Global Security Report: End of Year 2016

2016 was another tumultuous year in the realm of cybersecurity. Attackers leveraged many new attack vectors, as well as utilizing other tried and true methods that have been successful in the past, to net billions of dollars along the way. The victims of these attacks ranged across a broad spectrum from small business to some of the largest public and private organizations in the world.

If 2015 was the "year of the breach," then 2016 was the "year of the ransom." Ransomware boomed in 2016 with the majority of malware attacks being ransomware. However, the breaches did continue with some of the big names suffering some major setbacks.

New cybersecurity legislation took form in an effort to curb the efforts of cybercrime rings operating globally, while a new threat gained prominence in the form of a botnet (comprised of millions of IoT devices) capable of committing DDoS attacks with the likes that we have never seen.

https://appriver.wistia.com/medias/6y99654pn2

Ransomware as a Service

Ransomware is a notorious household name; it is the thief that holds one's files hostage until he pays the ransom to have his files safely returned to him. With the profitability of ransomware coupled with consumers having lax online security, the problem is likely to get worse.

Ransomware has proven to be extremely lucrative for malware authors. From the early days of CryptoLocker and CryptoWall, it was easy to tell this was going to bring in big amounts of cash to the parties that run the servers behind the infections. So much so that the future of ransomware seems to be heading in a more "user-friendly" direction for those wishing to run their own attacks and have the cash to do it.

Ransomware authors follow the same business cycle steps as normal computer coders, with the glaring exception that their illegal business is sold on the Dark Web. Malware authors offer their software to individuals or groups that are willing to distribute it—for a commission. The ransoms are paid to the author and then back to the distributor of the malware (with the developer

taking a cut of the cash). With examples provided, information on how to run the ransomware, and in some cases even support, it makes it easier than ever to get in to ransomware cybercrime.

Open source ransomware is also an option. It started out with a researcher posting open sourced code online for a ransomware tool he built. This software though had some purposefully built-in backdoors. With minimal effort, damage could be undone if a ransomware victim knew what to look for. To combat this, however, cybercriminals developed Ded Cryptor ransomware based on an open sourced version. With the purposefully built in weaknesses removed, Ded Cryptor isn't the only ransomware based on open source. With many other variants out there, it's likely a tactic that will grow in time as creators advance ideas and methods along.

New Legislation Aims to Protect Consumers and Intelligence Agencies

Early in the year, the EU governing bodies passed a new regulation known as the General Data Protection Regulation (GDPR). Intended to strengthen data security and protection in the EU, the GDPR aimed to simplify regulation under one unifying body within the EU. While it was officially adopted in April 2016, there will be a two-year transition period, so it won't be fully in place until 2018.

The regulation applies to both the processor of data based inside the EU or any outside the EU that are processing data for a resident of the EU. The term data seems to be applied fairly liberally in scope as it covers a wide range of person identifiers. While the new regulations will hopefully provide some much needed continuity throughout the EU with regards to data protection, it also carries some very harsh penalties including fines of up to four percent of a company's global turnover.

How this legislation will impact the UK remains to be seen given the outcome of the BREXIT vote and the UK's intention to leave the EU which should begin early 2017. However, the UK passed some of its own legislation in 2016 when the Investigatory Powers Bill passed both houses of parliament in November. The bill was hotly contested over the past year with opposition dubbing it the "snoopers' charter." The law would require telecoms to keep a detailed history of every user's Web activity (browser history, etc.) for a minimum of one year.

The bill also includes measures granting police and intelligence services the authority to hack into networks, computers and mobile devices when a warrant has been issued. The bill is intended to bolster the abilities and effectiveness of the state's intelligence agencies, and while they are certainly tasked with some paramount responsibilities (like protecting from terrorist attacks), the passage of a bill with so many privacy implications has certainly raised some eyebrows.

Meanwhile, the US has taken similar action by granting intelligence and law enforcement more latitude when investigating computer investigations. Under this new amendment to "Rule 41," investigators will have the right to search many computers anywhere in the US under one single warrant. Previously, the were tasked with getting warrants not just state by state but usually county by county. And while this is a welcome streamlining by those law enforcement agencies it has also been met with some resistance by opposition citing privacy violations as well as a violation of Fourth Amendment rights.

IoT Bots: the Rise of the Behemoth

The Internet of Things (IoT) has been a catchy phrase the past few years with the evergreen popularity of Internet-enabled devices. This term covers essentially most things on the Internet that are not computers or mobile devices; think along the lines of thermostats, refrigerators, smart watches, and webcams. Undoubtedly, checking the nanny or pet cam from one's phone, or setting one's house's temperature before heading home from work is pretty nice.

The growing popularity in Internet-connected smart devices is now starting to shine a bright light on the glaring lack of security these devices employ. Like staring in to a dark abyss, IoT devices with poor security have stared right back with their beady little eyes. In full force and on a global scale, botnets based on infected IoT devices popped up in large numbers in 2016. The amount of junk traffic these botnets could create for a DDoS (distributed denial of service) attack was staggering.

At the moment, the most popular IoT botnet is known as Mirai. This botnet was seen in the later part for 2016 being involved with DDoS attacks in excess of 600 gigabits per second. Attacks like these against websites or service providers brings any usability of their services down to zero during the attacks. This attack was used against the DNS provider Dyn, which in turn effected

services of large content providers like Twitter, Netflix, and Reddit during the attack.

The security issue with these devices comes from a lack of good security practices from the beginning of the device's creation. With issues like unpatched vulnerabilities and hard-coded default passwords on devices, it makes it much simpler for an attacker to gain access and use the devices for nefarious reasons. With most smart devices running some form of Linux, they are essentially small computers. Not taking their security serious in the same way a person would for a normal computer ends up being the downfall in the device's security.

So how does this problem get fixed? This may be the scarier part. Most vulnerable devices may never be fixed. This is due to a number of reasons. The manufacturer could be out of business, the device could already be end-of-lifed by the manufacturer and have no more updates, or the manufacturer may not even care enough to fix it. Some manufacturers are at least going the extra step in trying to better their products. NETGEAR announced a bug bounty on many of their systems and hardware that will help them make a more robust service and product line, as well as provide incentive for researches to make some extra cash by reporting flaws for a reward instead of using them for more nefarious reasons.

So what if device creators do release updates and patches to fix some of these issues? Well, that may not matter much either as most of these must be updated manually. Although often roundabout, webcams, routers, and other devices usually have an option in their interface to update the software.

However, most users with these devices are either ignorant or indifferent to the necessity of updating them. With how easy most of these are to set up (like just plugging in a webcam and scanning a QR sticker on the bottom) the amount of IoT devices is bound to keep growing.

The Federal Trade Commission recently announced a contest aimed at solving this problem. With a top prize of $25,000, they are looking for bright ideas on how to address the growing concern of IoT security, such as a home device that can update IoT devices automatically or any number of different ways to secure those devices.

Spearphishing Leads to Business Email Compromise

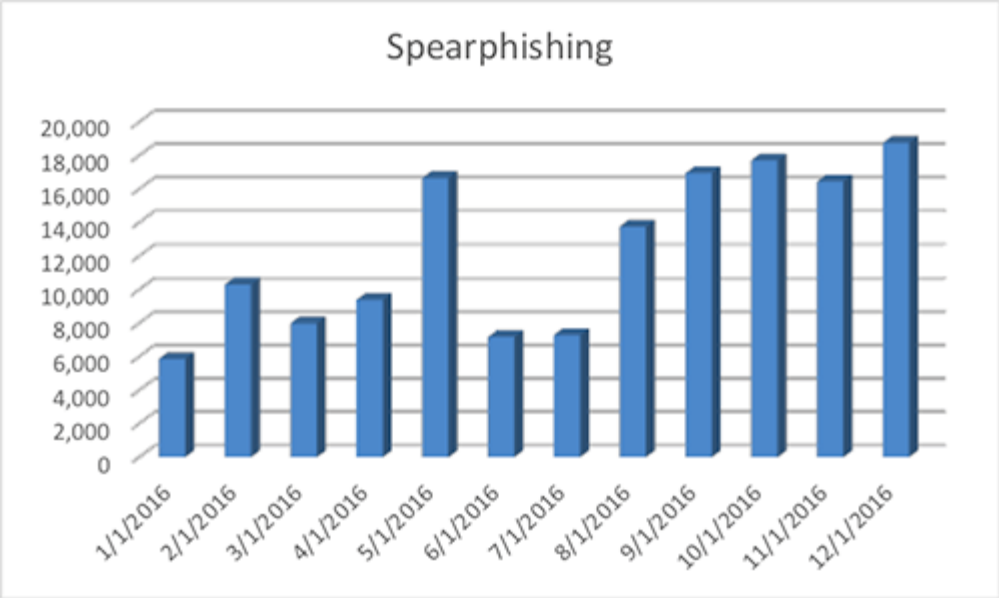
Today's phishing attacks range from highly targeted spearphishing to the more traditional cast net style attack. In both cases, cybercriminals have continued to hone their techniques to improve their success rate against their targets by adding greater detail and customization. Some of the more common phishing attacks seen in 2016 involved the use of attached HTM/HTML pages as well as PDFs with embedded links to phishing websites. In most cases, these were new variants of classic phishing techniques that have been in use for years. One relatively new technique uses spearphishing to commit wire transfer fraud (also known as BEC).

Business Email Compromise (BEC) started picking up in October 2015, and persisted throughout 2016. The details of the attack are evidence that the cybercriminals have spent time carefully gathering enough intelligence about the organization to craft an attack that is highly targeted. We have seen evidence suggesting that these attackers are utilizing social media sites like LinkedIn to gather intelligence.

These messages can be innocuous at first, with the hacker (disguised as an executive or internal employee) asking the victims if they are at their desks. To pull this off, the hacker sends the emails using a display address of the company's domain, but uses a reply-to address of an external domain, often a free email service. Using this method, the victims can often end up conversing with the hacker via email without realizing they are being duped.

These attacks have proven so effective that the FBI even released a recent warning about the increased traffic associated with this threat. According to the FBI, losses from this form of attack has totaled $2.3 billion since October 2013 with losses averaging $25,000-$75,000 per incident. AppRiver's SecureTide has its own proprietary technology that allows for the identification and quarantine of this type of attack.

The chart below depicts the spearphishing attack trend throughout 2016. As you can see, they are happening with greater frequency. In 2016, AppRiver's filters successfully captured roughly 150,000 of these attacks, each one highly targeted and personalized/customized.



Server Compromise

Data breaches have, unfortunately, become common to hear about these days. With so many organizations growing more and more of a networked footprint, it increases the pool of companies that can be targeted as well as the attack surface each company now has to defend. The year of 2016 was no different with some rather high profile data breaches occurring. Below, we've broken them down by sector.

Government: Close to 30,000 employee records of FBI and DHS agents were leaked online after the governmental departments suffered a data breach. The IRS had a data breach of citizen records in the estimated area of 700,000 affected users due to a flaw in part of their system to check tax records. Late in 2016, the US Election Assistance Commission (they are in charge of certifying the security of voting machines) announced they suffered a hack and found out by finding their login credentials for sale online. More than a hundred credentials were for sale and some included “the highest administrative privileges." The Illinois Board of Elections suffered a hack in which up to 20,000 personal voter records may have been compromised. Arizona State Board of Elections had up to 200,000 compromised.

LinkedIn: In Q2 of 2016, the business oriented social network site LinkedIn announced details about a data breach of user passwords totaling around 167

million. This was another case where the actual details were stolen long before a bigger announcement was made. In this case they believe the encrypted passwords were stolen in 2012, but the full depth of how much information was taken was not found out until years later.

MySpace: The MySpace data breach announcement came around the same time as LinkedIn's announcement, but the MySpace affected user count was close to 430 million user details taken. The accounts effected were believed to be older ones as well, users prior to 2013. Stealing user information from social networking platforms is popular as hacked accounts are used to push malware, generate ad revenue through clicks, or even for hackers to tout their hacking prowess.

Yahoo: One of the more recent breaches and likely the largest we know that happened in 2016 was the user data breach related to Yahoo accounts. Clocking in at around one billion users affected, it was a big one. While they believe the breach itself happened around 2013, this discovery and subsequent public announcement of a breach came at a bad time for Yahoo. Verizon Communications has been signing agreements and looking to purchase Yahoo's business. With bad news like this affecting the Yahoo image as a whole, this could cause some raucous waves in the business agreements being hammered out.

Botnet takedowns Short-lived

Over the past year, it seems that malware levels are consistently doubling themselves every quarter. However, suddenly and without warning, there was a global disruption in malicious email traffic—falling to less than one tenth of prior daily volume. As of June 1, 2016, malware traffic was down by 90-95 percent, begging the question "Why?"

This drop in traffic was driven in large part by a period of inactivity from the Necurs botnet, which until June 1 had been driving the massive distribution of both Locky Ransomware and the Dridex Trojan.

This was reminiscent of an event back in 2015 when Necurs had "gone dark" (albeit temporarily) immediately following the arrest of a Dridex botnet administrators. On that very same day, news broke of the Russian-based cybercrime group commonly referred to as Lurk or Buhtrap (based on the

malware families they commonly used to infect their targets) had been arrested in a coordinated multi-regional arrest. When the dust settled, 50 individuals had been arrested in connection to the group that had been wreaking havoc on banks across Russia for months.

The Lurk/Buhtrap group had been operating since at least 2011, and over the years had transitioned from attacking consumers to committing highly targeted attacks aimed exclusively at Russian banks, using phishing emails to compromise their targets. These attacks have become much more sophisticated from when the group first appeared. Before their arrest, they would successfully compromise at least 13 Russian banks and steal in excess of $25 million (1.7bn Roubles).

So what is the connection between this Russian group and the drop off in global malware traffic? Perhaps just timing. Maybe the Necurs operators were temporarily spooked. At any rate, the respite from Necurs was short-lived and on June 21, 2016, it resumed blasting huge malware bursts. Since then, Necurs has sustained the constant barrage of malware attachments and further solidified itself as the largest worldwide botnet in operation with what we believe is close to 10 million bot nodes globally.

Mobile Malware going Mainstream

Malware designed to target mobile devices has been growing in recent years. 2016 was the year that it finally started to garner some major headlines as it began to have much broader sweeping impact than in years past.

A great example of this is the “Gooligan” malware discovered by researchers at Checkpoint Security. This threat made headlines in November as it was said to have been discovered on over one million Android devices. The malware affected multiple versions of the OS and was essentially a huge advertising fraud scheme that would download apps from the Google Play Store and rank them with five stars. Forbes reported that the scheme may be netting the perpetrators as much as $320,000 per month. And though Google has stated that they saw no evidence that the infections had been used to access personal information like emails or account details, that possibility still exists and could be leveraged at any point.

Gooligan was reportedly based on an older piece of malware known as Ghost Push. Ghost Push was already one of the most prolific forms of mobile malware circulating in 2015, which goes to show the evolution of these threats over time. As more ways are found to monetize this sort of activity, the threats will evolve through whatever necessity dictates.

Android OS, in particular third party app markets, is still the hotbed for this sort of activity. However, there may be more on horizon for iPhone users.

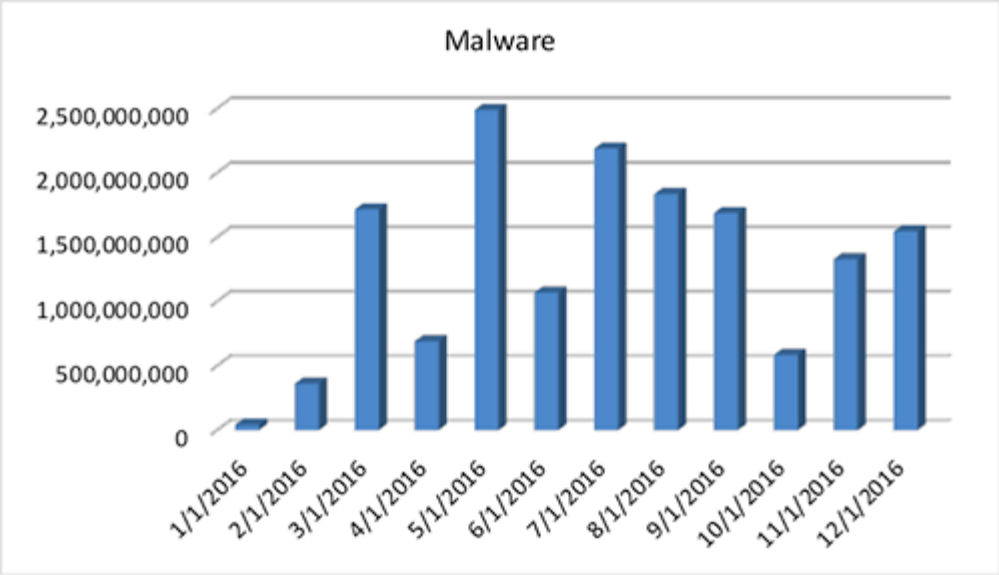
In August, Apple released a security update for vulnerabilities that had been disclosed to them as a result of the recent discovery of a very advanced exploit chain-type malware. The malware some are now referring to as “Trident” used multiple “zero-day” exploits that could essentially jailbreak an iOS9 device, thus giving the attacker access to emails, texts, voice calls and the phones camera, microphone and location. This malware was discovered only after malicious links leading to the exploit were sent to a human rights defender in the UAE. There is no telling how many times this threat had been used in the time from its creation to until the time Apple patched the exploits, but was certainly greater than zero. It was later discovered that it had been created and presumably sold by NSO Group—a company that specializes in “cyber warfare.”

Now that this exploit has made it into the wild, we are likely to see it--much like a biological virus—come back to us in a new mutated form.

Malware Traffic

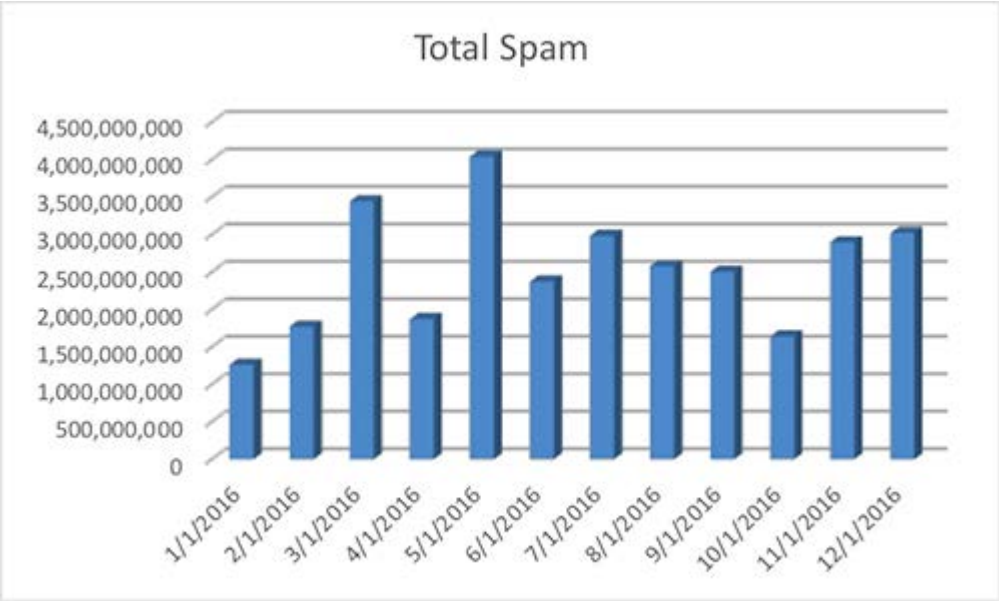
In 2016, our SecureTide email solution quarantined about 15.5 billion emails containing malware. Malware volume skyrocketed this year, increasing by over 800 percent from the previous year.

This year’s malicious traffic relied heavily upon the use of macro embedded documents and malicious JavaScript attachments. Attackers also utilized the more traditional zipped executable approach along with some less common methods, like the use of legacy Word template files. Below you can see the steady increase of malicious email activity over the past four quarters.



Spam Traffic

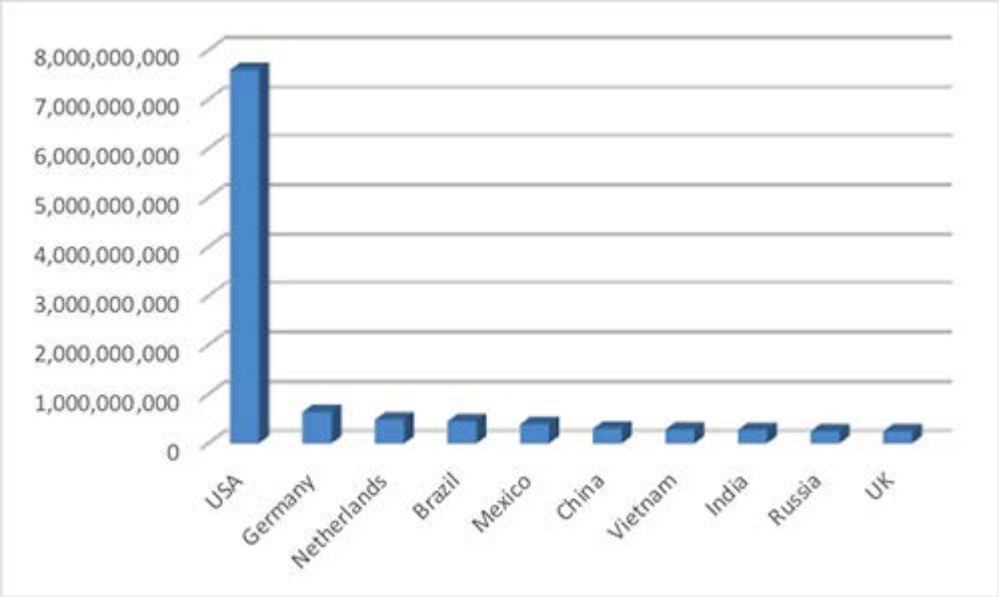
Total spam traffic remained steady in 2016. In total we quarantined 30.4 billion spam messages in 2016. Just over half of those messages either containing or leading directly to a malware payload.



("Spam" is defined here as any unwanted message)

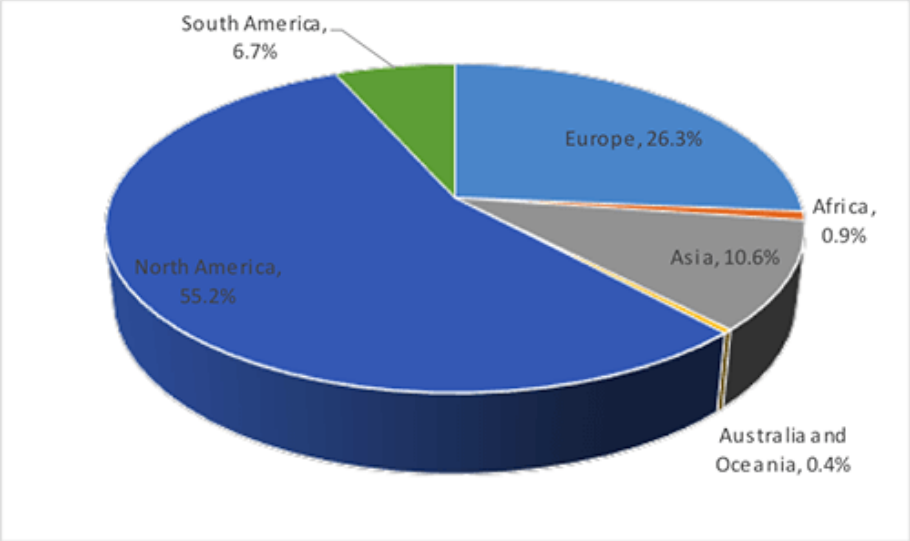
Top Ten

Of the billions of spam messages quarantined in 2016, nearly 70 percent of them originated in one of these ten countries. Once again the US led the way blasting out nearly ten times as much spam volume as the second highest country (Germany).



Spam Traffic by Region

The chart below represents the global distribution of spam sources by region as seen by our filters.



2017 Predictions

- IoT botnets will continue to wreak havoc: While device manufacturers and service providers alike are ramping up efforts to combat IoT botnet activity, over the short term this problem will only get worse. Expect to see more wide sweeping and major disruptions to the Web due to IoT botnets being leveraged to commit DDoS attacks.
- Ransomware will continue to be the most prolific threat on the web today: Expect to see more variation and customization with these attacks given the attackers propensity to innovate new ways to make a profit and that profit may bear out some record setting cybercrime earnings in 2017. We also expect to see some new variants that target so other IoT devices to be held for ransom.
- Mobile malware will finally become a household name: The rise of malware designed to target mobile operating systems has been building over the years, but 2017 may be the year when the issue becomes more widespread, perhaps driven by an explosion in mobile ransomware. As people are now doing so many things from their smartphone like shopping, banking and paying bills this provides a fertile ground for the attackers looking to take advantage.
- New legislation will be passed to give more investigative powers to law enforcement: New legislation in the UK and US has granted far greater powers to investigative agencies when dealing with computer access and warrants. This should lead to a least several big wins for law enforcement combatting computer crimes.
- Acts of cyber aggression will become the new front lines between nation states: 2016 saw an escalation of cyber espionage by nation states. And while we are becoming more and more cognizant of cyber hacks by nation-states, there are likely still hundreds, possibly thousands, that we are not privy to. We predict that we will see these hacks continue to ramp up as the stakes get higher and higher.