The Heritage Foundation

ISSUE BRIEF

No. 4636 | DECEMBER 2, 2016

Cyber Attacks on U.S. Companies in 2016

Riley Walters

This *Issue Brief* is a continuation of a series of papers on cyber attacks against U.S. companies since 2014[1] and 2015.[2] While the means of cyber attacks vary, the pattern of targets has been relatively consistent. Large databases, as well as point-of-sale systems, continue to be targeted for financial gain. Hackers with possible ties to nation-states continue to target infrastructure as well as systems for political insight.

Because reporting companies may not realize their systems have been compromised until long after the attack began, the list below is organized by date of when attacks or breaches were publicly announced, rather than when they might have occurred.

December 2015

- **Bowman Dam (infrastructure).** Iranian hackers reportedly gained control of this New York dam's sluice system in 2013, although the controls were manually disconnected at the time of the cyber breach.[3] In March 2016, the Department of Justice (DOJ) indicted one of the hackers employed at an Iran-based computer company with possible ties to the Islamic Revolutionary Guard Corps.[4]

This paper, in its entirety, can be found at **http://report.heritage.org/ib4636**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

- **Hyatt Hotels Corporation (hotel).** The hotel chain owner announced that it had identified malware on payment processing systems used at a number of locations.[5] Weeks of investigation revealed that malware had affected the systems at 250 locations between August and December 2015.[6] The malware collected payment information specific to credit card information.[7]

- **MacKeeper (technology).** Security researcher Chris Vickery discovered in Shodan (a specialized search engine and online database) the usernames, passwords, and other information for 13 million users of MacKeeper, a performance optimizing software for Apple computers.[8]

- **A Whole Lot of Nothing LLC (spam e-mail company).** The DOJ arrested three men linked to a hacking and scamming scheme that originated as early as 2011. The group targeted the personal information of almost 60 million people—often contained in targeted corporate databases—to be used in spam campaigns. Their operations ultimately generated $2 million in illegal profits.[9]

- **Voter records.** Vickery found the information of 191 million registered U.S. voters in a public-facing database.[10] While there were only 142 million register voters in 2014, information in the database goes as far back as 2000—meaning it could still contain the information of deceased registered voters. There also may be instances of duplication from combining multiple databases. As of yet, no one has come forward as the owner of the database.

- **Alliance Health (online health portal).** The online portal that facilitates support and information communities across health providers may have exposed personal health information of its 1.5 million users. The exposure likely came from a misconfiguration with its MongoDB database installation.[11] Forty thousand individuals were eventually informed their information had been exposed for 30 months.[12]

January 2016

- **Voter records.** Vickery discovered another public-facing database, storing upwards of 56 million voters' information.[13]
- **The Wendy's Company (restaurant).** Wendy's first reported it would be investigating a possible breach that compromised customer payment information at its franchise stores. By June, investigators determined that at least 1,025 Wendy's locations had been affected, beginning as early as fall 2015.[14]

February 2016

- **U.S. Department of Homeland Security, Federal Bureau of Investigation (government).** A hacker with the Twitter handle @DotGovs released online the names and contact information of 29,000 Department of Homeland Security and FBI employees.[15]

1. Riley Walters, "Cyber Attacks on U.S. Companies in 2014," Heritage Foundation *Issue Brief* No. 4289, October 27, 2014, http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014.
2. Riley Walters, "Cyber Attacks on U.S. Companies Since November 2014," Heritage Foundation *Issue Brief* No. 4487, November 18, 2015, http://www.heritage.org/research/reports/2015/11/cyber-attacks-on-us-companies-sincve-november-2014.
3. Danny Yadron, "Iranian Hackers Infiltrated New York Dam in 2013," *The Wall Street Journal*, December 20, 2015, http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559 (accessed November 30, 2016).
4. News release, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," U.S. Department of Justice, Office of Public Affairs, March 24, 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged (accessed November 30, 2016).
5. News release, "Hyatt Notifies Customers of Malware Activity," Hyatt Hotels, December 23, 2015, http://newsroom.hyatt.com/news-releases?item=123450 (accessed November 30, 2016).
6. "Hyatt's Malware Attack Hit 250 Hotels," *Fortune*, January 15, 2016, http://fortune.com/2016/01/15/hyatts-malware-attack/ (accessed November 30, 2016).
7. News release, "Hyatt Completes Payment Card Incident Investigation," Hyatt Hotels, January 14, 2016, http://newsroom.hyatt.com/news-releases?item=123453 (accessed November 30, 2016).
8. Brian Krebs, "13 Million MacKeeper Users Exposed," KrebsonSecurity, December 14, 2015, https://krebsonsecurity.com/2015/12/13-million-mackeeper-users-exposed/ (accessed November 30, 2016).
9. News release, "Three Men Arrested in Hacking and Spamming Scheme; Targeted Personal Information of 60 Million People," U.S. Department of Justice, U.S. Attorney's Office, District of New Jersey, December 15, 2015, https://www.justice.gov/usao-nj/pr/three-men-arrested-hacking-and-spamming-scheme-targeted-personal-information-60-million (accessed November 30, 2016).
10. Dissent, "191 Million Voters' Personal Info Exposed by Misconfigured Database (UPDATE2)," Databreaches.net, December 28, 2015, https://www.databreaches.net/191-million-voters-personal-info-exposed-by-misconfigured-database/ (accessed November 30, 2016).
11. Dissent, "Misconfigured Database May Have Exposed 1.5 Million Individuals' PHI: Researcher (UPDATE2)," Databreaches.net, December 22, 2015, https://www.databreaches.net/misconfigured-database-may-have-exposed-1-5-million-individuals-phi-researcher-2/ (accessed November 30, 2016).
12. "Alliance Health Reports 30-Month Health Data Exposure," HIPPAA Journal, February 17, 2016, http://www.hipaajournal.com/alliance-health-reports-30-month-health-data-exposure-8317/ (accessed November 30, 2016).
13. Max Metzger, "Mystery Database Leaks Conservative's Personal Details," *SC Magazine*, January 5, 2016, http://www.scmagazineuk.com/mystery-database-leaks-conservatives-personal-details/article/463052/ (accessed November 30, 2016).
14. Brian Krebs, "1,025 Wendy's Locations Hit in Card Breach," KrebsonSecurity, July 8, 2016, https://krebsonsecurity.com/2016/07/1025-wendys-locations-hit-in-card-breach/ (accessed November 30, 2016).
15. Lorenzo Franceschi-Bicchierai, "Hacker Publishes Personal Info of 20,000 FBI Agents," Motherboard, February 8, 2016, https://motherboard.vice.com/read/hacker-publishes-personal-info-of-20000-fbi-agents (accessed November 30, 2016).

March 2016

- **Verizon Enterprise Solutions (network management).** One-and-a-half million Verizon Enterprise customers' contact information was possibly compromised by a security vulnerability. A prominent hacker offered access to the online database for $100,000.[16]

May 2016

- **LinkedIn (online social networking).** Updating the impact of a 2012 breach that saw the exposure of 6.5 million users' passwords, the company confirmed that the true number is now likely closer to 167 million users, 117 million of whom had both their e-mails and passwords exposed.[17]

- **Myspace (online social media).** The same hacker who advertised the compromised LinkedIn database online claim to have a database of Myspace users' credentials—427 million passwords and 360 million e-mail addresses.[18]

- **Noodle & Company (restaurant chain).** The food chain first began investigating its networks after unusual activity was noticed by its credit card processor. Malware led to customers' credit and debit card information being compromised at a number of its locations between January and June.[19]

June 2016

- **Democratic National Committee (political organization).** The political organization's networks were illegally accessed by two separate cyber groups with possible affiliation to the Russian government's Russia Main Intelligence Directorate (GRU) and Federal Security Service (FSB).[20]

- **Voter information.** Chris Vickery found another online database holding 154 million U.S. voters' information and discovered that an IP address based out of Serbia had been interacting with the database as early as April 2016.[21]

- **CiCi's Pizza (restaurant chain).** News of this point-of-sale breach affecting customers' payment information first broke on KrebsOnSecurity. CiCi's Pizza eventually acknowledged the breach and that the compromise to its systems began as early as March 2016.[22] CiCi's Pizza has 135 locations.

July 2016

- **Citibank (banking).** Ninety percent of Citibank's networks across North America were taken offline after an employee in charge of the bank's IT systems, following a poor performance review, sent malicious code to 10 core Citibank Global Control Center routers, shutting down nine of them. He has since been sentenced to 21 months in federal prison and fined $77,200.[23]

16. Brian Krebs, "Crooks Steal, Sell Verizon Enterprise Customer Data," KrebsonSecurity, March 24, 2016, https://krebsonsecurity.com/2016/03/crooks-steal-sell-verizon-enterprise-customer-data/ (accessed November 30, 2016).
17. Lorenzo Franceschi-Bicchierai, "Another Day, Another Hack: 117 Million LinkedIn Emails and Passwords," Motherboard, May 18, 2016, http://motherboard.vice.com/read/another-day-another-hack-117-million-linkedin-emails-and-password (accessed November 30, 2016).
18. Lorenzo Franceschi-Bicchierai, "Hacker Tries to Sell 427 Million Myspace Passwords for $2,800," Motherboard, May 27, 2016, http://motherboard.vice.com/read/427-million-myspace-passwords-emails-data-breach (accessed November 30, 2016).
19. "Notice of Data Security Incident," Noodles & Company, June 28, 2016, http://www.noodles.com/security/ (accessed November 30, 2016).
20. Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," Crowdstrike, June 15, 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (accessed November 30, 2016).
21. Chris Vickery, "Another U.S. Voter Database Leak," MacKeeper, June 26, 2016, https://mackeeper.com/blog/post/239-another-us-voter-database-leak (accessed November 30, 2016).
22. Brian Krebs, "Cici's Pizza: Card Breach at 130+ Locations," KrebsonSecurity, July 19, 2016, http://krebsonsecurity.com/tag/cicis-pizza-breach/ (accessed November 30, 2016).
23. News release, "Former Citibank Employee Sentenced to 21 Months in Federal Prison for Causing Intentional Damage to a Protected Computer," U.S. Department of Justice, U.S. Attorney's Office, Northern District of Texas, July 25, 2016, https://www.justice.gov/usao-ndtx/pr/former-citibank-employee-sentenced-21-months-federal-prison-causing-intentional-damage (accessed November 30, 2016).

August 2016

- **Dropbox (online).** The number of account credentials exposed in a 2012 breach was increased to 68 million users.[24] Hackers were reportedly able to access accounts utilizing a Dropbox employee's password and credentials, possibly taken from the 2012 LinkedIn breach.[25] Yevgeniy Nikulin was indicted on October 20, 2016, for his involvement with both the Dropbox and LinkedIn breaches.[26]

- **Banner Health (health care).** Almost four million patients, physicians, and customers were affected. The breach was first noticed on July 7, 2016, affecting payment card information. A subsequent breach led to the unauthorized access of patients' personal identifiable information, such as birthdates, claims information, and possibly social security numbers.[27]

- **Oracle MICROS (payment).** Operator of 330,000 cash registers globally, this point-of-sale service was reportedly infected by malware.[28] The exploit has a possible connection to the Carbanak gang, an Eastern European hacker group linked to stealing $1 billion from up to 100 banks worldwide,[29] and may also have ties to a Russian security firm.[30]

September 2016

- **Yahoo Inc. (online).** The online company reported that more than 500 million of its users' names, e-mail addresses, birthdates, phone numbers, and passwords were compromised in a 2014—possibly state-sponsored—breach. Yahoo began investigating the breach after 280 million users' information was being offered for sale on the dark web.[31]

- **SS&C Technology (technology).** Tillage Commodities Fund, one of SS&C's clients, was scammed for $5.9 million by reported Chinese hackers. The hackers sent SS&C staff scam e-mails ordering wire transfers of Tillage's money.[32]

October 2016

- **Dyn (online).** The domain name service server was taken offline a number of times, attributed to widespread denial of service attacks. Internet-facing devices were used in this attack after being formed into a botnet through malware. The outage affected how users could access popular sites such as Twitter, Netflix, and *The New York Times*.[33]

24. Joseph Cox, "Hackers Stole Account Details for Over 60 Million Dropbox Users" Motherboard, August 30, 2016, http://motherboard.vice.com/read/hackers-stole-over-60-million-dropbox-accounts (accessed November 30, 2016).
25. Kate Conger and Matthew Lynley, "Dropbox Employee's Password Reuse Led to Theft of 60M+ User Credentials," Tech Crunch, August 30, 2016, https://techcrunch.com/2016/08/30/dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/ (accessed November 30, 2016).
26. News release, "Yevgeniy Nikulin Indicted for Hacking LinkedIn, Dropbox and Formspring" Department of Justice, Office of Public Affairs, October 21, 2016, https://www.justice.gov/opa/pr/yevgeniy-nikulin-indicted-hacking-linkedin-dropbox-and-formspring (accessed November 30, 2016).
27. News release, "Banner Health Identifies Cyber Attack," Banner Health, August 3, 2016, http://www.modernhealthcare.com/assets/pdf/CH10636283.PDF (accessed November 30, 2016).
28. Brian Krebs, "Data Breach at Oracle's MICROS Point-of-Sale Division," KrebsonSecurity, August 8, 2016, http://krebsonsecurity.com/2016/08/data-breach-at-oracles-micros-point-of-sale-division/ (accessed November 30, 2016).
29. Press release, "The Great Bank Robbery: Carbanak Cybergang Steals $1bn from 100 Financial Institutions Worldwide," Kapersky Labs, February 16, 2015, http://www.kaspersky.co.in/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide (accessed November 30, 2016).
30. Brian Krebs, "Carbanak Gang Tied to Russian Security Firm?" KrebsonSecurity, July 18, 2016, https://krebsonsecurity.com/2016/07/carbanak-gang-tied-to-russian-security-firm/ (accessed November 30, 2016).
31. Robert McMillan, "Yahoo Says Information on at Least 500 Million User Accounts Was Stolen," *The Wall Street Journal*, September 22, 2016, http://www.wsj.com/articles/yahoo-says-information-on-at-least-500-million-user-accounts-is-stolen-1474569637 (accessed November 30, 2016).
32. Jon Marino, "China Hackers Swipe Millions in Data Breach," CNBC, September 16, 2016, http://www.cnbc.com/2016/09/16/china-hackers-swipe-millions-in-data-breach.html (accessed November 30, 2016).

- **U.S. Department of the Treasury, Office of the Comptroller of the Currency (OCC) (government).** In November 2015, a former employee at the OCC downloaded swaths of information onto two portable storage devices before his retirement, leading to the unauthorized removal of more than 10,000 unclassified records.[34]

November 2016

- **Friend Finder Networks (online).** The company behind adult online websites such as Adultfriendfinder.com reported that the accounts of 412 million users were exposed online.[35] The online servers were reportedly breached by hackers in October.[36] No credit card information was exposed, but usernames, e-mails, passwords, and date-of-last-visit became available.

Conclusion

This list of successful and notable cyber incidents hardly scratches the surface of the number of smaller attacks or breaches that occur on a daily basis. With this in mind, Congress and the Administration should continue to encourage the sharing of threat information. Either through formal methods with the government and information-sharing centers or through informal communication, threat information sharing can help mitigate the spread of malicious software. The U.S. should continue to improve and encourage the use of existing avenues of information sharing such as those created by the Cybersecurity Act of 2015.[37]

Serious discussions need to take place on how to empower the private sector to engage in more active defense of its networks. The U.S. should create a defined system of active cyber defense that enables private companies to do more to defend their networks. This system should not allow unrestricted "hack back," but should permit firms to use more assertive cyber tools that improve investigatory and attribution capabilities. Despite the potential threats that malicious actors may pose to U.S. online databases and network systems, the Internet and electronic devices continue to drive the economies of the world. The U.S. needs to take cybersecurity seriously while at the same time allowing innovation to continue to thrive.

*—**Riley Walters** is a Research Associate in the Douglas and Sarah Allison Center for Foreign Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*

33. Riley Walters and Jacob Jordan, "U.S. Must Remain Vigilant to Counter Cyberattacks," Daily Signal, October 26, 2016, http://dailysignal.com/2016/10/26/how-a-cyberattack-took-down-twitter-netflix-and-the-new-york-times/.
34. News release, "OCC Notifies Congress of Incident Involving Unauthorized Removal of Information," U.S. Department of the Treasury, Office of the Comptroller of the Currency, October 28, 2016, http://www2.occ.gov/news-issuances/news-releases/2016/nr-occ-2016-138.html (accessed November 30, 2016).
35. "Sexual Secrets for Hundreds of Millions Exposed in Largest Hack of 2016," Leaked Source, November 13, 2016, https://www.leakedsource.com/blog/friendfinder (accessed November 30, 2016).
36. Lorenzo Franceschi-Bicchierai, "Hookup Service 'Adult FriendFinder' May Have Been Hacked—Again," Motherboard, October 19, 2016, http://motherboard.vice.com/read/hookup-service-adult-friendfinder-may-have-been-hacked-again (accessed November 30, 2016).
37. Cybersecurity Information Sharing Act of 2015, S.754, 114th Cong., 1st Sess., https://www.congress.gov/bill/114th-congress/senate-bill/754/text (accessed November 30, 2016).

Appendix: Additional Resources on Cybersecurity and Cyber Incidents

Steven Bucci, Paul Rosenzweig, and David Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2785, April 1, 2013, http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace.

David Inserra and Paul Rosenzweig, "Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation," Heritage Foundation *Issue Brief* No. 4288, October 27, 2014, http://www.heritage.org/research/reports/2014/10/continuing-federal-cyber-breaches-warn-against-cybersecurity-regulation.

Riley Walters, "Continued Federal Cyber Breaches in 2015," Heritage Foundation *Issue Brief* No. 4488, November 19, 2015, http://www.heritage.org/research/reports/2015/11/continued-federal-cyber-breaches-in-2015.

Riley Walters, "Cyber Attacks on U.S. Companies in 2014," Heritage Foundation *Issue Brief* No. 4289, October 27, 2014, http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014.

Riley Walters, "Cyber Attacks on U.S. Companies Since November 2014," Heritage Foundation *Issue Brief* No. 4487, November 18, 2015, http://www.heritage.org/research/reports/2015/11/cyber-attacks-on-us-companies-since-november-2014.