***Author: Andrew Hayter; Security Evangelist, G Data Software***

If 2015 was the Year of the Breach, will 2016 become the year of the ransomware? With company breaches of personally identifiable information (PII) happening in epidemic proportions during 2015, will that threat be overtaken by threats from the recent proliferation of ransomware?

Ransomware is not going away anytime soon. There is much education needed for the vulnerable and non tech-savvy public. None of the popular operating systems are immune to ransomware. We are now seeing ransomware targeting just about every operating system platform with recently Linux machines infected, joining Windows, Android, and iOS as at risk. And to be sure, paying the ransom is not an option.  Paying ransoms only funds more criminal activity.

High profile data breaches will continue unabated, as the attack surface is rich with targets that are not properly protected. In 2015 we have seen everything from small successful attacks right up to the OPM breach, which saw 21 million records of PII taken.  This suggests that there are many more, equally vulnerable systems out there to compromise.

**The New Threat Kid on the Block**

Could this also be the year of mobile malware?  Pervasive mobile apps will also likely be infected with malware and distributed through the Google Play and iOS App stores. Mobile device users are becoming a larger target as the number of devices grows.  Many people own multiple devices and so the attack surface is huge. Additionally, the temptation to download and install apps from less than reputable sources will continue to bring malware along for the ride.

Social Engineering will continue to pay off for those that take the time to do the research to find the right information and subject to steal credentials from, which is turn is often used to further penetrate a corporate system. Closely aligned with social engineering is phishing.  Phishing will continue to bait the unsuspecting in to click on malicious links or attachments. This leads to infections with Trojan Horses or malware creating a serious problem for the end-user and their systems.

**Haunted By Lack of Experts**

Pre-installed malware becomes an unwanted accessory to Android phones and tablets.  It has been known for a couple of years now that many new Android mobile phones come pre-installed with malware.  Just recently it was discovered that many off-brand tablets also come with this pre-installed malware. Do you get what you pay for?  It’s possible that the less expensive brands have less control over their supply and distribution chains, causing the device to become infected.

In summary, 2016 looks to be as bad a year for cyber-threats as any year we have seen.  Corporations will be targeted, governments will be exposed and end-users will be their own worst enemy.