Issue date: October 2015
CYBER EXTORTION RISK REPORT 2015

Contents

Introduction ........................................ 3

Statistics ........................................... 3
  Total cost of cybercrimes in five countries ....... 3
  Type of cyber attacks ............................. 4
  Average days to resolve attack .................. 4
  Average annualised cybercrime cost weighted by attack type ....... 5

Types of threats .................................. 5
  Denial of Service (DoS) .......................... 5
  Stealing confidential data ....................... 12
  Sextortion .................................... 17
  Ransomware / data kidnapping ................. 19
  Mobile device ransomware ..................... 22
    Android .................................... 22
    Apple iOS .................................. 23

Outlook for 2016 ................................... 23

NYA cyber response and consultancy ............. 25
Introduction

In 2015 according to the United Nations Broadband Commission for Digital Development more than 3.1 billion people (43% of the world population) accessed the Internet regularly and 40% of all mobile subscriptions are smartphones. By 2020 it is estimated that more than 4 billion people will have regular access to the Internet and 70% of all mobile subscriptions will be smartphones. The opportunity for cybercrimes is immense and was estimated by McAfee in June 2014 to have cost the global economy a “conservative estimate” of USD375 billion. In the UK GHCQ and MI5 stated in January 2015 that eight in every 10 large British companies suffered a serious cyber security breach during 2014.

Cyber extortion like kidnap for ransom, traditional extortion and maritime piracy remains massively underreported. The City of London Police and the FBI both estimate that 85% of national cybercrimes are not reported. As a result information is confined to open source material and gives a selective and incomplete view of cyber extortion. This was seen most dramatically in October 2015 when cybercrimes were recorded for the first time in UK national crime statistics, as a result the national crime rate increased by 107%.

Cybercrimes in general and cyber extortion in particular are growing threats to individuals, businesses and organisations globally. Similar to other organised crime, cybercrime is a transnational phenomenon which the UN Office on Drugs and Crime describe as “a borderless realm”. Consequently solving a case, as Europol states is “often complex and resource intensive”.

Statistics

Total cost of cybercrimes in seven countries (in millions)

<table>
<thead>
<tr>
<th>Country</th>
<th>FY2013</th>
<th>FY2014</th>
<th>FY2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>$11.56</td>
<td>$12.69</td>
<td>$15.42</td>
</tr>
<tr>
<td>Germany</td>
<td>$7.56</td>
<td>$6.13</td>
<td>$7.50</td>
</tr>
<tr>
<td>Japan</td>
<td>$6.73</td>
<td>$6.91</td>
<td>$6.81</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>$4.72</td>
<td>$5.80</td>
<td>$6.32</td>
</tr>
<tr>
<td>Brazil*</td>
<td>$3.85</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Australia</td>
<td>$3.67</td>
<td>$3.99</td>
<td>$3.47</td>
</tr>
<tr>
<td>Russia*</td>
<td>$3.33</td>
<td>$2.37</td>
<td></td>
</tr>
</tbody>
</table>

Source: ‘2015 Cost of Cybercrime Study: United States,’ Ponemon Institute, October 2015

Ponemon Institute estimates the average cost of annualised cybercrime in 2015 to USD7.7 million (with a range from USD0.31 million to USD65 million). The HM Government-sponsored PWC
Information Security Breaches Survey 2015 found that for companies employing more than 500 people, average costs of cybercrime was between USD2.2 million and USD4.8 million. For small and medium-sized enterprises (SME), the average cost was between USD115,000 and USD477,340.

**Types of cyber attack**

The above graph summarises the types of attack methods experienced by participating companies since 2012. It is notable that malicious coding incidents have increased by 55% since 2012. In 2015 it was found that at least 1.9 successful attacks were conducted each week against surveyed businesses, up from 1.7 in 2014 and 1.4 in 2013. HM Government and PWC report found 90% of large organisations (up from 81%) and 74% of SMEs (up from 60%) had experienced a cyber security breach in the past year.

**Average days to resolve attack**

The above graph shows that the mean number of days to resolve a cyber attack is 46 days (up from 31 in 2014) at an average cost of USD21,155 per day or USD973,130 over the 46 day period to resolution*. This is an increase of 52% (up from USD639,462) in cost and 48% in time compared to 2014. (*Resolution does not necessarily mean the attack has been removed or stopped, as the attack may be dormant or undetected)

**Average annualised cybercrime cost weighted by attack type**

![Average annualised cybercrime cost weighted by attack type](image)


The above graph compares results over four years, showing the percentage of annualised cost of cybercrime allocated in nine attack types compiled from all benchmarked organisations. It is noticeable that the cost of all cybercrimes, apart from phishing, significantly declined.

**Types of threat**

**Denial of Service (DoS)**

DoS attacks are the traditional method of cyber criminals, involving the disabling of a target website by overloading it with ‘requests’ (i.e. visiting the webpage) from multiple computers, causing the target website to ‘crash.’ A distributed DoS attack (DDoS) involves the use of hundreds or thousands of compromised computers known as ‘botnets’ or ‘zombies’ to send these requests without the owner’s knowledge (most are home computers). Kaspersky Labs found in Q1 and Q2 of 2015 that DDoS attacks occurred in 79 countries but that 77% of attacks targeted resources in the same ten countries (China, USA, South Korea, Canada, Russia, France, Vietnam, Croatia, Germany and Hong Kong). These attacks originate from extortionist groups such as DD4BC, rented from hackers for hire for as little as USD38 per day or politically motivated co-ordinated assault from hacktivist collectives such as Anonymous and AntiSec. IDG Research Services found that DDoS attacks are on average not detected for 4.5 hours, and a further 4.9 hours passes before mitigation can commence. Kaspersky Labs reports that in Q2 2015 72.3% of attacks lasted less than four hours.
Despite the commonly held belief that DoS attacks do not result in the theft of information or other security loss, Neustar Insights annual survey in 2014 found 55% of DDoS targets were also victims of theft. This included the loss of customer data, loss of intellectual property and financial theft, with one attack on an undisclosed bank resulting a loss of USD9 million in 48 hours. The other financial impact comes from the loss of revenue, which may occur due to the loss of service during the attack and the time taken to retrieve that service. For example, businesses that rely heavily on Internet vending (i.e. online gambling) are commonly targeted during peak times to maximise the financial and reputational damage inflicted.

Targets for DoS extortion attacks vary significantly depending on the objective of the attack, traditionally these attacks target commerce websites who are reliant on a functioning website for revenue. Verizon Data Breach Investigations Report for 2015 found that 2014 DDoS incidents mostly targeted public institutions, retailers, financial services, administrative and professional services. Other targets have included Bitcoin exchanges, gambling and online casinos but also purely Internet based companies of all sectors and services. Throughout 2015 an emerging trend has seen financial institutions targeted in sustained DDoS attacks. Ransoms or extortion payments are demanded almost exclusively in Bitcoins due to their anonymity. Publically released demands range from USD250 to USD25,000, though often are in the hundreds.

In 2015 there has been an increase in DDoS attacks for non-extortion related objectives. Attackers' objectives can be political (either state-sponsored action or Hacktivist) or retaliatory against law enforcement actions. Some attacks have even been launched without an identifiable motive. The last category ranges from those determined to demonstrate their ability to conduct attacks through to highlighting security flaws in the attacks network capabilities. These attacks have targeted governmental, academic, law enforcement, gambling, political and NGO websites.

![Number of DDoS attacks by victim industry sector using 2435 incidents recorded in 2014. Source: 'Verizon 2015 Data Breach Investigation Report'](image_url)

![Biggest Impact of DDoS outages:](image_url)

*Source: 'Neustar Annual DDoS Attacks and Impact Report – 2014 The Danger Deepens'*
Recent Cases

- **30 September 2015 – Government of Thailand (Thailand)** – Thai Government Portal, Finance Ministry, Ministry of Information and Communication Technology, state owned CAT Telecom and International Security Operations Command (ISOC) were taken offline for most of the evening in a planned hacktivist attack. The attack was in response to Bangkok’s plans to create a government run ‘Single Gateway’ for all Internet traffic.

- **28 September 2015 – Rutgers State University (USA)** – A DDoS attack affected IT services across the university network, resulting in periodic outages in campus Wi-Fi, email services and two university online resource platforms. The attack resulted in cancelled classes and exams, the inability to submit electronic assignments and failures in the enrolment system. This was the fourth DDoS attack on the university since November 2014 and the first since a USD3 million upgrade in network security. The upgrade had forced Rutgers to raise tuition fees by 2.3%. An alleged hacker, Exfocus, taunted Rutgers officials and students on Reddit, Twitter and other social media claimed he was paid USD500 per hour in Bitcoins to conduct the attack. In response, petitions formed calling for refunds in tuition fees due to the effects of the attacks on their education.

- **02 September 2015 – Greater Manchester Police (UK)** – A Lithuanian hacker caused the police constabulary force website to be taken offline twice in a night. The hacker through Twitter told local press that the attack was ‘to show the failure of security in these large systems’.

- **01 September 2015 – National Crime Agency (UK)** – Hacking group Lizard Squad took the NCA website offline briefly in retaliation for the arrest of six suspects on cybercrimes.

- **05 August 2015 – Carphone Warehouse (UK)** – Three sub-divisions (OneStopPhoneShop, e2save and Mobiles) websites went offline in a sizeable DDoS attack. However the attack was a cover to help infiltrate the retailers databases, as a result names, addresses, dates of birth and bank details of 2.4 million customers were stolen from the three sub-divisions, iD Mobile, Carphone Warehouse as well as data stored for Talk Mobile and TalkTalk Mobile. Amongst the data was also 90,000 encrypted customer credit card details. The Information Commissioners Office announced it was to investigate the incident. Public and press criticism was levelled at Carphone Warehouse for their response to the incident, including not reporting the incident to the Metropolitan Police despite informing the press that it had.

- **31 July 2015 – Unknown businesses (USA)** – The Internet Crime Complaint Center (IC3) and FBI issued a public service announcement warning of “an increasing number of complaints from businesses reporting extortion campaigns via email. In a typical complaint, the victim business receives an email threatening a Distributed Denial of Service (DDoS) attack to its Website unless it pays a ransom. Ransoms vary in price and are usually demanded in Bitcoin. Victims that do not pay the ransom receive a subsequent threatening email claiming that the ransom will significantly increase if the victim fails to pay within the time frame given.”

- **31 July 2015 – Royal Bank of Scotland Group (UK)** – RBS Group suffered a DDoS attack that prevented its 6.5 million customers from accessing NatWest, RBS and Ulster online accounts for 50 minutes. The attack occurred on a Friday as monthly salaries were being processed. In December 2013 NatWest and RBS online accounts were affected for less than a day under a DDoS attack, again timed to coincide with the monthly salary payments.

- **21 June 2015 – LOT Polish Airlines (Poland)** – A DDoS attack on the over-ground terrestrial telecommunication network caused the flight plan systems to go offline and forced the airline to cancel 10 flights and delay 12 others on its European routes, temporarily grounding 1,400 passengers at Warsaw Chopin Airport.
• 17 June 2015 – Government of Canada (Canada) – Hacktivist group Anonymous attacked the main IP address of the Government of Canada in response to the C-51 anti-terror bill, the incident caused the websites for nearly all Federal Government departments to be taken offline. For at least two hours email accounts of government employees were also inaccessible.

• 21 May 2015 – Financial organisations (Iceland) – Two cyber security companies’ state in a press release that DD4BC and other criminal groups have targeted organisations in Iceland with extortion related DDoS attacks.

• 09 May 2015 – Bank of China and Bank of East Asia (Hong Kong SAR) – The websites of both financial institutions were attacked in a DDoS attack. The matter was referred to Hong Kong Police once emails demanding payments in Bitcoins in exchange for no future attacks were received. The Cyber Security and Technology Crime Bureau reported that preliminary investigations revealed the attack came from multiple countries. Hong Kong media believed the hacking group, DD4BC was behind the incident.

• 08 May 2015 – Several high profile targets (Switzerland) – Swiss Governmental Computer Emergency Response Team advised that it was “aware of several high profile targets in Switzerland that have recently received a blackmail from DD4BC and have subsequently suffered from DDoS attacks”.

• 06 May 2015 – At least five unknown organisations (New Zealand and Australia) – The National Cyber Security Centre (NCSC) issued a security advisory stating “several organisations have received extortion emails threatening a sustained DoS unless a payment is made to the email sender. To demonstrate that the threat is credible, shortly after receiving the extortion email, the organisations are then hit with a short-duration DoS attack, lasting up to an hour”. The New Zealand Internet Task Force (NZITF) advised “at least four New Zealand organisations that NZITF knows of have been affected so far. A number of Australian organisations have also been affected”. The attacker sent emails to both support and helpdesk email addresses or targeted individuals. The ransoms commonly shared a request for 25 Bitcoins and were associated with the hacking group, DD4BC.

• 09 April 2015 – Pokerstars (Costa Rica) – An online casino was hit by DDoS attacks that take the website offline for several hours. Pokerstars was mentioned in a DD4BC extortion email as a previous target on 10 April.

• 09 April 2015 – Redbet.com (Malta) – Sports gambling website experienced a sustained DDoS attack lasting approximately a week. The company told customers on a forum “last week we received an email from a group of hackers threatening to disrupt our services with a DDoS attack should a ransom payment not be made”.

• 20 March 2015 – GreatFire (Unknown) – Not for profit activist group, which monitors blocked websites and keywords in the People’s Republic of China, came under a sustained DDoS attack. The website received 2,500 times the normal traffic or 2.6 billion request per hour, causing their bandwidth costs to increase to USD30,000 per day. The attack spread to the American coding website, GitHub, as traffic was redirected from Chinese search engine Baidu to two GitHub’s webpages which contained links to websites banned in China (one of which was run by GreatFire). The attack lasted for five days and is widely attributed to Chinese authorities.

• 12 March 2015 – Bitmain (PRC) – An email was received from the hacking group DD4BC threatening Bitmain and their services (Bitmain Technologies, AntPool and Hashnest). That day the company released a public statement saying we “will not invite future attacks of this sort by giving in to the demands of hackers”. The 10 Bitcoin ransom demanded was used to offer a bounty for the full and proven identity of DD4BC, this remains unclaimed.
Redacted copy of the extortion email received by Bitmain

Hello,

To introduce ourselves first:

http://bitcoinbountyhunter.com/8h3o.html
owner-accuses-costa-of-withholding-info

Or just google “DD4BC” and you will find more info.

So, it’s your turn.

Unless you pay 10 BTC to [redacted] within 12 hours from now, your pool servers are going under heavy DDoS attack.

Pay, and you will never hear from us again.

Usually, we attack first, then ask BTC to stop, but since your pool is too big, one of the largest Bitcoin pools, we are giving you time to act first, because we are well aware that even 1 hour offline would cause much larger damage than 10 BTC.

12 hours, because we are not in the same time zone and it’s morning in china, so we want to make sure that you had time to act.

AS PROOF that this is not an empty threat, we will run a small attack on your servers now – [IP REDACTED]. Don’t worry it’s not going to be hard and will run for just 1 hour, so your server will not get null routed.

But if not paid, all your servers are going down for good.

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps.

IMPORTANT: You don’t even have to reply, just pay 10 BTC to [REDACTED] – we will know it’s you and you will never hear from us again.

But if you ignore us, attack will start and price to stop will go up to 20 BTC and will keep going up for every day of delay.

ONE MORE TIME: It’s a one-time payment. Pay and you will not hear from us ever again!

Thank you.

Redacted copy of the extortion email received by Bitmain

- **11 February 2015 – Government of The Netherlands (Netherlands)** – The Hague released a brief statement to confirm that for most of the day the Dutch government websites were taken offline in a DDoS attack. Newspapers and telecom provider, Telford, were also affected.

- **25 December 2014 – Sony PlayStation and Microsoft Xbox (Worldwide)** - Hacking group, Lizard Squad, overwhelmed the Microsoft Xbox Live and Sony PlayStation networks on Christmas Day. The service was taken offline completely for the combined 158 million subscribers. Member Two from Lizard Squad responded to media requests over why the group had attacked the network by stating ‘because we can’. Microsoft restored Xbox Live services shortly after the initial attack, however Sony took more than two days to restore its PlayStation Network.

- **13 October 2014 – Cex.io (UK)** – Bitcoin exchange website attacked in a DDoS attack by DD4BC, an extortion demand of two Bitcoins was received for stopping the attack.

- **25 September 2014 – Nitrogen Sports (Costa Rica)** – Online Bitcoin sports gambling website sustained a DDoS extortion attack lasting up to 16 November 2014. Attacker, allegedly DD4BC, posts taunting messages on forums and emails the company with demands for two Bitcoins. The company told the media “this particular hacker has been attacking us since July. We actually did pay him for a while to buy ourselves some time to put additional protections in place. He has escalated his attacks and his demand for money, and we felt that it was time to take a stand”.
Forum posts by DD4BC taunting Nitrogen Sports

- **17 June 2014 – Code Space (USA)** - A code hosting company collapsed following an extensive hacking. The attack began on 17 June with a DDoS attack against its servers. The attack then gained control of Amazon EC2 Control Panel (a web service that offers cloud computing platforms to run their own applications). Upon discovering the hackers' access, the company attempted to regain control by changing passwords. However, the hacker had already created a number of backup logins and began deleting random parts of the panel. By the time the company regained control, the cyber attack had erased partially or all of its data, backups, machine configurations and offsite backups. Due to the cost of resolving the issue and expected refunds, the company was placed into an “irreversible position”, which led it to cease trading. The attack lasted just 12 hours.

- **11 June 2014 – Feedly / Evernote (USA)** – Two companies, the RSS Feed provider and note taking app producer, were hit by DDoS extortion attacks and caused both services to fall offline periodically over the next three days. The attacks increased in severity as the companies refused to discuss extortion payments and jointly cooperated with the FBI.

- **June 2014 – Moz (USA)** - Marketing analytics software company. The company’s chief technology officer, Anthony Skinner, brought in CloudFare but the attacks continued. The company refused to pay the initial demand of USD200, this subsequently increased to USD2,000. The company is co-operating with Feedly who were affected by a similar attack. The attack continued throughout June, the company refused to pay. The FBI believed the hacker
behind the attack was linked to the June 2014 DDoS attack on Move and the National Association of Realtor.

- **May 2014 – Plenty of Fish (POF) (Canada)** – The popular dating website (70 million members) was contacted at 06:54 PT warning of an impending DDoS attack. At 08:13 PT the five-hour attack began affecting approximately one million users, the website followed by iOS and Android apps were taken offline. An initial offer of USD2,000 was offered by the attacker’s Gmail address at 12:09 PT. The company responded by publicly releasing information on the attack and stating ‘it’s not unusual for a large target like us to receive threats that turn out to be false… we were certainly not interested in negotiating’.

Screenshots released by POF of the contact received from the attacker

- **16 April 2014 – Typepad (USA)** – Commercial blogging service used by media organisations including the BBC, Sky News, CBC, ABC and MSNBC suffered a six-day DDoS attack. The service was only online intermittently for at least five days. The company released very few details but described the attack as “similar to an attack on Basecamp”.

- **24 March 2014 – Basecamp (USA)** – Online project management software company experienced a DDoS extortion attack, the company refused to pay and as a result their services became unavailable. The attacker was identified through his Gmail address as being responsible for similar attacks.

- **February 2014 - Meetup (USA)** - Social network portal that facilitates offline group meetings. The attack occurred just four minutes from the initial demand, made by email to founder Scott Heiferman and chief technology officer, Gary Burns. Attack loaded 40 times the normal data flow onto the company’s site. The attack caused disruption for four days. Company decided not to pay, for fear of return of attacks or other groups targeting their services. Demand of USD300 in Bitcoins.

- **31 January 2014 – Vimeo (USA)** – Alternative video-sharing website main domain was taken offline in a DDoS attack, the service was restored on the evening of 01 February.

- **19 December 2013 – People’s Bank of China (PRC)** – Following the 05 December and 18 December decision by the central bank to stop accepting new deposits in Bitcoins, a DDoS attack was launched on the banks website and Weibo account.

- **July 2013 – Unknown gambling website (UK)** - Two Polish men arranged to meet the owner of the company (whom they had known for four years). They threatened to shut down the website unless he did not hand over half of the business (reportedly worth £30m). On 03 August the
company sustained a DDoS attack rendering the website inoperable for five hours, causing a loss of GBP32,000. Owner reported incident to Greater Manchester Police, both were subsequently convicted of cyber extortion.

Stealing confidential data

Cyber criminals continually attempt to exploit loopholes and security vulnerabilities within organisations’ IT systems in order to access confidential company details or customer data. Verizon 2015 Data Breach Investigation Report found that in 60% of cases attackers are able to compromise an organisation within minutes. Once successfully done, cyber extortionists notify the company and demand money upon the threat of publicly releasing data - causing service disruption, reputational damage and potential financial costs to the target organisation. As such, many organisations have given in to cyber extortionists and paid the demands. However, doing so could increase the risk of them being attacked again.

TrendMicro had concluded that healthcare insurers and providers have accounted for 26.9% of data breaches between 2005 and 2015, yet only 7% of these breaches were related to hacking (60% related to lost devices). Symantec recorded a 72% increase in cyber attacks on healthcare sector companies from 2013 to 2014. Hackers target the healthcare sector due to the high resale value of personal health records. Jim Trainor of the FBI Cyber Security Division stated that individual records are valued between USD20 to USD70. Online analysis by NPR in February 2015 revealed that a “value pack” of 10 Medicare numbers was valued at 22 Bitcoins (USD4,700) on the Deep Web. In comparison a list of 10,000 valid email addresses with customised filters (such as age, gender, country etc.) can sell for USD127.

One of the most worrying developments is the scale of hacking and data breaches. In 2014 Adobe, AOL, Apple, Dominos Pizza, eBay, Gmail, Home Depot, JP Morgan Chase, Nintendo, Snapchat, Target and UPS were hacked. Collectively these companies lost 512.21 million records (compared to 823 million records lost worldwide in all of 2013) and in the case of Home Depot the cost of simply refunding and reissuing data cost USD60 million. Target suffered a financial implication of USD172 million, a 7.7% drop in shares and a significant drop in consumer confidence. The CEO Gregg Steinhafel resigned after 35 years of service in the company.

Alternatively hackers can use the stolen data to create brand and reputational damage to the organisation, these data breaches may result in the full or partial publication of the breach onto Deep Web. Publication normally occurs shortly after the public announcement of the breach and exacerbates the reputational damage, as records are used by other cyber extortionists in identity theft crimes. State sponsored data breaches, the majority emerging from China, have targeted both public and private organisations across the world.

Recent Cases

- **21 October 2015 – TalkTalk (UK)** – Telecom group suffered a breach of its website resulting in the theft of up to four million current and former customer details (personal details, contact details, account numbers and card / bank account details). TalkTalk customers were unable to access the My Account section of the website on the afternoon and evening of 21 October as a result of a DDoS attack. On 23 October Chief Executive Dido Harding informed the media that she had received a ransom email from a hacker, customer data was reportedly on sale on the Deep Web. TalkTalk shares dropped by over 12% and reached its lowest level since 2013 in response to the announcement. This breach was the third cyberattack in a year to affect TalkTalk customers.

- **02 October 2015 – Scottrade (USA)** – Retail brokerage firm emailed its customers to inform them that the company had suffered a data breach on its networks. It is believed the breach occurred between late 2013 and early 2014 but remained undetected until the FBI informed
Scottrade. Approximately 4.6 million customer details, including client names and addresses were stolen.

- **01 October 2015 – Experian (Ireland)** – World’s largest consumer credit monitoring corporation revealed that hackers stole approximately 15 million sensitive personal records belonging to T-Mobile customers (25% of its customers). Information included identifying personal information, Social Security numbers, passport numbers and driving license numbers.

- **08 September 2015 – Excellus BlueCross BlueShield (USA)** – Health insurer suffered a hacking incident that stole more than 10 million identifying records.

- **07 August 2015 – American Airlines and Sabre Corp (USA)** – Chinese linked hackers attacked the travel reservation systems of both companies stealing traveller information.

- **July 2015 – Bitdefender (Romania)** – Internet security software company was attacked by a hacker called DetoxRansome that managed to penetrate the company servers and steal company login credentials for SME customers (approximately 1% of its client base). DetoxRansome sent tweets to the company demanding USD15,000 for the data and releasing more than 250 accounts and passwords. He offered to sell the data to journalists for eight Bitcoins. DetoxRansome Twitter account had similar messages offering to sell confidential data from fashion houses Louis Vuitton and Fendi, Gazprom and 67,000 credit card details.

- **17 July 2015 – UCLA Health System (USA)** – University of California hospital administration may have lost 4.5 million patient records but is still uncertain as to when the incident occurred and to what extent the hackers accessed files. UCLA admitted that patient records were not encrypted.

- **15 July 2015 – Ashley Madison and Established Men (Canada)** – Online dating service aimed at those wishing to have affairs was attacked by hacking group, The Impact Team. The group threatened to expose user data if the parent company did not cease operations. A data cache containing 37 million real names, home addresses, email addresses and credit card transaction records was released on 21 July, a day after Avid Life Media assured users of the security of its site. The data breach caused substantial reputational damage as it was revealed that Avid Life Media received USD1.7 million per year from users to delete profile data but it subsequently did not. At least four suicides have been attributed to the data breach. In August 2015 a USD567 million class-action lawsuit was brought against the company, shortly after the group chief Noel Biderman resigned. Following the publication of the data cache on the Deep Web cyber criminals utilised the personal data to begin multiple cybercrime campaigns against Ashley Madison users. Malware and spyware campaigns emerged following the publication with phishing email campaigns. Cyber extortionists began a targeted email campaign against users demanding Bitcoin extortions. The US Marine Corp investigated the matter to ensure “security standards compliance”.

Selection of tweets sent to Bitdefender from the extortionist Twitter account, DetoxRansome
Example of an Ashley Madison related extortion email. CloudMark Intelligent Network Security revealed Bitcoin transactions, netting approximately USD6,400 over a four day period

- **04 June 2015 – Akorn Inc (USA)** – Pharmaceutical company suffered a loss of 35,000 to 50,000 unique records from its customer database. On 20 April the company discovered that personal information was compromised through four employee email accounts. The hacker, using an alias ‘Mufasa’, posted on Deep Web forums offering the database and business related information to the highest bidder. ‘Mufasa’ offered to sell the data back to Akorn for USD5,000, yet there were “some offers on the table”.

- **May or June 2015 – United Continental Holdings (USA)** – Hackers stole millions of confidential data including flight manifests, passenger lists and passengers flight histories from United Airlines, it is also believed that the mergers and acquisition strategy was also stolen. Hackers are linked to previous Chinese data breaches involving the theft of security-clearance records from the US Office of Personnel Management and medical data from Anthem Inc. It is theorised that the theft from one of the largest US government contractors would allow the cross-referencing with other recent breaches to track specific government, intelligence and military officials.

- **14 May 2015 – mSpy (Russia or Ukraine)** – Parental mobile tracking app developers suffered a breach of more than 400,000 user records (20% of its customers), which was subsequently posted on the Deep Web. The data included Apple IDs and accompanying passwords, tracking data, 145,000 payment details, calendar data, corporate emails, photographs and private conversations. Deep Web forums revealed organising of data kidnapping against Apple iOS devices.

- **May 2015 – Adult Friend Finder (USA)** – Online adult-oriented social network suffered a loss of 3.5 million member details. Thai hacker ROR[RG] claimed that the company owed his friend USD250,000 in unpaid fees. As a result the leak was proof of an initial claim that ROR[RG] held the data and wished payment in full plus an additional USD100,000. The database of Adult Friend Finder later emerged for sale at USD17,000 but was later leaked for free on the Deep Web. Forum moderators noted that the database had been traded since early March 2015.

- **April 2015 – US Office of Personnel Management (USA)** – Hackers stole sensitive personnel information from 21.5 million federal workers and contractors in March 2014 but was only noticed in April 2015. The hack was discovered during an investigation into an unrelated April 2015 breach that resulted in the theft of 4.2 million records. The hack went deeper than initially thought when security-clearance related background information was found amongst that stolen.
Criticism from Democrats, Republicans and the House Committee on Oversight and Government Reform revealed that data was not encrypted. Director of the OPM, Katherine Archuleta, was forced to resign under pressure on 10 July 2015.

- **27 March 2015 – British Airways (UK)** – Hackers steal “a small proportion of its millions of customers” frequent-flyer Executive Club and Avios accounts (estimated to be tens of thousands). On 30 March British Airways and Iberia temporarily suspended the use of air miles to ensure the prevention of theft after reports emerged on social media of non-customer use of Avios and Executive Club points.

- **29 January 2015 – Premera (USA)** – Health insurer discovered a sophisticated hacking and theft of more than 11 million personal records dating back to 05 May 2014. Customers and former customers from Blue Cross, Blue Cross Blue Shield of Alaska and affiliate brands Vivacity and Connexion Insurance Solutions were affected. Investigations revealed that personal information including bank account, medical claims, clinical information and Social Security numbers were amongst the stolen data.

- **29 January 2015 – Anthem Inc. (USA)** – Health insurer informed customers that for several weeks in December 2014 hackers stole 80 million health plans of current and former members. It emerged that the personal information including names, dates of birth, Social Security numbers, health care ID numbers, addresses, email addresses, employment information and income data was not encrypted. The hack was highly sophisticated with a targeted phishing campaign aimed at high level IT access employees. At least five employees were tricked into using their network credentials which allowed access to the network.

- **07 January 2015 – Banque Cantonale de Geneve (BCGE) (Switzerland)** – Financial institution announced that hacking group, Rex Mundi, had stolen personal data of thousands of clients. A threat to publish 30,192 emails was made by the group unless USD11,437. BCGE refused to pay and at 17:00 UTC on 09 January 2015 half of the data breach was published online. Rex Mundi tweeted “If you are a BCGE customer, we are glad to let you know that your privacy is not worth 10,000EUR to your bank”.

- **25 December 2014 – China Railway Corporation (PRC)** – Two Chinese hackers stole 130,000 user details stored in the online ticket sale system (www.12306.cn) using account names and passwords leaked by other websites. The information including real names, ID numbers, phone and email contacts was then sold for an undisclosed profit. China Railway stated that the leak
was stemming from third party website plugins or apps used by 12306.cn. Both hackers were arrested by police.

- **18 December 2014 – National Industrial Credit Bank (Kenya)** – Two males hacked into the NIC Bank customer database and threatened to publish the information if they were not paid 200 Bitcoins (USD60,000). Both suspects were arrested.

- **21 November 2014 – Sony Pictures (USA)** – An email in broken English was sent to CEO Michael Lynton, Chairman Amy Pascal and other executives warning of “great damage” and asking for “monetary compensation” to avoid such a situation. The email was leaked following the 24 November malware attack on Sony Pictures that leaked more than 30,000 documents, 47,000 Social Security numbers, thousands of private emails, scripts and copies of upcoming film releases. Sony Co-Chairman Amy Pascal resigned in the wake of the scandal, it is estimated that the leaks cost Sony in excess of USD35 million.

Despite the confirmation from the White House, FBI and National Security Agency (NSA) that North Korea was responsible for the data breach, doubts remain over the origin of the attackers. Evidence exists to show links to Russian hackers and non-native use of Korean.

- **July 2014 – European Central Bank (Germany)** - The ECB received an anonymous email demanding an unknown ransom amount in exchange for stolen email addresses and contact data from the event register of the ECB internal electronic systems and areas of their website which contained sensitive market information. The ECB refused and informed ECB data security and the German Federal Police. Outcome is unknown.

- **June 2014 – Domino's Pizza (France)** – Hacking group, Rex Mundi, stole data from 650,000 (592,000 French and 58,000 Belgium) customers in France and Belgium. Amongst the data were passwords, contact details and delivery instructions. Data was only protected by an MD5 hash encryption (deemed in 1996 to contain easily exploited flaw in its encryption). Rex Mundi threatened to release the data unless USD40,800 was paid. Domino’s refused and announced the data loss after four days.

- **May 2013 – Unknown Dental Practice (USA)** – Malicious software bypassed the practice firewalls and encrypted X-ray images. Hackers believed to be in Eastern Europe then demanded USD500 in Bitcoins to unlock the files. The ransom would increase by USD500 per day until payment was reached in full. Outcome unknown.

- **May 2012 – Elantis (Belgium)** – Credit provider was hacked and database tables stolen including login credentials, personal data and salary information. Hackers ransomed this for USD197,000.
• **April 2011 – Sony PlayStation Network (USA)** - hackers in a determined DDoS attack successfully stole the personal details (including credit card numbers) of millions of gamers, which were subsequently leaked online. As a result of the public breach, Sony’s share price fell and it was fined a record GBP250,000 by the UK Information Commissioner’s Office (ICO) in January 2013 after the conclusion of its investigation.

• **May 2008 – Virginia Prescription Monitoring Program (USA)** – Hackers gained access to 8,257,378 patient records along with 35,548,087 prescriptions. The files were then encrypted and threatened to be sold or deleted unless the company paid USD10 million. Outcome unknown.

• **Late 2007 – Nokia (Finland)** – Hackers stole for ransom the encryption keys for the Symbian mobile operating system. This meant that Nokia could not ensure that apps available on its own app store had been approved and vetted by the company. In Q4 2007 50.9% of all smartphone sales were produced by Nokia and were powered by Symbian. Concerned over the security of Symbian, Nokia decided to pay the undisclosed ransom. In secret Nokia contacted the National Bureau of Investigation, the NBI organised a sting operation using the ransom payment as bait. The ransom was placed in a bag in a car park near the Särkänniemi Amusement Park in Tampere, the Finnish Police observed the lifting of the bag but subsequently lost the suspect. MTV News in Finland uncovered the story in 2014 and as at 17 June 2014 the case remains unsolved.

**Sextortion**

**Overview**

Sextortion is a cyber variant of the traditional evidence based blackmail. Syndicates target victims with fake Facebook and other social network accounts. The extortionist then engages in chat, which becomes lewd. The victim is then asked to expose himself or herself on webcam or perform a sex act (or both), this is recorded and used to blackmail. A variant has been identified by Interpol in which the sexual video chat is interrupted by a child appearing on screen, all communication is abruptly cut and a payment demand follows on police headed paper threatening criminal investigation. The victim can be blackmailed for either sexual favours or payment in return for non-disclosure of the explicit images, videos or conversations. The crime divides into two distinct categories, paedophilia sextortion and criminal sextortion. According to TrendMicro’s 2015 report, ‘Sextortion in the Far East’, monetised sextortion emerged into Q3 of 2012.

Criminal sextortion payments based on NYA’s investigation of 316 records shows that average payment is USD1030 (70 recorded over USD1,000 and highest recorded USD23,000), demands are kept in the low hundreds to ensure means of payment and lowers the likelihood of law enforcement involvement. Interpol estimates that annual profits for organised crime “certainly runs to tens of millions of dollars”. 73% of the incidents that NYA investigated required payment via Western Union and 21% via MoneyGram.

The crime primarily targets males, there is a minority of female cases. NYA research observed no particular region is targeted, with reports of sextortion crimes conducted in Arabic, English, French, German, Dutch, Korean, Japanese and Mandarin. It is the belief of the FBI and Singapore Police Force that the majority of cases originate in Asia. NYA research shows that 46% of sextortion emerges from Philippines, 38% from Morocco and 5% from Côte d’Ivoire. There are several distinct areas of crime with East and Southeast Asia (Philippines, China, Japan and South Korea), North Africa (Morocco, Algeria and Egypt) and Europe (France, UK, Spain, Germany and Austria) are the most commonly known sextortion originating countries. Interpol intelligence suggests that sophisticated organised crime groups run sextortion ‘agents’ who are provided incentives for being the best performing blackmailer.
Victims are not specifically targeted; instead phishing campaigns seek to entice as many victims as possible. This ensures that the crime involves little to no investment and low risk for comparatively high rewards upon successful completion of a sextortion scam. NYA’s research has shown that Facebook, Chatroulette, Omegle, Tinder, Skype, Skout and Kik are the most common sites/apps for sextortionist targeting.

TrendMicro has observed the emergence of Android OS sextortion on mobile devices, which differs by interrupting the explicit act through a fake technical issue. The sextortionist uses the technical issue as a pretext to make the victim install malware apps on their device, the apps harvest contact details to show victims the list of potential recipients if they refuse to pay.

Recent Cases

- **January 2015 – UK** – North Yorkshire Police released information about ‘Cathy Wong’ who befriended at least three male students on Facebook and conducted sextortion via Skype. ‘Cathy’ initially stated her grandmother was ill and requested USD4,500, on their refusal she revealed the explicit film footage and threatened to post it on YouTube.

- **August 2014 – United Arab Emirates** – Dubai Police have registered 13 cases of cyber blackmail during Ramadan and 33 incidents since January 2014. Young professionals in managerial and administrative positions are lured through social media.

- **August 2014 – Singapore** – Crime statistics from January to June 2014 show that of 132-reported cyber extortion cases, the majority are sextortion. Victim profile is usually 20 to 30 year old and working at a professional or managerial level.

- **July 2014 – Canada** – Nicholas De Carlo (29) faces 30 criminal charges from 13 women over the hacking of private email accounts and theft of personal data and explicit images. It is believed many were hacked through forgotten passwords and answering security questions, the answers gained from Facebook pages.

- **May 2014 – UK** – West Midlands Police stated that eight male victims in “recent months” had been targeted in sextortion incidents. The victims were initially contacted on Facebook and conducted the conversations through Skype or Facetime and took explicit screen grabs. One victim faced a demand of USD5,000 or was threatened with the images being emailed to his girlfriend and daughter.

- **May 2014 – Philippines** – Philippine National Police (PNP) in co-operation with the Hong Kong Police Force, US Department of Homeland Security and Interpol arrest 58 Filipino nationals out of 100 targeted suspects in a sextortion ring. Victims were targeted in Hong Kong, UK, US, Australia and the Republic of Korea. Ransoms ranged from USD500 to 15,000. US Embassy in Manila reported that among the victims were US military personnel.

- **May 2014 – Malaysia** – Salesman (37) was befriended by a Filipino woman on the social network Tagged. They both engaged in cyber sex over Skype and swapped nude photographs. The girl then later sent him a list of all his family members and friends on Facebook and threatened to reveal her evidence if he did not pay USD790. Amount reduced to USD253 and paid in Marikina City, Philippines. Later she demanded a further USD750.

- **March 2014 – Japan** – Two men are arrested on suspicion of being members of a sextortion gang, who stole approximately USD29,200 from 22 victims from December 2013 to January 2014.
Ransomware / data kidnapping

Overview

Ransomware is a type of ‘malware’ or malicious software, which infects a victim’s computer and encrypts the data contained and / or locks the computer – denying the victim access to part or all of their computer’s functions and data. Bromium has recorded ransomware infections against 230 file types, an increase of 228% since 2013.

The software can be implanted or installed from an email attachment, an infected program or a compromised or malicious website (the latter method is known as ‘drive-by downloads’). Multiple campaigns have centred on gas and electricity companies like Enel or postal services such as DHL, USPS, Australia Post, Royal Mail, Post Denmark, PostNord, Correos and Norway Post. The cyber extortionist then demands a sum of money or compels the victim to part with their money by some other means, in order for their data to be unlocked and / or their computer made accessible again.

Ransomware dates as far back as 1989 but has developed considerably in the last 10 to 20 years and has become professionalised by organised criminal gangs targeting both organisations and individuals. Intel Security witnessed a 155% increase in ransomware samples in 2014. The FBI and National White Collar Crime Center has received 2,275 ransomware reports totalling USD1.1 million in losses from June 2014 to March 2015. Whereas Europol recorded 250,000 infections and a combined ransom total in excess of USD27.26 million in the first two months of 2013.

University of Kent Interdisciplinary Research Centre in Cyber Security survey showed 41% have agreed to pay ransomware, this is in line with TrendMicro estimates a 30% ransomware payment rate. The majority are believed to be SME's or private individuals. This is a marked increase from the 2012 Symantec estimate that approximately 2.9% of users paid a malware ransom, the increase can be attributed to the sophisticated encryption techniques that is now common in ransomware.

Since Blackshades Net, DarkComet, Zues, Xroist, CryptorBit, CryptoDefense, Cryptowall and latest Cryptolocker version 3.0 are the most common ransomware currently circulating. Spreading via phishing campaigns (such as 250,000 victims from the 10 million British phishing emails sent posing as Royal Mail) the malware is believed to have originated in Russia.

The FBI and US CERT have observed ransoms between USD200 to USD5,000 being demanded in Bitcoins. The 2015 Trustwave Global Security Report estimated that up to 1,425% return can be achieved in a single malware campaign. Dell SecureWorks Counter Threat Unit has seen ransoms payments as large as USD10,000 after four to seven days.

Ransomware and malware is the most common cyber threat encountered by public and private organisations, however very few private businesses reveal ransomware infections. The majority of cases listed below are from public bodies that have a legal responsibility to disclose information breaches. As a result the list significantly underestimates private organisations, especially corporation interests. In 2015 the Ponemon Institute Cost of Cybercrime Study found that 98% of the businesses surveyed had experienced malware attacks within the past year.

Less common variants include:

- **Naturalising Ransomware:** Urausy and Pollishaltikuksen are two common strains of “naturalising ransomware”. Naturalising ransomware contain stock templates which automatically customise by extracting the default language setting, IP address and time zone settings from the victim computer. Both ransomwares then access their pre-prepared headers matching local law enforcement agencies. Example templates exist for all EU member states as well as countries of North America, Oceania and some Asian, Central and South American nations. Regional and international variants have been seen posing as the FBI, Interpol, Europol and Council of Europe.
• **Card authentication ransomware (Linkup):** A variant of the original ransomwares, convincingly branded as the Council of Europe that blocks Internet access by modifying the domain name system (DNS) settings to instead refocus the captured computer to ‘mine’ (a process that assists in managing Bitcoin transactions). For the user the only obvious sign of infection is that all web domains entered show a European Council verification message, requiring users to verify their identity through the entry of credit card information.

• **Webcam ransomware:** A variant of Urausy with the inclusion of a display window in which the infected computer webcam is displayed, in an effort to guilt the victim into paying the imposed fine. Domestic branding and Ukash/Paysafecard payment method are all seen variants.

• **‘Evidence’ based ransomware or police ransomware:** Purporting to be from national agencies (such as the Department of Homeland Security, FBI, NSA and French Ministry of the Interior) the computer is locked due to “suspicion of illegal content downloading and distribution”, which almost universally is child pornography. This variant uniquely then displays examples of illegal content “found” and displays extracted information such as IP address, ISP, operating system and user name as evidence. A minority of these include a webcam display.

![Screenshot of CryptoLocker 2.0 on an infected Windows XP and Windows 7 (Bitcoin ransom is USD130 and USD526)](image)
Recent Cases

• **October 2015 – FBI Cyber Counterintelligence Program (USA)** – Comments made by Assistant Special Agent Joseph Bonavolonta at the Cyber Security Summit 2015 were reported online. He stated that “the ransomware is that good. To be honest, we often advise people just to pay the ransom”.

• **September 2015 – Customers of Post Denmark and PostNord (Denmark)** Customers were sent a phishing email pretending that a parcel needed to be redelivered, this email contains a strain of CryptoLocker named “crypt0l0cker”. The email originated from a server in Russia.

  ![Screenshot of the phishing email for Post Denmark](image)

• **August 2015 – Tasmanian Chamber of Commerce and Industry (Australia)** – The organisation was hit by a Cryptolocker ransomware attack with a USD350 ransom. On advice of the IT company the ransom was paid as it was cheaper to pay the overseas hackers than unencrypt the files.

• **August 2015 – Competition and Consumer Commission (Australia)** – The commission received 2,500 complaints in 2015 and estimates that over USD400,000 ransom had been paid.

• **April 2015 – Advantage Benefits Solutions (USA)** – A consultant company computer was infected with ransomware and within several hours the malware had spread to the server and the backup drives. The malware encrypted the claims information and financial data. The company paid the USD400 ransom via MoneyGram and the files were unencrypted within 72 hours.

• **April 2015 – CoValence Inc (USA)** – Producer of private-label skin care products admitted to four ransomware attacks in the previous six months.

• **January 2015 – Midlothian Police Department, Chicago (USA)** – Hackers infected the police server with Cryptoware from a phishing email and ransomed the department for USD500 in Bitcoins. The department paid the ransom.

• **December 2014 – Tweksbury Police Department, Boston (USA)** – CryptoLocker ransomware infected the police server and delivered a USD500 ransom. The department agreed to pay the ransom.

• **November 2014 – Dickson Sheriff Office, Tennessee (USA)** – A hacker named ‘Nimrod Gruber’ using a CryptoWall ransomware encrypted over 72,000 files. Upon the advice of sheriff the ransom was paid via Western Union and a further USD3,000 was paid for a contractor to clean the files.

• **June 2014 – Durham Police Department (USA)** – A police officer opened an email from a known contact and opened a link that downloaded the Cryptowall malware. On 06 June there
was widespread difficulties in accessing files. The town’s IT manager took the network offline and isolated the virus. Instructions were sent to the department for a ransom but the email was not opened. The situation was contained within 48 hours at a cost of nearly USD3,000.

- **February 2014 – Inspector General for Health and Human Services (USA)** – During a meeting with the US task force set up to counter CryptoLocker ransomware, an official revealed his agency had suffered “20-25 incidents”.

- **November 2013 – Swansea Sheriff Office, Massachusetts (USA)** – Hackers placed CryptoLocker malware onto the police computer system and ransomed the data for USD750. The department paid the ransom in full.

- **October 2013 – National Aeronautics and Space Administration (NASA) (USA)** – NASA Ames Research Center, Kennedy Space Center and Visitor Center had several computers infected with CryptoLocker ransomware “resulting in the loss of access to NASA data”. NASA did not pay the ransom and was able to recover some data.

### Mobile device ransomware

#### Android

According to NetMarketShare 53.5% of mobile and tablets operate on Android, yet in June 2015 Pulse Secure estimated that 97% of all mobile malware operates on Android devices. Pulse Secure identified 1,268 known families of Android malware. AV-Test currently has identified more than 5.2 million Android OS malware apps, a new infected app is developed at a rate of one every five minutes. Android suffers disproportionately high levels of malicious apps due to both the open nature of its OS and the ability to install apps via third party stores.

From 2010 to early 2014 Android ransomware was neither sophisticated nor based on encryption, instead the majority were lockscreen ransomware such as Koler Lockerdroid.E and Fakedefender. A lockscreen ransomware would effectively remove the users ability to control the phone by constantly arranging the ransom window to the foreground using an infinite loop. No encryption occurred on user data and the malware was, on a varying scale of difficulty, able to be removed by the Android Debug Bridge (ABD) or deactivating Administrator rights and uninstalling in Safe Mode.

In June 2014 Simplocker emerged as the first malware which, once installed, located and encrypted files (pictures, PDF, documents, audio and video files) on the SD card and ransomed the files decryption. Variants emerged shortly after discovery including one that took a victims photo. However, ransom demands were low (averaging USD21) and payable only in Ukrainian hryvnias or Russian roubles. Analysis by ESET revealed 90% of infection had occurred in Russia or Ukraine.

By July 2014 Simplocker had migrated to English language and Android devices were infected with an FBI police ransomware strain, which claimed the victim had accessed child abuse images or child and zoophilia pornography. A ransom of USD300 was demanded via MoneyPak. The page said that if the demands were not met, criminal charges would be filed. Encryption was broadly unchanged but had the capability to encrypt ZIP, 7z and RAR archive files, which was also able to encrypt Android backup files. The ransomware spread to over 30 countries in a matter of weeks.

In September 2015 ESET researchers discovered Lockerpin.A, which gained Device Administration privileges by using a Trojan disguised as an “Update Patch Installation”. Once installed the ransomware locks the device and sets a new PIN for the lock screen. Like Simplocker, it utilises an FBI police ransomware warning and demands a USD500 ransom. The user has no effective means of regaining access unless the device utilises a security management solution or factory reset is conducted. The PIN is automatically generated and is unknown to the attacker or victim. ESET analysis detected 77% of devices infected were in the USA.
All strains of Simplocker and Lockerpin.A utilise social engineering techniques to prompt victims to install the Trojan. Adverts and phishing emails for pornography (such as Porn Droid and Adult Player), Adobe Flash Player and malicious versions of Grand Theft Auto and other leading game titles are the most common means of Trojan installation.

**Apple iOS**

According to NetMarketShare 38.5% of mobile and tablets operate on iOS, yet malware and ransomware remains almost unknown on iOS devices. This is a direct result of Apple’s tightly controlled App Store and heavy vetting of all apps that are placed on the marketplace. Installation of apps outside the controlled environment of the App Store is severally limited and is almost impossible without an enterprise developer certificate, which is only issued by Apple.

On the night of 26 May 2014, iPhone, MacBook and iPad users in Australia and New Zealand were alerted by their devices that the Find My iPhone feature had been activated. The ransom message displayed stated that a USD100 ransom was required to unlock their device and was payable via MoneyPack, Ukash or PaySafeCard. The attack spread to USA, Canada and Europe. Despite initial industry concerns the attack was not a result of ransomware. The attack utilised stolen passwords and email addresses from previous mass data breaches and affected users who reused passwords for their iCloud accounts. In June 2014 the Russian Ministry of Internal Affairs arrested two suspects for the breach.

Approximately 12 malware strains are known to exist on Apple iOS devices and of these only seven can only target jailbroken iOS devices. The majority of these targeted older versions of iOS and have been patched to not affect the latest iOS releases.

Since November 2014 the emergence of sophisticated third-party app installer malware families such as WireLurker and YiSpecter on non-jailbroken iOS devices show that security can be breached, yet the eventual aim of these campaigns are unknown. Others like Masque Attack, which replicate approved apps with malicious variants, and XcodeGhost, which infects approved apps, are aimed at stealing confidential data such as banking details.

On 18 October SourceDNA discovered that advertising coding developed by YouMi, mostly used by Chinese App Store developers, had become the first known way to circumvent the app review process and harvest user and device usage details that are currently banned by Apple. Apple swiftly banned all apps using YouMi’s coding from the App Store and will deny all future YouMi coded apps.

Overall Apple has remained secure against threats to its iOS, Sophos states “evidence of malicious malware showing up in the App Store is anecdotal at best”. The recent emergence of malware and security breaches capable of circumventing Apple’s strict security policies is both limited and academic. All breaches have been quickly resolved and have been limited to very specific entry points. As a result, there is no evidence to suggest that in the short to medium term Apple iOS devices will become targeted by malware campaigns capable of sustaining ransomware demands.

**Outlook for 2016**

- In 2016, the only consistent development will be the continued under-reporting of what is now almost certainly the most prolific form of extortion.

- The rise of the Dark Web in the public consciousness has brought to light the continued commoditisation of ransomware and outsourcing of DDoS, Botnet and other malicious services. The availability of free ransomware toolkits and cybercriminals for hire to disgruntled employees and politically motivated hacktivists is a worrying development. Despite unprecedented efforts by the FBI, National Crime Agency, Europol and Interpol to counter cybercrime organisation, this market remains operational and will continue to evolve to thwart efforts to contain its activities.
• Ransomware will continue to evolve as it adapts to changing habits and our continued reliance on tablets and smartphones. Ransomware however will remain static or slow growth in one crucial way, the ransom demands. Symantec analysis in 2015 noted that the original AIDS Trojan demanded USD189 in 1989. This amounts to USD368 once inflation is taken into account. The average ransom demand from ransomware in 2015 is just over USD300. As a result, it would seem unlikely to increase beyond the USD700 heights seen in the last several years.

• DDoS attacks combined with data breaches will continue to affect both public and private organisations regardless of size or sector in 2016. In 2015, there was no sign of any decline in data theft for ransom attacks and recent incidents like TalkTalk show that ransoming of stolen data will continue to affect major corporations in repeated cyber attacks.

• Sextortion will continue to be a major venue stream for transnational organised crime and low barriers to entry potentially allows a simple and relatively safe entry into cyber extortion for novice cybercriminals. Following Ashley Madison extortion cases and the concerns raised by the Australian and American departments of defence, 2016 may see the emergence of targeted sextortion campaigns against employees with the aim of leveraging access into corporate or government information systems. The presence of blackmail material would certainly raise hesitation by the employee to report to the company or to law enforcement agencies.

• As the "Internet of Things" is growing, the technologically interconnected remains unabated. In 2014 Europol warned that connected devices such as smart doors, cars and meters were all vulnerable to cybercrime and this proved true. 1.4 million vehicles produced by Fiat Chrysler, a United Airlines flight, Spanish smart electricity meters, TrackingPoint smart rifles and a Samsung Smart Fridge were amongst the smart technology hacked in 2015. In 2016, there remains a threat of the emergence of a new type of extortion that targets remotely individuals, homes, cars or indeed cities. The risk of murder or extortion over medical equipment is present and already existing.

• By the end of Q4 2015 International Data Corporation expects that 45.7 million units of wearable technology will be shipped, an increase of 133.4% on 2014. Symantec has raised concerns that wearable devices remain exposed to the risk of ransomware and have demonstrated that wearable technology can be attacked by existing ransomware. A TrendMicro survey found 80% of European organisations were seeing an increase in the number of staff bringing wearable devices to work. As a result the threat of ransomware to individuals and potentially cyber security threats to businesses through wearable technology could develop through 2016.

• Point-of-sales (POS) terminals experienced significant malware infections and data breaches with Hilton Hotel and its subsidiaries, Trump Hotel Collection, Mandarin Oriental Hotel Group, FireKeepers Casino and Hotel and Las Vegas Hard Rock Hotel and Casino being the highest profile cases in 2015. TrendMicro has shown that malicious tampering can occur either onsite or through network connection and can be specifically targeted through server access. Symantec hypothesised on a ransomware infection against POS terminals in “Evolution of Ransomware” report, but the data theft and ransoming of captured data is also a threat to POS operators. The loss of POS terminals for even several hours would have a dramatic financial repercussion on a major retail corporation. The evolution of POS breaches in 2016 will be a major cyber security concern for all customer-facing sectors.
Cyber security response and consultancy

Cyber extortion can take a number of forms and may not be initially appear the primary motive of a system breach, but distributed denial-of-device (DDoS), data breaches, sextortion and ransomware are growing extortion threats throughout all sectors.

As a leading global risk and crisis management consultancy we have over 25 years’ experience of advising clients during extortion incidents, our experience of cyber related extortion has grown in line with this burgeoning crime. Throughout a cyber extortion incident, the role of our response consultants is to provide advice to ensure that extortionist communication, stakeholder communication and other measures are conducted according to tried and tested crisis response procedures.

We offer a range of preventative cyber security management planning and training courses to ensure that an organisation can respond effectively to safeguard brand reputation and help ensure business continuity.

About NYA

NYA International is a leading global risk and crisis management consultancy. Since 1990 we have helped organisations to maximise opportunities and operate successfully in complex environments around the world. We help our clients to understand the threats and vulnerabilities to their people, assets and international operations, improve their resilience and effectively mitigate and manage a wide range of security-related problems and crises. NYA has one of the largest specialist response teams in the industry and experience of advising on around 80-100 crisis incidents each year.

www.nyainternational.com

Limitation

Our opinion and advice is given on the basis of the information given to us in our instructions and the surrounding circumstances known to us to exist at the time when those instructions are given. We do not accept responsibility for verifying the information or investigating beyond its limits. Subsequent changes to relevant information or to the surrounding circumstances may affect the reliability of our opinion and advice but we do not accept responsibility for that effect. We do not accept responsibility for the outcome of action taken or not taken as a result of our opinion and advice unless the possibility of that action being taken or not taken is set out in specific terms in our instructions.

Contact us

t: +44 (0)207 291 7700
e: info@nyainternational.com
w: www.nyainternational.com
@NYAintl