of choice for cybercriminals.

- Targeted Attacks – looking to gather intellectual properties.
- DNSChanger – tricks consumers into thinking they are on a legitimate website.
- Botnets – looking for smaller botnets which are harder to detect.
- Modularisation – hackers adding their own plug-ins to web browsers.
- Mobile Attacks – Zitmo and Spitmo still the most popular phone malware.
- Rogue Certificates – hackers are creating these.
- NFC Malware – NFC payment systems with phones.
- Share Baiting – Videos your "friends" recommend that come with a survey.
- Online Privacy – the value of your personal data is huge.
- HTML5 - integrating programs with browsers makes it easier for criminals.
- Unregistered Markets – setting up illegal sites in unregistered markets.

Have a safe and secure 2013, everyone!

Our Top 10 Good, Bad, and Ugly Security Stories

The Security Chronicles Pub Team

Since security is such a serious issue, we thought the following might be a fun way to lighten up end the year. Here are the top 10 security stories we hope never to see again.

1. Burger King Employee Stands on Lettuce: Busted by Internet
   Yahoo

   Ever feel like nothing is secret anymore because of the Internet? You may be right. It took 4Chan users only 15 minutes to track down and bust the Cleveland-area [U.S.] Burger King employee who stood on top of two containers of shredded lettuce and then posted a picture of the gross act.

2. [May the (En)Force(ment) Be with You — Security Lessons from Star Wars]
   Infosecurity

   Star Wars: A New Hope is more than just an epic tale of the galaxy-wide struggle between the Galactic Empire and the Rebellion, and the triumph of good over evil. It's also a great example of how a series of basic infosecurity mistakes can cost even a massive, powerful (but evil) organization like the Empire dearly.

---

3. [Police: Pa. Mom Changed Her Kids' Grades]
   CBS News

   A Pennsylvania [U.S.] woman allegedly changed her children's grades after logging into a school computer system using passwords obtained when she worked for the district.

---

4. [Gmail Location Data Led FBI to Uncover Top Spy's Affair]
   Wired

   Every year careless hackers, cyberstalkers, and others are undone by the digital trails they leave behind for law enforcement to collect and trace back to them.

   But who would have thought the nation's top spy chief would be undone so easily by digital footprints left behind in Gmail?

---

5. [Harry Potter's Emma Watson Most Dangerous Celebrity to Search For on Web]
   Network World

   Emma Watson, best known for her portrayal of Hermione Granger in the Harry Potter movies, has been named most dangerous celebrity to search for on the web in [McAfee's annual report].

---

6. Justin Bieber and Selena Gomez Tape Lures Users to Shady Survey Sites
   Softpedia

   Cybercriminals have often attempted to trick users into visiting their malicious websites by promising them adult tapes featuring Justin Bieber and Selena Gomez. While the two were separated, the scams appeared to have died out, but now that they're back together, social media sites are once again flooded with such schemes.

---

7. Chuck Norris Dies, but Only in Malicious Scam
   Softpedia

   Facebook members may be offered a link to a video that shows how Chuck Norris died, but instead of a video, they're either served with a survey scam or a malicious browser component.

---

8. Anonymous Eavesdrops on FBI Anti-Anonymous Strategy Meeting
   Wired

   As FBI [U.S. Federal Bureau of Investigation] and Scotland Yard investigators recently plotted out a strategy for tracking suspects linked to Anonymous, little did they know that members of the group were eavesdropping on their conference call and recording their plans.

---

9. The 25 Worst Passwords of 2012, and Easy Ways to Avoid Them
   GCN

   Bad passwords never die — in fact, they don't even fade away.

   The worst offenders: Younger People Lax on Password Choice: Study.

   Related reading: Check Your Password — Is It Strong?

10. Security Tip: Before Being Interviewed on TV, Wipe Passwords off Whiteboard
Sophos

    If you haven't already guessed, Hasło is the Polish [word] for "Password."

    As we have explained before, if a TV crew is visiting your office it may be sensible to remove any passwords which could appear in the background.

    In fact, maybe it makes sense not to have these passwords on show regardless of whether someone is pointing a video camera around the place or not.

    Just saying ...