Long-Form Content Sample

George Donnelly
Freelance Writer
me@georgedonnelly.com
+1 (215) 360-3513
GeorgeDonnelly.ninja

The Top 119 Hacks of 2015

Hacking entered a new stage in 2015 and it's only getting more hostile and aggressive as darknet operators line their pockets with the proceeds of data breaches through extortion, identity theft and fraud - crimes that threaten the very foundations of 21st century society.

Up first on the *Hacked* radar are the massive Experian, Anthem, OPM and United Airlines hacks that doxxed a nation. From credit to health to government employees and travel records, respectively, the Chinese yanked the digital rug out from under the United States in 2015.

The dating site Armageddon of Ashley Madison, Adult Friend Finder and Russia's Topface was no laughing matter either, with more than 60 million accounts forced out of the closet - including blackmail-ready sexual preferences, fetishes and other embarrassing secrets.

But that was merely the tip of the iceberg as a Bitcoin exchange lost $5 million in a cringe-worthy social engineering ploy and a crowdfunding darling was gutted in a hack that makes you wonder if their CEO was left with a shirt on his back.

Then there was the guy who hacked his way out of prison, two hacking teams who got their rear ends handed to them, flying jumbo jets from coach and the savvy ex-wife who hacked her way to higher alimony payments.

From ransomware and DDoS attacks to malvertising and social engineering, here are your top 119 hacks of 2015, organized into three groups: private sector, government and individuals.

Private Sector Most Impacted

1. Credit Agency Experian - 15 Million

Experian, one of the largest data brokers and credit agencies in the world, was hacked in early October, exposing 15 million people's information. T-Mobile USA users who applied for credit checks are also affected.

The hackers got away with names, addresses and Social Security, driver's license and passport numbers.

From customer loyalty cards to public records of real estate liens and bankruptcy, Experian is at the center of American commercial life, making this a very serious breach indeed. Automated advertising networks use Experian's databases to make ads relevant to users, among other applications.

This isn't Experian's first time in the dog house. A 2014 hack of a subsidiary exposed 200 million Social Security numbers.

2. Health Insurer Anthem - 80 Million

In the largest ever breach at a health care company, insurer Anthem lost the unencrypted records of 80 million customers to Chinese hackers in early February, including names, dates of birth, Social Security numbers, and home addresses - all in plain text.

Health care data is both very valuable to identity thieves and relatively unguarded, so expect more health care hacks.

3. Fly Passenger Jets from Coach

Cybersecurity consultant Chris Roberts claims he hacked into the onboard systems of both Boeing and Airbus models of passenger jets and controlled the airplane while in fight as many as 20 times, using only a laptop and a modified Ethernet cable.

Then he tweeted about it, leading to his unsurprising detention at the hands of the FBI and the seizure of his laptops and other electronics devices.

4. Dating Site Ashley Madison - 37 Million

It was Armageddon for unfaithful husbands across North America when hacker group Impact Team stole dating site Ashley Madison's database of 37 million customers as punishment for their own immorality, according to the hackers.

The hack shook site owner Avid Life Media (ALM) to the core with the theft of not just the 10GB database of customer data but also employee records, including bank accounts and salaries, and blueprints of the company's internal servers.

Suicide and extortion were the predictable outcome. ALM responded by placing a $500,000 bounty on the heads of Impact Team.

5. Dating Site Adult Friend Finder - 3.5 Million

In another hack sure to lead to more pain and suffering - and not in a good way - a hacker took Adult FriendFinder's database of the sexual preferences, fetishes and secrets of more than 3.5 million people in March.

Additional exposed personal information includes email addresses, usernames, passwords, birthdays and zip codes but not credit card data.

One hacker already used Twitter and the hacked data to identify several impacted individuals, including a Washington police academy commander, an FAA employee, a California state tax worker and a naval intelligence officer.

6. United Airlines - 3.5 Million

The Chinese struck again in June, this time at the world's second-largest airline, United Airlines, with a hack that included flight manifests detailing passenger information and destinations.

Researchers believe this is the same group of Marvel-fanboy hackers that took down Anthem (see number 2 above) and executed the ground-shaking OPM hack (see number 70 below) against the US federal government. The Chinese are building a massive database, the researchers think, to catalog and track the movements of federal employees, perhaps with an eye to blackmail and/or to recruiting people with security clearances.

Chinese military hackers have also repeatedly hit the U.S. Transportation Command, the Pentagon agency that coordinates defense logistics and travel.

7. Card Company Moonpig - 3 Million

A security flaw in the systems of personalized card company Moonpig exposed the personal information of 3 million customers in July. The information made its way online through a loophole that enabled hackers to access sensitive data simply by entering a customer ID.

8. Carphone Warehouse - 2.4 Million

The names, birthdates, addresses and banking information of more than 2.4 million customers of British mobile retailer Carphone Warehouse were lost in an August hack. The credit card information for 90,000 of those customers was also lost.

9. Crowdfunding Site Patreon - 2.3 Million

Crowdfunding company Patreon was gutted in a late-September hack that saw 15 GB of password data, previously private donation records, and source code dumped online due a facepalm-worthy goof.

Patreon was warned ahead of the hack about a remote code execution vulnerability due to a public debugger they had made available, likely through simple negligence or gross naivete.

10. Italian Hacking Team

In a delicious example of turnabout being fair play, the Italian Hacking Team was itself hacked, possibly by a government, and a file archive made available.

11. Mobile Spyware Maker mSpy - 400,000

In another ironic case, mSpy, the maker of tools to help people spy on their kids and partners, was hacked. Several hundred gigabytes of emails, text messages, payment and location data, photos, corporate email threads, Apple IDs, passwords and payment information on 400,000 customers were published.

12. Medical Informatics Engineering

Medical Informatics Engineering, an Indiana company that makes Web-based health information-technology software lost the protected health information of an unknown number of patients from about 100 small- to medium-sized physician offices in a June hack.

Patient names, mailing and email addresses, birthdates, and for some patients, Social Security numbers, laboratory results and the very valuable (to identity thieves) dictated reports and medical conditions, but not financial information, were lost.

13. Apple iCloud - 225,000

Jailbreaking your iPhone can't hurt anything, right? Wrong. In the largest Apple account hijack ever, the KeyRaider malware hacked 225,000 jailbroken Apple devices, resulting in the taking of Apple usernames, passwords and GUIDs. Some victims were locked out of their iPhones and iPads and many were faced with ransom demands.

14. Trump Hotel Collection

Hackers siphoned customer credit card data out of Trump Hotels for a full year, between May, 2014 and June, 2015. Credit card numbers, expiration dates and back-of-card security codes were stolen.

15. Apple App Store

Making its second appearance on the list is Apple, which saw more than 4,000 iOS apps infected with the XcodeGhost malware via a bootleg Chinese copy of its Xcode development tools.

The App Store faces a new threat now in the form of YiSpecter, malware that spreads by unusual means and will hijack both jailbroken and non-jailbroken Apple devices in unexpected ways.

16. Chrysler Cars - 471,000

In a July *Wired* report, two white-hat security researchers showed us how to assume total control of a Chrysler Jeep Cherokee via a remote hack, which affects as many as 471,000 vehicles. Chrysler is offering a software update to counter the threat.

17. Dating Site Plenty of Fish

UK dating site Plenty of Fish was infected with the Tinba spying malware in August that masquerades as an advertisement (malvertising) in order to grab members' financial information. It is not known how many of the site's 100 million members were affected.

18. Bitcoin Exchange Bitstamp - $5 Million

In a social engineering exploit that makes you wonder if there are any signs of life left at Bitcoin exchange **Bitstamp**, more than 18,000 bitcoin were lost after a series of highly-targeted phishing attacks.

19. Ride-sharing service **Uber** saw 50,000 of its drivers compromised in a data breach and countless users being charged for rides they did not take, though they seem mostly unaware of it.

20. Online foreign exchange broker **FXCM Inc.** saw its shares fall by 25 per cent when hackers issued wire transfers from customer accounts. All of the funds have been returned.

21. DARPA hacked a **Chevrolet** Impala in February in an effort to highlight automakers' security shortcomings. The government hackers got control over everything from the windshield wipers to braking and acceleration. In a related development, **General Motors** doesn't get a pass as its OnStar app, with more than 3 million users, can also reportedly be hacked. In another case, researchers hacked a Chevy Corvette via text message. Federal agencies with large fleets are thought to be especially vulnerable.

22. A hacker named "Mastermind" made off with 20 million usernames and email addresses from the Russian dating site **Topface** in January.

23. The **Houston Astros** baseball franchise lost their central database, the repository of all the team's baseball knowledge, to a hack likely performed by rival team the St. Louis Cardinals in July.

24. **British Airways** saw tens of thousands of its frequent-flyer accounts accessed by hackers in late March. No names, addresses, bank details or other personal information were taken.

25. Hackers stole customer credit card data from the upscale **Mandarin Oriental Hotel** in March.

26. In a broad hack that compromised point-of-sale registers used in gift shops and restaurants, the **Hilton Hotel** chain lost customer credit card data.

27. The hacking group **Lizard Squad** was itself hacked when its website and Twitter accounts were taken down and its customer database was exposed.

28. Videogamer social network **Raptr** was hacked and asked users to change their passwords in February.

29. In another case of naughty advertisements (malvertising) attacking website users, Porn Site **RedTube** was hacked in February.

30. Hackers used **Yahoo** in August in another malvertising hack to infect millions of visitors with malware that left them open to ransomware.

31. Thousands of vulnerable **WordPress** websites were used by hackers to infect vistors with malware in September.

32. The New York police got into the hacking game in March with subtle, yet biased, changes to **Wikipedia** pages dealing with victims of NYPD excessive force.

33. **Wikipedia** was hit again in May with another political hack, this time UK politicians David Cameron, Caroline Lucas and Nick Clegg's Wikipedia pages were replaced with a demand to vote for the Labour party.

34. The browsers **Safari, Chrome, Firefox and Internet Explorer** were all hacked for prize money at the 2015 Pwn2Own Contest in Vancouver in March.

35. In a particularly offensive hack,**The Dublin Rape Crisis Centre** website was defaced by a group affiliated with ISIS.

36. **Tesla Motors'** website and Twitter accounts were hacked by a group called Autismsquad via social engineering. No data was lost.

37. ISIS struck the **BBC** in April by interrupting a live evening broadcast with the printed words "Je suIS IS" and "CYBERCALIPHATE."

38. In a similar attack, **TV5Monde** in French went off the air for three hours and its website and Facebook page were also hacked by ISIS-affiliated groups.

39. **Linux Australia** was hacked via a buffer overflow attack in March and the personal information of conference attendees was taken.

40. Hack group Team GhostShell claimed in July that it compromised more than **300 websites** and posted over 13,000 users' personal information online, likely in an attempt to remind the world that they still exist.

41. Email service provider **SendGrid** was hacked in April in order to send an email investment scam to Bitcoin exchange Coinbase's customers.

42. Indian music streaming service **Gaana** was hacked in May through an SQL injection exploit, resulting in the loss of millions of users' account information.

43. The ***Washington Post*** lost its mobile site temporarily to a hack by the Syrian Electronic Army in May.

44. **Malaysia Airlines** took another hit in January when the ISIS-affiliated hacking group Official Cyber Caliphate hacked its website. No internal systems were affected.

45. **Abu Dhabi TV and Al Ittihad** had their websites hacked by hacking group Youth of Islamic Caliphate with a simple redirection.

46. ISIS hackers struck again, this time in the US, defacing business websites across the nation in early March, including the **Indianapolis Downtown Artists and Dealers Association** and the Pittsburgh marketing firm **Eyeflow**.

47. The **Kentucky Republican Party** website did not lose any information in a Memorial Day hack.

48. Canada's **Bloc Québécois** party saw its website hacked in March by a group upset about its stance on the wearing of the Muslim head covering (hijab).

49. In a curious and careless twist, a special **Microsoft** website dedicated to resisting NSA surveillance was hacked. It was running an old version of WordPress.

50. **Houston's KBXX 97.9** was hacked in July to display the N-word on listener radios where song titles are usually shown.

51. A hacker named Savaka blackmailed **Plex**, maker of media server and home theater software, after a forum hack that led to the taking of usernames and passwords.

52. Indian state-owned telecom company **Bharat Sanchar Nigram Limited** (BSNL) was hacked and data stolen by Anonymous group OpsIndia, who shamed them for storing passwords in plain text.

53. The gaming distribution platform Steam was hit with a social engineering hack in July through its parent company, **Valve**. Usernames, hashed and salted passwords, game purchase information, email addresses, billing addresses and encrypted credit card information were taken.

54. **KMart Australia** lost customer names, email addresses, home addresses, telephone numbers, and product purchase details in a September hack.

55. A vulnerability in the website of another Australian department store, **David Jones**, was used by hackers to grab names, email addresses, mailing addresses and order details of customers who have shopped on the store's websites but no credit card information was taken.

56. Hacktivist collective Anonymous shut down the websites of several California community newspapers operated by **Embarcadero Media Group**, including *Palo Alto Weekly*, *Mountain View Voice*, *Pleasanton Weekly* and *The Almanac*.

57. The **Costco** photo center website was hacked and personal information stolen in late September. The company is offering one year of identity protection for affected customers.

58. In a hack that could have been performed by the Three Stooges, Muslim hackers attempting to disrupt travel across the Western world instead hacked journey planning website **TravelWest's** bus timetable in Bristol, UK.

59. Google Vietnam was hacked with a simple DNS redirect in late February.

60. Google Malaysia fell victim to a similar attack in April.

61. In yet another simple DNS attack, Lizard Squad redirected **Lenovo's** domain away from its website in late February.

62. The ***New York Post*** **and UPI** had their Twitter accounts hacked in January. The clever hackers announced, among other things, that "World War III has begun." UPI's website was also hit.

63. French newspaper ***Le Monde***'s Twitter account was hacked by The Syrian Electronic Army in January.

64. Cyber Caliphate struck again in January at the Twitter accounts of news organizations ***Albuquerque Journal*** **and WBOC 16** in Maryland.

65. Crayola lost its Facebook page briefly to hackers who posted NSFW content in January.

66. In an attack reminiscent of Crayola's, **Delta's** Facebook page was hacked in February.

67. ISIS's CyberCaliphate struck once again in February when it took control of **Newsweek's** Twitter account, **IBTimes.com** and the breaking news system of a Maryland television station.

68. Swastikas peppered **Chipotle's** Twitter account briefly in February after a hack.

69. Twitter itself took it on the nose in February when CFO Anthony Noto's public account was hacked in a simple spam attack.

Large Scale Government Hacks

70. The OPM Hack - 21.5 Million

Mid-year we discovered the gargantuan breach known as the OPM Hack, after the **United States Office of Personnel Management**, in which more than 21.5 million people's personal information was stolen, much of it extremely sensitive in nature, likely by Chinese government hackers intent on building a vast database of US government employees.

Lost in the attack was not just personally identifying information such as Social Security numbers, names, dates and places of birth, and addresses but also detailed security-clearance-related background information - the kind that could be used to blackmail current, former and wannabe executive branch federal employees.

Hackers also grabbed 5.6 million fingerprint records. Now, despite name changes, secret agents can be identified by their fingerprints, thus putting their lives in great danger.

Months later, the federal government still had not notified those affected.

71. Japan Pension Service - 1.25 Million

Japan's national pension system was also hacked mid-year and the pension IDs, names, addresses and birth dates of 1.25 million Japanese were stolen. The most sensitive information, including financial details, was reportedly exempt from the hack.

72. UK's Wandsworth Prison

In a hack called “ingenious” by his judge, UK man Neil Moore created a fake court website and email account via a smuggled cell phone. He then sent **Wandsworth Prison** officials an email instructing them to release him - which they promptly did! His deception was only discovered three days later. Another three days after that, Moore turned himself in.

73. The White House

Russian hackers tricked someone at the **White House** into giving them unlimited access to an unclassified White House network in April. No classified data was compromised.

74. The Pentagon

Russian hackers penetrated an unclassified email system at the **Pentagon** in August, affecting 4,000 military and civilian employees and personnel working for the Joint Chiefs of Staff. No classified information was lost in the attack.

75. The U.S. military’s **Central Command** fell victim to ISIS hackers in January who took control of their Twitter and YouTube accounts and claimed to release secret documents that weren’t actually secret.

76. The **US Army’s** public website was hacked with a demand to end the training of rebel fighters inside Syria in June.

77. Hacker group Cyber Berkut claimed in February to have hacked a Ukrainian chief military prosecutor and stolen documents showing that the **Ukraine** was fairing poorly in its quiet war with Russia.

78. Anonymous doxxed 4,200 **US Census Bureau** employees in a July hack that was not expected to cause much harm.

79. **Democracy** itself has been hacked, according to former US Vice-President Al Gore, by short-term thinking in the corporate world.

80. ISIS took down **Chile's** Ministry of Defense website in February.

81. Six government websites in **Thailand** were hacked in August by a Muslim group to draw attention to the plight of persecuted Rohingya Muslims.

82. A group of white hat hackers hacked 24 **Saudi Arabian** government websites in August in an attempt to warn administrators of lax security.

83. **Saudi Arabia** took it on the nose again in September when Anonymous hacked multiple government websites to protest the death sentence against pro-democracy activist Mohammed al-Nimr, who was 17 at the time of the protests.

84. Several of African country **Ghana's** government websites fell to hackers in late January.

85. ISIS took over the website of Caribbean island nation **St. Vincent And the Grenadines** in a May hack.

86. A Muslim hacker team took down the website of the **Philadelphia City Council** in May.

87. The website of the **New Jersey Casino Reinvestment Development Authority** was hacked by an ISIS-affiliated group in April.

88. Anonymous took down the **Montreal police and police union** websites in April in response to accusations of brutality during student demonstrations.

89. The tiny Canadian town of **Terrasse-Vaudreuil**, population 1,971, had their website inexplicably hacked by a group calling themselves the Middle East Cyber Army in late January. No private information was taken.

90. Muslim hackers defaced the websites of Florida's **Gainesville Regional Transit System and the City of Gainesville's** parking website in late March.

91. New York's **Commack School District** was hacked and a small number of student records taken in September.

92. West Virginia's **Wayne County Board Of Education** website was hacked by ISIS supporters in September.

93. The **Alabama state legislature** had their email hacked in May without any apparent impact.

94. A pro-Palestine group hacked **Hinds County, Mississippi's** website and left a propaganda message.

95. Anti-ISIS Kurdish sympathizers hacked the website of the **Etowah County, Alabama** Sheriff's Office.

96. No personal information was lost in the hack of **Warrenton, Oregon's** website in September.

97. Practical jokers hacked a **Gwinnett County, Georgia** road sign in July to read "Ebola Outbreak Ahead."

98. The Indian state of **Kerala** lost its website to Pakistani hackers in late September.

99. The **Pakistan High Commission in India** had its website hacked in August.

Celebrities and Regular People Hit Too

100. Taylor Swift

Taylor Swift took it in stride when her Twitter and Instagram accounts were hacked by Lizard Squad in late January. Hackers sent out a few innocuous tweets to the pop star's 51 million followers - the fourth largest Twitter account. A similarly inoffensive photo went out to her 20 million Instagram followers.

101. Babies in Houston and Minnesota

Taking the cake for creepiest hack, **baby** monitors were compromised in Houston and Minnesota. Cyberstalkers played eerie music, commented on diaper loads and rotated cameras at their pleasure.

102. 10,000 Routers

An unknown hacker infected more than **10,000 Linux routers**, mainly in China and Brazil, with the Linux.Wifatch malware - a hack that actually makes the routers more secure and protects its victims. The malware uses a P2P network to stay updated.

103. Ex-Husband Hacked for Alimony

An **ex-husband** saw his Charles Schwab and Google accounts hacked by his ex-wife in a successful bid to increase his alimony payments. Family court granted the savvy mother of two a 50 percent increase in the man's monthly payments after she presented the stolen documents.

104. US Military Spouses

ISIS sympathizers took over the Twitter account of a **US Marine's wife** and used it to threaten other military spouses and the family of President Barack Obama, in a late January hack.

105. Vine Star Ben Phillips Wiped Out

Vine star **Ben Phillips** saw his 1-million-follower Vine account hacked and all his videos deleted in March. Phillips claimed to make £2,000 per second from his vines, thus proving the value of backups once and for all.

106. Jamie Oliver, Again and Again

British TV chef **Jamie Oliver** saw his website infected by malware that can harm site visitors for a second and third time this year. They think they have it under control *this* time.

107. Ecuadorean Activist Dr. Carlos Figueroa

Ecuador's domestic intelligence agency, SENAIN, was blamed for an August hack against Ecuadorean opposition activist and fugitive **Dr. Carlos Figueroa** that saw his email and Facebook accounts compromised. Further investigation revealed that Ecuador used tools sold by the Italian Hacking Team to perform the hack.

108. Hong Kong Politician Regina Ip

Hong Kong Politician **Regina Ip** almost lost $65,000 in a February email account phishing hack. The hackers got access via an email attachment that Ip downloaded.

109. A Florida man's **TrueCrypt** password was cracked by the FBI in August. Whether the FBI just found his password somewhere or whether they actually cracked the widely-used TrueCrypt software is not known.

110. American model and actress **Charlotte McKinney's** Instagram account was hacked in July and nude photos posted.

111. Mom of Kim Kardashian **Kris Jenner** had her Apple iCloud account hacked in April and was reportedly being blackmailed over a nude video.

112. Celtics basketball player **Jae Crowder's** Instagram account was hacked in August by his partner who uploaded a photo of Crowder and a woman his partner alleged was his mistress.

113. Singer **Pink** had her Twitter account hacked in June and a tweet promoting adult movies was sent out.

114. Reality TV star "**Snooki**" had her Instagram account hacked by Muslim hackers in January who uploaded a photo of a person in a Muslim hijab.

115. British reality star **Gemma Collins** saw her 1-million-follower Twitter account hacked in March.

116. British TV personality **Katie Hopkins's** Twitter account was hacked in June. The hackers tweeted claims of a sex tape and made fun of her weight.

117. Pro wrestler **Cesaro's** Twitter account was hacked and supportive tweets sent out in mid-February.

118. American alternative rock band **Death Cab For Cutie** saw its Facebook account hacked and NSFW images posted in late August.

119. Former cricket player **Kumar Sangakkara's** Twitter account was hacked and obscene photos posted in September.

And the Winner is…

Everybody loses in the hacking free-for-all except, maybe, for those hackers that escape getting hacked themselves. But there is one clear winner: Bitcoin.

Darknet cybercriminals need a currency that's outside of the international legal framework. They need a currency that can be transmitted quickly without problematic banking approval and inconvenient government seizures. That currency, for better or worse, is Bitcoin.

Whether Bitcoin's status as the cybercriminal's currency of choice will threaten mainstream adoption of the pioneering cryptocurrency remains to be seen.

So stay safe out there, keep your passwords strong, prepare yourself now in case of a hack and check out *Hacked*'s must-read followup piece: 15 Hacks to Expect in 2016.

George Donnelly
Freelance Writer
me@georgedonnelly.com
+1 (215) 360-3513
GeorgeDonnelly.ninja