CHAPTER VI

Select Ethical-Hacking Incidences: Chaos Computer Club, CyberBerkut, LulzSec, Iranian Cyber Army, and Others

This chapter takes selected notable ethical-hacking incidences from the quantitative work in chapter 3 and breaks down each incident by: group, target, date, source, motivation, type of attack, whether any other groups claimed responsibility, damage caused, and additional important information. This chapter addresses select incidences for the Chaos Computer Club, CyberBerkut, LulzSec, and others. Again, some of the incidences from the last two chapters, this chapter, and the preceding chapter will be explored in detail from technical, political, criminological, and policy perspectives based on their classification in chapters 7 and 8.

CHAOS COMPUTER CLUB (CCC)

CCC—German Government

ITEM	NOTES
Target:	German government
Date:	October 26, 2011
Source:	Chaos Computer Club website, available at http://ccc.de/en/updates/2011/staatstrojaner. J. Leyden, "German states defend use of 'Federal Trojan'," *The Register*, October 12, 2011, available at http://www.theregister.co.uk/2011/10/12/bundestrojaner/.

	WikiLeaks, "Skype and the Bavarian Trojan in the middle," available at http://wikileaks.org/wiki/Skype_and_the_Bavarian_trojan_in_the_middle. "German hackers discover government spying" (Al Jazeera English, October 25, 2011), available at http://www.youtube.com/watch?v=lIwa_-jvbDQ.
Motivation:	Breach of rights by government and law enforcement, use of the Bundestrojaner (federal Trojan)
Type of attack:	Release of information, analysis of code. (Short critique available at http://web17.webbpro.de/index.php?page=analysis-of-german-bundestrojaner.)
Any other groups claiming responsibility:	No
Damage caused:	Reputation of government. This highlights issues of government-sanctioned malware use beyond the scope of what the courts and laws provide.
Additional important information:	Data encryption is non-existent or ineffective, can be accessed by almost anyone with an internet connection, which presents significant privacy issues outside of direct government involvement.

CCC—Hamburg attack

ITEM	NOTES
Target:	Hamburg bank, Bildschirmtext network
Date:	1985
Source:	J. Harrington, "Hacktivism: What is the Chaos Computer Club?," *Suite101*, September 8, 2011, previously available at http://joharrington.suite101.com/hacktivism-what-is-the-chaos-computer-club-a387917. WIKIPEDIA, "Chaos Computer Club," available at http://en.wikipedia.org/wiki/Chaos_Computer_Club.
Motivation:	To protest use of biometric data for personal documents
Type of attack:	Unauthorized access, modification of data, theft
Any other groups claiming responsibility:	No
Damage caused:	Some DM 135,000 from the bank was "donated" to the CCC

Additional important information:	The funds were apparently returned the next day. Conflicting information regarding date of the hack. Some say 1984, others say 1985. Possibly closer to 1985, though unconfirmed.

CCC—Quicken

ITEM	NOTES
Target:	Quicken database
Date:	1996
Source:	F. von Leitner, "Chaos Computer Club Clarifications," *Tasty Bits from the Technology Front*, February 17, 1997, available at http://tbtf.com/resource/felix.html. Wikipedia, "Chaos Computer Club," available at http://en.wikipedia.org/wiki/Chaos_Computer_Club.
Motivation:	To highlight system flaws
Type of attack:	Data modification, unauthorized access, fraud (though unlikely for personal gain)
Any other groups claiming responsibility:	No
Damage caused:	Changed personal data, cloned SIM cards, wrote ActiveX control, which, once executed, turns off Internet security
Additional important information:	

CCC—German government

ITEM	NOTES
Target:	German government, Minister of the Interior Wolfgang Schäuble
Date:	2008
Source:	S. Ragan, "CCC is at it again—hands out copies of German Interior Minister's fingerprint," *Tech Herald*, August 1, 2008, available at http://www.thetechherald.com/article.php/200814/581/
Motivation:	To protest use of biometric data for personal document authentication
Type of attack:	Unauthorized access.

Any other groups claiming responsibility:	No
Damage caused:	Duplicated the minister of interior's fingerprint (unknown whether the copy was obtained physically or digitally, i.e., from a database) and made it widely available. Fooled biometric scanners.
Additional important information:	Though biometric data is unique to individuals, databases containing such information can be compromised.

CYBERBERKUT

CyberBerkut—US vice-president

ITEM	NOTES
Target:	Joseph Biden's (then US vice-president) delegation officials
Date:	November 25, 2014
Source:	CyberBerkut, "CyberBerkut gained access to the documents of Joseph Biden's delegation officials," November 25, 2014, available at http://cyber-berkut.org/en/
Motivation:	CyberBerkut disagree with Washington's interference in Ukraine's internal affairs
Type of attack:	Unauthorized access of confidential files belonging to the US State Department via an official's mobile device.
Any other groups claiming responsibility:	No
Damage caused:	Publication of confidential government documents.
Additional important information:	CyberBerkut suggested the documents show that the Ukrainian army had become a branch of the US armed forces. They also detailed a high volume of financial support, some of which was credited to the personal accounts of Ukrainian military personnel.

CyberBerkut—German government

ITEM	NOTES
Target:	German government websites
Date:	January 7, 2015
Source:	D. Lynch, "Pro-Russian Hacker Group CyberBerkut Claims Attack On German Government Websites," *International Business Times*, January 7, 2015, available at http://www.ibtimes.com/pro-russian-hacker-group-cyberberkut-claims-attack-german-government-websites-1775874. CyberBerkut, "CyberBerkut has blocked German Chancellor and the Bundestag's websites," January 7, 2015, available at http://cyber-berkut.org/en/.
Motivation:	To urge the people and government of Germany to stop providing financial and political support to the political regime in Kiev, Ukraine's capital city. It accused the Ukrainian Prime Minister of using money from the European Union and International Monetary Fund to fund the war in eastern Ukraine.
Type of attack:	DDoS attack
Any other groups claiming responsibility:	No
Damage caused:	Several German government websites were brought down, including that of the German chancellor's government seat and the Bundestag.
Additional important information:	The attack was executed a day before the chancellor was to meet with the prime minister of Ukraine.

CyberBerkut—Ukrainian politician

ITEM	NOTES
Target:	Dmytro Yarosh (Ukrainian far-right politician)
Date:	February 1, 2015
Source:	RT, "Hacktivist leak alleges 'extortion & money laundering' by Ukraine's Right Sector leader," February 1, 2015, available at http://rt.com/news/228387-ukraine-hacktivists-leak-yarosh/

Motivation:	To disclose corruption and economic crimes in Ukraine. CyberBerkut said: "We are publishing documents that expose the criminal activities of the head of Ukrainian neo-Nazis, which confirm multiple incidences of extortion—the illegal and cynical seizure of properties and businesses belonging to Ukrainian citizens by Yarosh and his associates. The stolen money is then taken out of the country through fronts and deposited in offshore accounts."
Type of attack:	Unauthorized access and publication of documents allegedly obtained from the office of Dmytro Yarosh
Any other groups claiming responsibility:	No
Damage caused:	Publication of legal documents, Yarosh's passport and private documents, several contracts for the purchase and lease of property, allegedly signed under coercion, but which do not directly identify Yarosh.
Additional important information:	Yarosh was placed on Interpol's wanted list in 2015, at Russia's behest, for inciting terrorism (his name was removed in 2016). He has served in the Ukrainian parliament since November 2014. In 2014 Ukraine was named the most corrupt country in Europe by Transparency International. CyberBerkut is named after the previous, pro-Russian Ukrainian administration's unit responsible for public security, known for brutality; it has a reputation for targeting government figures and executing DDoS attacks.

ITEM	NOTES
Target:	Central Election Commission of Ukraine
Date:	May 21, 2014
Country:	Ukraine
Source:	A. K. Jha, "Pro-Russian Hackers leaks documents from Central Election Commission of Ukraine," *Tech Worm*, May 24, 2014, available at http://www.techworm.net/2014/05/pro-russian-hackers-leaks-documents.html. The hackers claimed responsibility for the attack in a statement released on their website, and said they would continue to make such information public on the following website: http://www.cyber-berkut.org/en/.
Motivation:	To protest the "legitimization of crimes"

Type of attack:	Destroyed the network and computing infrastructure of the Ukrainian election commission. Leaked information.
Damage caused:	As above
Additional important information:	Ethical-hacking protest. The leaks came just two days before presidential elections in Ukraine. Hackers also leaked a large archive of emails, as well as the technical documentation of the commission's system administrators. The hackers gave a "thank you" message to the commission of Ukraine, saying: "Our special thanks for a fascinating quest to wonderful administrators who were storing data on access to the network in text files on their desktops."

LULZSEC

LulzSec—Sony BMG Greece

ITEM	NOTES
Target:	Sony BMG—Greece
Date:	May 22, 2011
Source:	C. Wisniewski, "Sony BMG Greece the latest hacked Sony site," *Naked Security*, May 22, 2011, available at http://nakedsecurity.sophos.com/2011/05/22/sony-bmg-greece-the-latest-hacked-sony-site/. E. Mills, "Hackers taunt Sony with more data leaks, hacks," *CNET*, June 6, 2011, available at http://news.cnet.com/8301-27080_3-20069443-245/hackers-taunt-sony-with-more-data-leaks-hacks/.
Motivation:	Unspecified
Type of attack:	SQL injection, unauthorized access, data leak
Any other groups claiming responsibility:	No
Damage caused:	Release of usernames, identities, and email addresses of users registered on SonyMusic.gr. Release of internal network map.

Additional important information:	Large quantity of information reported to be incorrect. The hack emphasized that companies need to be more aware of the importance of performing penetration tests to ensure security.

LulzSec—FBI

ITEM	NOTES
Target:	Infragard (Atlanta)—FBI affiliate
Date:	June 3, 2011
Source:	R. Beschizza, "LulzSec claims FBI affiliate hacked, users and botnet are exposed," *Boing Boing*, June 3, 2011, available at http://boingboing.net/2011/06/03/lulzsec-claims-fbi-a.html. "LulzSec hacks Atlanta Infragard and challenges FBI" (June 3, 2011), available at http://www.youtube.com/watch?v=aROWwEIPgJA.
Motivation:	Unspecified
Type of attack:	Unauthorized access, data leak, modification of data, defacement
Any other groups claiming responsibility:	No
Damage caused:	Released personal information stored in the user database of 180 users, defaced http://infragardatlanta.org/, and caused reputational damage
Additional important information:	N/A

LulzSec—PBS

ITEM	NOTES
Target:	PBS
Date:	May 29–30, 2011
Source:	C. Wisniewski, "PBS.org hacked... LulzSec targets Sesame Street?," *Naked Security*, May 30, 2011, available at http://nakedsecurity.sophos.com/2011/05/30/pbs-org-hacked-lulzsec-targets-sesame-street/ (last accessed May 31, 2011).

	S. Ragan, "PBS: LulzSec attack an attempt to chill journalism," *Tech Herald*, May 30, 2011, available at http://www.thetechherald.com/article.php/201122/7215/PBS-LulzSec-attack-an-attempt-to-chill-journalism. "Happy Hour: Weinergate, PBS Hacked" (June 1, 2011) http://www.youtube.com/watch?v=BiGEIPT8XFQ.
Motivation:	According to Wisniewski, LulzSec "took offense to the portrayal of Bradley Manning in a segment on PBS's Frontline news magazine program"; pro-WikiLeaks attack
Type of attack:	As per Ragan, LulzSec claimed "they used a zero-day exploit in Movable Type 4 and were able to compromise Linux servers running outdated kernels."
Any other groups claiming responsibility:	No
Damage caused:	Released login credentials of database administrators/users and those of affiliates; defaced/injected their own website
Additional important information:	N/A

LulzSec—CIA

ITEM	NOTES
Target:	CIA
Date:	June 15, 2011
Source:	J. Davis, "LulzSec's CIA hack just one of many high-profile hackings," *International Business Times*, June 15, 2011, available at http://www.ibtimes.com/articles/163678/20110615/google-lulzsec-s-cia-hack-just-one-of-many-high-profile-hackings.htm (last accessed June 20, 2011). S. Schroeder, "LulzSec Hackers Take Down CIA Website," *Mashable*, June 16, 2011, available at http://mashable.com/2011/06/16/lulzsec-hackers-cia/. "LulzSec Hacks the CIA" (June 17, 2011), available at http://www.youtube.com/watch?v=QzQMBaIjo_w.
Motivation:	Unspecified
Type of attack:	DDoS

Any other groups claiming responsibility:	No
Damage caused:	CIA website was inaccessible for an unspecified period, though reported as "several hours."
Additional important information:	N/A

LulzSec—Lockheed Martin

ITEM	NOTES
Target:	Lockheed Martin
Date:	May 2011
Source:	Sky News, "Cyber-Warfare: The New Global Battlefield," October 31, 2011, available at https://news.sky.com/story/cyber-warfare-the-new-global-battlefield-10484457. "Chinese Regime Suspected in Lockheed Martin Hacking" (NTDTV, June 7, 2011), available at http://www.youtube.com/watch?v=1OXO0xgN1TU.
Motivation:	Unknown
Type of attack:	Unauthorized access
Any other groups claiming responsibility:	No
Damage caused:	Lockheed Martin claimed that no crucial data had been taken, though Sky News reported the company's "internal systems took a few days to fully recover."
Additional important information:	Many sources refer to Lockheed Martin being hacked and a recovery time of several days, though details are sparse. As per Sky, "Shortly after the breach, the UK government announced the formation of the National Cyber Security Programme, a special unit of the Ministry of Defence tasked with reducing the UK's vulnerability to cyber crime and attacks."

LulzSec—Russia

ITEM	NOTES
Target:	Sony Pictures Russia
Date:	June 6, 2011
Source:	E. Mills, "Hackers taunt Sony with more data leaks, hacks," *CNET*, June 6, 2011, available at http://news.cnet.com/8301-27080_3-20069443-245/hackers-taunt-sony-with-more-data-leaks-hacks/. L. Constantin, "Sony Pictures Russian Website Compromised," *Softpedia*, June 6, 2011, available at http://news.softpedia.com/news/Sony-Pictures-Russian-Website-Compromised-204563.shtml.
Motivation:	Unspecified
Type of attack:	SQL injection
Any other groups claiming responsibility:	No
Damage caused:	Site inaccessible for an unspecified amount of time (presumably down for maintenance). The hackers "published the structure of the database which appears to contain information about accounts registered on the content management solution (CMS) used by Sony Pictures, as well as the site's forum," Constantin reported.
Additional important information:	In announcing the hack on Postbin, they wrote "in Soviet Russia, SQL injects you..."

LulzSec—Brazil

ITEM	NOTES
Target:	Brazilian Government websites—website of the president, country's tax agency, Ministry of Sports, and political parties Brazilian Corporations—Petrobras Oil & Gas Company, Rede Globo television network
Date:	2011
Source:	P. Olson, "How Twitter Helped Brazil Become a Hotbed for Hacktivists," *Forbes*, February 27, 2012, available at http://www.forbes.com/sites/parmyolson/2012/02/27/how-twitter-helped-brazil-become-a-hotbed-for-hacktivists/

Motivation:	Unknown
Type of attack:	Data theft and publication
Any other groups claiming responsibility:	No
Damage caused:	Personal information of federal police agents and Petrobras employees was published.
Additional important information:	Associated with the broader LulzSec movement. Group noted for their use of Twitter.

LulzSec/Lance Moore—AT&T

ITEM	NOTES
Target:	AT&T
Date:	2011
Source:	FBI, "Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks" (press release, July 19, 2011), available at http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks (last accessed November 10, 2011). A. Martin, "How Two LulzSec Hackers Slipped Up," *The Atlantic*, July 20, 2011, available at https://www.theatlantic.com/technology/archive/2011/07/how-two-lulzsec-hackers-slipped/353089/.
Motivation:	Part of "50 Days of Lulz." "Just because we could."
Type of attack:	Unauthorized access/hack
Any other groups claiming responsibility:	LulzSec publicized that they had obtained and published the stolen information. Unclear whether Moore is a member of LulzSec or whether LulzSec published the information uploaded by Moore to file-sharing websites.
Damage caused:	Theft of confidential business information and publication via file-sharing websites
Additional important information:	Moore is a customer-support contractor and "exceeded his authorized access to AT&T servers" (i.e., a grey-hat hack). Moore is charged (there is no public record of the case having been resolved) with one count of accessing a protected computer without authorization.

	The charge of intentional damage to a protected computer carries a maximum penalty of ten years in prison and a $250,000 fine. Each count of conspiracy carries a maximum penalty of five years in prison and a $250,000 fine.

LulzSec—Jamaican Credit Union, school computers

ITEM	NOTES
Target:	Jamaican Credit Union and school computers
Date:	2012
Source:	J. Halliday and C. Arthur, "Anonymous' Release of Met and FBI Call Puts Hacker Group Back Centre Stage," *Guardian*, February 3, 2012, available at http://www.guardian.co.uk/technology/2012/feb/03/anonymous-hack-met-fbi-call
Motivation:	To release members of Anonymous who had been arrested and detained
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	Jamaican Credit Union and several school computers hacked
Additional important information:	User arrested by joint operation between London Metropolitan Police and the FBI

LulzSec/Ryan Cleary—IFPI, BPI, SOCA

ITEM	NOTES
Target:	International Federation of the Phonograph Industry, British Phonographic Industry, Serious Organised Crime Agency
Date:	October–November 2010
Source:	V. Dodd and J. Halliday, "Teenager Ryan Cleary Charged Over LulzSec Hacking," *Guardian*, June 22, 2011, available at https://www.theguardian.com/technology/2011/jun/22/ryan-cleary-charged-lulzsec-hacking
Motivation:	To protest intellectual property laws
Type of attack:	DDoS, Botnet
Any other groups claiming responsibility:	Other Anonymous members were involved

Damage caused:	Cleary conspired to impair the operation of a computer
Additional important information:	In a statement, police said Cleary "did conspire with other person or persons unknown to conduct unauthorized modification of computers by constructing and distributing a computer program to form a network of computers (a botnet) modified and configured to conduct Distributed Denial of Service attacks." Cleary was charged with five offences stemming from the Criminal Law Act and the Computer Misuse Act; investigation by London Metropolitan Police's e-crime unit.

LulzSec—MilitarySingles.com

ITEM	NOTES
Target:	Dating site MilitarySingles.com
Date:	2011
Source:	C. Arthur, "Hacking Group Claiming to be LulzSec Targets US Military Dating Website," *Guardian*, March 28, 2012, available at http://www.guardian.co.uk/technology/2012/mar/28/hacking-group-lulzsec-dating-website
Motivation:	Unknown—potentially military protest or personal protest
Type of attack:	Unauthorized access
Any other groups claiming responsibility:	No
Damage caused:	Emails, passwords, and physical addresses of members leaked on Pastebin website
Additional important information:	

IRANIAN CYBER ARMY

Iranian Cyber Army—Twitter

ITEM	NOTES
Target:	Twitter
Date:	December 17, 2009
Source:	*Green Voice of Freedom*, "Who are the 'Iranian Cyber Army,'" December 15, 2010, previously available at http://en.irangreenvoice.com/article/2010/feb/19/1236 (last accessed December 16, 2010).

	"Twitter Hacked by Iranian Cyber Army (Poetry Reading)" (December 19, 2009), available at http://www.youtube.com/watch?v=rVHZ4MaCmmQ.
Motivation:	Appears to be retaliation for Western sanctions on Iran
Type of attack:	Unauthorized access, modification of data, re-directing communications, website defacement.
Any other groups claiming responsibility:	No
Damage caused:	Twitter and many sub-domains were inaccessible for an unspecified period. DNS redirection means that the site itself may not have been defaced; rather, that users were being sent to the wrong page.
Additional important information:	N/A

Iranian Cyber Army—Baidu

ITEM	NOTES
Target:	Baidu
Date:	January 11, 2010
Source:	BBC News, "Baidu hacked by 'Iranian cyber army.'" January 12, 2010, available at http://news.bbc.co.uk/2/hi/8453718.stm (last accessed January 13, 2010). *Green Voice of Freedom*, "Who are the 'Iranian Cyber Army,'" December 15, 2010, previously available at http://en.irangreenvoice.com/article/2010/feb/19/1236 (last accessed December 16, 2010).
Motivation:	Anti-democracy
Type of attack:	DNS cache poisoning, unauthorized access, modification of data, re-directing communications, website defacement
Any other groups claiming responsibility:	No
Damage caused:	Biadu website inaccessible for approximately four hours
Additional important information:	Unknown whether DNS records or the site itself was compromised. Interesting to note the attack of a Chinese tech giant—versus, say, Twitter in the United States—given Iran's good relations with China.

Iranian Cyber Army—VoA

ITEM	NOTES
Target:	Voice of America and related sites
Date:	February 22, 2011
Source:	S. Ragan, "Iranian Cyber Army defaces Voice of America and 93 other domains (Update)," *Tech Herald*, February 22, 2011, available at http://www.thetechherald.com/article.php/201108/6849/Iranian-Cyber-Army-defaces-Voice-of-America-and-93-other-domains. "VOICE of America News Website Hacked By Iranian Cyber Army" (February 22, 2011), available at http://www.youtube.com/watch?v=nDkVveI4G8Q.
Motivation:	To protest American interference with Islamic countries
Type of attack:	DNS cache poisoning, unauthorized access, modification of data, re-directing communications, website defacement
Any other groups claiming responsibility:	No
Damage caused:	Re-directed the Voice of America home site to one with a protest message. Claim to have hit ninety other sites with the same attack (most of them VOA-related). Sites inaccessible for an unspecified period
Additional important information:	N/A

Iranian Cyber Army—Tech Crunch

ITEM	NOTES
Target:	Tech Crunch
Date:	January 26, 2010
Source:	TechnoFriends, "TechCrunch Hacked? (yes, Techcrunch got hacked)," January 26, 2010, available at http://technofriends.in/2010/01/26/did-techcrunch-got-hacked/ (last accessed November 15, 2010). J. Kirk, "Iranian Cyber Army Moves Into Botnets," *PCWorld*, August 25, 2010, available at http://www.pcworld.com/businesscenter/article/208670/iranian_cyber_army_moves_into_botnets.html.
Motivation:	Unknown

Type of attack:	Potentially DNS cache poisoning, social engineering, and denial-of-service attack.
Any other groups claiming responsibility:	No
Damage caused:	Per Kirk, the group "installed a page on TechCrunch's site that redirected visitors to a server that bombarded their PCs with exploits in an attempt to install malicious software."
Additional important information:	N/A

OTHER GROUPS

Honker Union of China

ITEM	NOTES
Target:	US Military and government servers and sites
Date:	April 2001
Source:	J. Nazario, "Politically Motivated Denial of Service Attacks," available at http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf. T. L. Thomas, "The Internet in China: Civilian and Military Uses," *Information & Security: An International Journal* 7 (2001), 159–173, available at http://fmso.leavenworth.army.mil/documents/china-internet.htm.
Motivation:	Retaliation for mid-air collision of a Chinese fighter jet and US spy plane, which killed the Chinese pilot
Type of attack:	DDOS, unauthorized access, modification of data, website defaced, defacement of websites
Any other groups claiming responsibility:	Not claiming responsibility but certainly participating were the Hacker Union of China and the China Eagle Union
Damage caused:	Defaced or crashed some hundred websites. Majority were .gov and .com domains. Defacements of US sites included the posting of pictures of the dead Chinese pilot and anti-US messages. Similar acts perpetrated by pro-US hackers on approximately 300 Chinese websites.

Additional important information:	Some pro-Chinese hackers wiped several compromised servers. Generally considered bad form to do so.

Unknown—Response to Chinese embassy bombing

ITEM	NOTES
Target:	US Energy and Interior Departments, National Park Service websites
Date:	May 9, 1999
Source:	CNN Tech, "Hackers attack US government Web sites in protest of Chinese embassy bombing," May 10, 1999, available at http://edition.cnn.com/TECH/computing/9905/10/hack.attack/ (last accessed November 10, 2011)
Motivation:	To protest NATO bombing of Chinese embassy in former Yugoslavia
Type of attack:	Unauthorized access, modification of data, defacement
Any other groups claiming responsibility:	No
Damage caused:	Websites were defaced for an unspecified period. One site was down for over twenty-four hours.
Additional important information:	White House website also went off-line, though this was claimed to be the result of equipment failure and not the work of hackers

Freedom Force Cyber Militia

ITEM	NOTES
Target:	Al-Jazeera—Qatar-based satellite TV network
Date:	March 25, 2003
Source:	Reuters, "War Hack Attacks Tit For Tat," *Wired*, March 28, 2003, available at http://www.wired.com/politics/law/news/2003/03/58275 (last accessed November 10, 2011)
Motivation:	To protest airing footage of British/American POWs and soldiers
Type of attack:	Unauthorized access, modification of data, and defacement
Any other groups claiming responsibility:	No

Damage caused:	Website defaced with pro-Western/US messages, Arabic-language version unavailable for twenty-four hours, English-language version unavailable for over five days.
Additional important information:	N/A

Operation Moonlight Maze

ITEM	NOTES
Target:	US Defense And Energy Departments, NASA, and US weapons labs
Date:	March 1998–1999
Source:	Bloomberg, "An Evolving Crisis," *Business Week*, April 10, 2008, available at https://www.bloomberg.com/news/articles/2008-04-09/an-evolving-crisis
Motivation:	Unknown
Type of attack:	Not specified
Any other groups claiming responsibility:	No
Damage caused:	Websites compromised
Additional important information:	Per a source quoted in the Bloomberg report: "At times, the end point [for the data] was inside Russia." The Russian Government denied responsibility.

Solar Sunrise (California and Israeli)

ITEM	NOTES
Target:	US Air Force and Navy computers
Date:	February 1998
Source:	Bloomberg, "An Evolving Crisis," *Business Week*, April 10, 2008, available at https://www.bloomberg.com/news/articles/2008-04-09/an-evolving-crisis
Motivation:	To protect Israel
Type of attack:	Malicious code
Any other groups claiming responsibility:	No

Damage caused:	Malicious code infected
Additional important information:	Some attacks routed through United Arab Emirates. The hackers were two teenagers from Cloverdale, California, and an Israeli accomplice who goes by the name of "Analyzer."

Unknown—US nuclear sites

ITEM	NOTES
Target:	National Nuclear Security Administration (NNSA), US Department of Energy
Date:	March 20, 2012
Source:	A. Tarantola, "US Nuke Stockpile Control Systems Are 'Under Constant Attack,'" *Gizmodo*, March 21, 2012, available at http://gizmodo.com/5895033/us-nuke-stockpile-control-systems-are-under-constant-attack
Motivation:	Anti-US sentiment and pro-nuclear proliferation
Type of attack:	Ten million attacks per day, mostly via botnets
Any other groups claiming responsibility:	"Other countries' [governments], but we also get fairly sophisticated non-state actors as well," according to the NNSA's head (quoted in Tarantola).
Damage caused:	Security breach resulted in classified-data theft (from Oak Ridge National Laboratory in April 2011)
Additional important information:	These types of attacks are expected and managed well. By creating an "air gap" in their system to disconnect themselves from the Internet and run on smaller private networks, the scope for attacks on nuclear facilities is reduced, despite persistent threats. Perhaps this should be a model for other sensitive facilities. By focusing more in intranets and air gaps some cyber-security obstacles may be overcome, or at least better managed.

Unknown—US Thrift Savings Plan

ITEM	NOTES
Target:	US federal employees belonging to the Thrift Savings Plan
Date:	May 25, 2012
Source:	Fox News, "Cyberattack Targeted Personal Data of over 100,000 Federal Employees," May 26, 2012, available at https://www.foxnews.com/tech/cyberattack-targeted-personal-data-of-over-100k-federal-employees

Motivation:	Unknown
Type of attack:	Unknown
Any other groups claiming responsibility:	No
Damage caused:	Personal information on 100,000 federal employees seized, including detailed information on $133 billion worth of assets
Additional important information:	No funds were believed to be compromised

Hacker Prank—"Zombie" Attack

ITEM	NOTES
Target:	Two TV stations in Michigan and several in California, Montana, and New Mexico.
Date:	February 18, 2013
Source:	J. Finkle, "Zombie Attack Exposes Security Flaws, Experts Say," *Sydney Morning Herald*, February 15, 2013, available at http://www.smh.com.au/technology/technology-news/zombie-attack-exposes-security-flaws-experts-say-20130215-2egpw.html
Motivation:	Prank to expose security flaws
Type of attack:	The hackers used unchanged manufacturer's default passwords
Any other groups claiming responsibility:	No
Damage caused:	None, hackers just sent a bogus warning of a zombie apocalypse
Additional important information:	Per Finkle, "A male voice addressed viewers in a video posted on the internet of the bogus warning broadcast from KRTV, a CBS affiliate based in Great Falls, Montana: 'Civil authorities in your area have reported that the bodies of the dead are rising from the grave and attacking the living." The voice warned not "to approach or apprehend these bodies as they are extremely dangerous.'" A fear is that perpetrators could prevent the government from sending out public warnings during an emergency or attackers could conduct a more damaging hoax than a warning of a zombie apocalypse.

TeaMp0isoN

ITEM	NOTES
Target:	UK police, RIM Blackberry
Date:	August 9, 2011
Source:	D. Neal, "Team Poison hacks Blackberry after riots," *Inquirer*, August 9, 2011, available at http://www.theinquirer.net/inquirer/news/2100557/team-poison-hacks-blackberry-riots.
Motivation:	Protest UK police tracking of looters and rioters after a man was fatally shot by police in London
Type of attack:	Unauthorized access and data theft
Any other groups claiming responsibility:	No
Damage caused:	None. Claimed to have access to RIM employee information and threatened to use it in a menacing way.
Additional important information:	Hacked LulzSec in early July 2011

TeaMp0isoN—London Metropolitan Police Anti-Terrorist Hotline

ITEM	NOTES
Target:	Metropolitan Police Anti-Terrorist Hotline
Date:	April 10, 2012
Source:	M. Smolaks, "Two Possible TeaMp0isoN Members Arrested," Tech Week Europe, April 13, 2012, available at http://www.techweekeurope.co.uk/news/teamp0ison-policeteampoison-arrested-72738
Motivation:	According to statements made by the hackers, the attack was a response to the recent events when London Metropolitan Police's Counter Terrorism Command and British courts extradited Babar Ahmad, Adel Abdel Bary, and other terrorism suspects to be tried in America
Type of attack:	Hotline hacked, prank calling, and computerized auto-dialling
Any other groups claiming responsibility:	No

Damage caused:	Service disabled and private conversations between anti-terrorist hotline staff posted online.
Additional important information:	Extradition was a key theme here

Bank of England

ITEM	NOTES
Target:	No target—this is a protective mechanism taken by the Bank of England regarding ethical hacking
Date:	April 23, 2014
Country:	England
Source:	D. Wilson, "Bank of England turns to 'ethical hackers' to fix financial security," *Tech Rader,* April 23, 2014, available at http://www.techradar.com/au/news/internet/web/bank-of-england-turns-to-ethical-hackers-to-fix-financial-sector-security-1244589
Motivation:	To fix financial-sector security
Type of attack:	This was not an attack
Damage caused:	N/A
Additional important information:	Bank of England hired white-hat (ethical) hackers to test and improve the resilience of networks behind twenty of the United Kingdom's biggest banks and financial-services firms. The bank oversees a programme of ethical hacking designed to improve computer security in the financial sector. Bank of England will hire specialists from approved companies with CREST (Council for Registered Ethical Security Testers) certification, who will perform penetration testing to look for vulnerabilities that might be exploited by unscrupulous cyber criminals. The Bank of England plans have been piloted and it is expected that major players like the Royal Bank of Scotland and London Stock Exchange will take part.

Gator League

ITEM	NOTES
Target:	British intelligence and surveillance agency Government Communications Headquarters (GCHQ)
Date:	December 23, 2014
Source:	G. C. Kharel, "Hactivist Group Gator League Brings Down British GCHQ Website, Takes Blame for N Korean Internet Outage," *International Business Times*, December 24, 2014, available at http://www.ibtimes.co.in/gator-league-brings-down-british-gchq-website-takes-blame-n-korean-internet-outage-618166. *The Anonymous Log*, Facebook (January 4, 2015), https://www.facebook.com/TheAnonymousLog. RT, "Hacktivist group 'takes down' GCHQ website, claims N. Korean blackout," December 24, 2014, available at http://rt.com/news/217211-gchq-website-down-hackers/. AnonWatcher, "GCHQ Hacked. North Korea Claimed," *AnonHQ*, January 3, 2015, available at http://anonhq.com/gchq-hacked-north-korea-claimed/.
Motivation:	GCHQ is an UK intelligence branch in conflict with Anonymous and LulzSec, hacktivists responsible for DDoS attacks. Gator League and Anonymous are allies and this attack was the Gator League's Christmas attack.
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	Website down for more than an hour
Additional important information:	The GCHQ is an UK intelligence branch made up of specialist hackers tasked with using DDoS attacks against hackers themselves and revealing the identities of these hackers. A motivation for the hacktivists lies in the power that the GCHQ has, as it is not bound by international law and regulation.

Decocidio

ITEM	NOTES
Target:	European Climate Exchange
Date:	July 23, 2010
Source:	L. Leyden, "EU climate exchange website hit by green-hat hacker," *The Register*, July 26, 2010, available at http://www.theregister.co.uk/2010/07/26/climate_exchange_website_hack/ (last accessed July 27, 2010). Takver, "European Climate Exchange website hacked," *Independent Media Centre Australia*, July 25, 2010, available at http://indymedia.org.au/2010/07/24/european-climate-exchange-website-hacked (last accessed July 29, 2010).
Motivation:	Political protest related to carbon credits
Type of attack:	Unauthorized access, modification of data, website defaced
Any other groups claiming responsibility:	No
Damage caused:	Site was defaced for a weekend. Highlighted the group's opposition to carbon trading as a means of tackling climate change.
Additional important information:	Superficial solution when it may still be more profitable for a corporation to pay fines for environmental damage than to effectively minimize such damage. Cited links to the "Climategate" scandal in 2009, though information is sketchy. Leaked communications pertaining to manipulation of climate-change data by researchers. This was never found to be the work of hackers.

DAX stock index

ITEM	NOTES
Target:	German stock index DAX (or may have actually targeted French rugby team fan site)
Date:	October 2011
Source:	J. Leyden, "Hackers mistake French rugby site for German stock exchange," *The Register*, November 4, 2011, available at http://www.theregister.co.uk/2011/11/04/french_rugby_site_hacktivist_maul/.
Motivation:	Likely an Occupy Wall Street–style protest against the DAX website

Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	Accidently took down a French rugby team's fan site (allezdax.com) for two weeks.
Additional important information:	Not known who was responsible for the attack. Since no one has come forward, it can be assumed that the team website was not the intended target, though inconclusive. Seemed to have been reported only after the website was back up and running. Time of attack could possibly be mid-October.

Unknown—Union for a Popular Movement, France

ITEM	NOTES
Target:	Union for a Popular Movement (UMP), French political party
Date:	November 10, 2011
Source:	The Wrong Guy, "Activists hack French ruling party's phone numbers," *WhyWeProtest*, November 10, 2011, available at http://forums.whyweprotest.net/threads/activists-hack-french-ruling-partys-phone-numbers.96206/
Motivation:	Protesting apparent oppression of party members and treatment of protesters
Type of attack:	Unauthorized access and data leak
Any other groups claiming responsibility:	No
Damage caused:	Published personal details including phone numbers of senior members of right-wing French President Nicolas Sarkozy's UMP party
Additional important information:	N/A

French G20 conference files

ITEM	NOTES
Target:	G20 conference files from the French Finance Ministry
Date:	February 2011
Source:	S. Curtis, "China Implicated in Hack of French G20 Files," *Tech Week Europe*, March 7, 2011, available at https://www.silicon.co.uk/workspace/china-implicated-in-hack-of-french-g20-files-23062.
Motivation:	Protest in relation to Chinese government's treatment at the G20 (Chinese government resisted calls at the summit to target exchange-rate valuations, currency reserves, and economic surpluses)
Type of attack:	Most likely targeted Trojans embedded in legitimate government PDF files and other attachments
Any other groups claiming responsibility:	No
Damage caused:	Theft of G20 conference files and infection of up to 150 government computers
Additional important information:	No evidence of Chinese government involvement. However, according to an anonymous official, a "certain amount of the information was redirected to Chinese sites" (quoted in Curtis). "Although the Chinese connection has not been proved, there are hacker groups in China specialising in this sort of attack and claiming to be funded—directly or indirectly—by the military and/or government" (see Curtis).

RedHack

ITEM	NOTES
Target:	A number of organizations, including the cities of Kars and Amasya, the gas-distribution authority of Sakarya, the Ministry of Education.
Date:	February 10, 2014
Country:	Turkey

Source:	E. Kovacs, "RedHack begins hack attacks in protest against Turkey's New Internet Law," Softpedia, February 10, 2014, available at http://news.softpedia.com/news/RedHack-Begins-Hack-Attacks-in-Protest-Against-Turkey-s-New-Internet-Law-425418.shtml
Motivation:	To protest a new Internet law in Turkey, which is seen as a serious limit on freedom of speech
Type of attack:	Website defacement, copy of information, leak of information
Damage caused:	Defaced websites and leaked information
Additional important information:	RedHack leaked the phone numbers of "murderer police chiefs and superintendents." The hacktivists then defaced the website of the Kars municipality (kars.bel.tr), posting a message opposing the new Internet law. Another website targeted by RedHack was the gas-distribution authority of Sakarya, on which they posted a message saying that gas should be free because the government is "stealing enough from the people." The website of the city of Amasya was targeted, from which the hacktivists leaked AKP (Justice and Development Party) membership applications. The Ministry of Education was also attacked, whereby invoices and school expenditures were published online, on JustPaste.it. The hackers wrote on Twitter: "Ministry of Education—There are some astronomical expenditures which clearly shows there is degree of corruption, especially on water bills." The controversial Internet-censorship law has been criticized not only by Turkish citizens, but also by the EU. Peter Stano, spokesperson for European Commissioner for Enlargement Stefan Füle, said, "The Turkish public deserves more information and more transparency, not more restrictions. The law needs to be revised in line with European standards."

RedHack

ITEM	NOTES
Target:	Turkish Telecommunications Directorate (Telekomünikasyon İletişim Başkanlığı, or Tib)
Date:	March 28, 2014
Country:	Turkey
Source:	E. Kovacs, "RedHack Begins Hack Attacks in Protest Against Turkey's New Internet Law," *Tech Worm*, March 28, 2014, available at http://www.techworm.net/2014/03/redhack-ddoses-turkish.html
Motivation:	Done in protest of the government's banning of Twitter and YouTube across the country.
Type of attack:	DDoS
Damage caused:	Unknown
Additional important information:	TIB had blocked YouTube hours after an audio recording leaked, allegedly featuring the voices of Turkey's foreign minister, intelligence chief, and a top army general discussing the developments in neighbouring war-torn Syria was uploaded on YouTube. This ban came one week after TIB blocked Twitter in a move seen as a response to leaked audio recordings posted on site that appear to implicate Prime Minister Recep Tayyip Erodgan in the banning measure. In response to the banning of Twitter and YouTube, RedHack took down the website of the Presidency of Telecommunication and Communication of Turkey. The TIB website was attacked on a Thursday night and was restored on the Friday morning, but with an additional "tr" in the URL. The original URL listed on Google is still not available. Typing in the original URL, one is automatically redirected to the new URL. After the attack, RedHack posted this message on its Twitter account: "You forgot the coordinator of everything while calculating things. The ban is meant to be banned."

RedHack

ITEM	NOTES
Target:	Turkish Cooperation and Coordination Agency
Date:	May 18, 2014
Country:	Turkey
Source:	A. K. Jha, "RedHack leaks email id's and password from Turkish Cooperation and Coordination Agency (TIKA)," *Tech Worm*, May 18, 2014, available at http://www.techworm.net/2014/05/redhack-leaks-email-ids-and-password.html
Motivation:	Corruption of the government
Type of attack:	Email usernames and passwords of agency personnel were leaked
Damage caused:	Email usernames and passwords made public online, including via Twitter
Additional important information:	The leak was done to protest government corruption. The leak was announced on RedHack's Twitter account. The leak also served to shame the email users with claims that users had accessed adult dating sites.

Shaltai Boltai

ITEM	NOTES
Target:	Russian Prime Minister Dmitry Medvedev
Date:	August 14, 2014
Country:	Russia
Source:	A. K. Jha, "Russian Prime Minister's Twitter account hacked," *Tech Work*, August 14, 2014, available at http://www.techworm.net/2014/08/russian-prime-ministers-twitter-account.html
Motivation:	To criticize the Russian government and President Putin
Type of attack:	Twitter account hacked
Damage caused:	Russian prime minister's Twitter account hacked
Additional important information:	Medvedev's official Twitter account had more than 2.52 million followers and was hacked, the hackers posting tweets through the account, such as: "I am resigning. Ashamed of the actions of the government. I'm sorry, Forgive me."

	The hackers also managed to retweet several anti-Russian government and anti-Putin messages from several Russian anti-Putin journalists and democracy activists. The tweets were removed after about forty minutes and a spokesperson for the Russian government later acknowledged the hack. Hacker group Shaltai Boltai took responsibility for the hack. The group claimed it had obtained access to several of Medvedev's email accounts and data from three of his iPhones. Shaltai Boltai claimed they represent disgruntled Russian government officials upset at Putin's recent hardline turn and aggressive policy toward Ukraine.

Unknown—HKEx

ITEM	NOTES
Target:	Hong Kong Stock Exchange (HKEx)
Date:	August 10, 2011
Source:	C. Wisniewski, "Hong Kong stock exchange (HKEx) website hacked, impacts trades," *Naked Security*, August 10, 2011, available at http://nakedsecurity.sophos.com/2011/08/10/hong-kong-stock-exchange-hkex-website-hacked-impacts-trades/. C. Wisniewski, "Hong Kong stock exchange attacked for second day in a row," *Naked Security*, August 12, 2011, available at http://nakedsecurity.sophos.com/2011/08/12/hong-kong-stock-exchange-attacked-for-second-day-in-a-row/.
Motivation:	Possibly to accompany occupy movements
Type of attack:	DDoS
Any other groups claiming responsibility:	Unknown
Damage caused:	Unspecified
Additional important information:	Possibly perpetrated by Anonymous

Unknown—Activism by mail

ITEM	NOTES
Target:	Chinese government
Date:	February 1, 2001
Source:	M. Farley, "Dissidents Hack Holes in China's New Wall," *Los Angeles Times*, January 4, 1999, available at http://articles.latimes.com/1999/jan/04/news/mn-60340
Motivation:	Freedom of speech, pro-democracy
Type of attack:	Subversion of security measures and mail/email
Any other groups claiming responsibility:	Multiple groups, including Bronc Buster, Cult of the Dead Cow, and the Hong Kong Blondes
Damage caused:	No apparent damage. Subversion of security protocols by using private email to distribute pro-democracy literature. Such literature was also sent to many Chinese government officials.
Additional important information:	N/A

Unknown—Hong Kong Civil Referendum Website

ITEM	NOTES
Target:	Hong Kong Civil Referendum Website
Date:	March 23, 2012
Source:	Reuters HK, "Hackers 'disable' Hong Kong Civil Referendum Website," *Guardian*, March 23, 2012, available at http://www.guardian.co.uk/world/2012/mar/23/hackers-hong-kong-civil-referendum
Motivation:	Unknown
Type of attack:	DDoS (suspected)
Any other groups claiming responsibility:	No
Damage caused:	Website disabled and servers "crippled"
Additional important information:	Website offered a mock civil referendum, launched to see how people would vote if given a choice. Completely non-binding and arguably not influential.

Unknown—GreatFire

ITEM	NOTES
Target:	GreatFire, a Chinese activist group that monitors and challenges Internet censorship in China.
Date:	March 19, 2015
Source:	A. Elise, A., "China Hacktivists GreatFire Hit with DDoS Attack Costing Up to $30,000 Per Day," *International Business Times*, March 21, 2015, available at http://www.ibtimes.com/china-hacktivists-greatfire-hit-ddos-attack-costing-30000-day-1854692.
Motivation:	Speculated to be in retaliation over an article in the *Wall Street Journal* describing escalating tension between free-speech activists and Internet censors, and outlining the effectiveness of GreatFire in delivering uncensored content into China
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	GreatFire.org went off-line and the group had to upgrade to faster servers to manage the request load (the site offers censorship-defeating Internet tools). The growing data requests costs up to $30,000 per day.
Additional important information:	N/A

ISIS hacktivists—China's Tsinghua University

ITEM	NOTES
Target:	Tsinghua University
Date:	January 18, 2016
Source:	W. Ashford, "Chinese university targeted by Islamic State hacktivist," *Computer Weekly*, January 18, 2016, available at http://www.computerweekly.com/news/4500271103/Chinese-university-targeted-by-Islamic-State-hacktivist
Motivation:	Recruit students to join the Islamic State (ISIS)
Type of attack:	Unknown
Any other groups claiming responsibility:	No

Damage caused:	University website pages were replaced with images of masked militants beneath the ISIS flag
Additional important information:	China was declared one of eighteen enemy states by ISIS in 2015; the Chinese government has blamed ISIS-affiliated militants for a series of armed attacks in the country's Xinjiang region.

Unknown—Japanese government

ITEM	NOTES
Target:	Japanese government
Date:	January 25, 2001
Source:	ABC News, "Japanese Web Sites Hacked," January 25, 2001, available at http://abcnews.go.com/Technology/story?id=99306&page=1 (last accessed November 14, 2011)
Motivation:	To criticize the Japanese government's refusal to acknowledge the 1937 Nanjing Massacre in China
Type of attack:	Unauthorized access, modification of data, defacement
Any other groups claiming responsibility:	No
Damage caused:	Website defaced for an unspecified period. The Japan Science and Technology Agency's home page redirected to an adult website.
Additional important information:	First-ever hacking of the Japanese government computer system. A posted message read: "The Chinese people must speak up to protest the Japanese government for refusing to acknowledge the historical misdeed of the 1937 Nanjing Massacre."

Unknown—Japanese websites

ITEM	NOTES
Target:	Japanese government websites (including the Defence and the Internal Affairs and Communications Ministries) as well as the Supreme Court and Tokyo Institute of Technology. The websites of banks, utilities, and other private companies were also hit.
Date:	September 21, 2012

Source:	P. Muncaster, "Chinese hacktivists launch cyber attack on Japan," *The Register*, September 21, 2012, available at http://www.theregister.co.uk/2012/09/21/japan_china_attack_sites_senkaku/
Motivation:	China-Japan dispute over the Diaoyu/Senkaku islands. To deface websites with pictures of the Chinese flag.
Type of attack:	DDoS and vandalism
Any other groups claiming responsibility:	No
Damage caused:	Government websites were off-line for a number of hours. The Tokyo Institute of Technology site was defaced and the names and telephone numbers of over 1,000 staff members were leaked.
Additional important information:	Three hundred Japanese websites were short-listed for attack on a message board of the Chinese hacktivist group Honker Union, while around 4,000 individuals had posted messages about planned attacks on Chinese chat site YY Chat.

Alexploiter

ITEM	NOTES
Target:	Yemen customs
Date:	May 8, 2011
Source:	M. Kumar, "Customs Authority of Yemen Hacked for Protests against Government," *Hacker News*, August 5, 2011, available at http://thehackernews.com/2011/08/customs-authority-of-yemen-hacked-for.html
Motivation:	Protesting Yemeni government
Type of attack:	Unauthorized access, modification of data, defacement
Any other groups claiming responsibility:	No
Damage caused:	Customs website defaced for an unspecified period
Additional important information:	N/A

Kaotik Team

ITEM	NOTES
Target:	Indonesian government
Date:	August 1, 1998
Source:	C. Nuttall, "Chinese protesters attack Indonesia through Net," *BBC News*, August 19, 1998, available at http://connections-qj.org/article/internet-china-civilian-and-military-uses
Motivation:	To protest government oppression and occupation of East Timor
Type of attack:	Unauthorized access, modification of data, and defacement
Any other groups claiming responsibility:	No
Damage caused:	Forty-five Indonesian government sites reportedly defaced for an unspecified period. The home page of a site at www.bkkbn.go.id was replaced with a message saying "Warning from Chinese…This page is hacked for your national day. Please keep this page for 48 hours and punish the murderers in May immediately."
Additional important information:	N/A

China (suspected)—Vietnam

ITEM	NOTES
Target:	Vietnamese government
Date:	Early June 2010
Source:	BBC News, "Vietname and China Hackers Escalate Spratley Island Row" June 9, 2011 available at https://www.bbc.com/news/world-asia-pacific-13707921
Motivation:	Response to Spratly Islands dispute between China and Vietnam
Type of attack:	Website defacement
Any other groups claiming responsibility:	Attacked websites did not have high security. Could have been anyone with an IP address from China, or one redirected to China

Damage caused:	Two hundred Vietnamese websites hacked, including the Ministry of Agriculture and Rural Development. Hackers changed the attacked sites' homepage interface and left messages in Chinese or English, together with the images of the Chinese flag, according to BBC, adding that the attack methods were not sophisticated and seemed spontaneous.
Additional important information:	Seems like a crude hacking attempt from independent/rogue hackers rather than the Chinese state. Chinese-state hacks do not typically feature the basic hacking/defacing features seen in this case. Demonstrates the use of hacking as a precursory method to actual physical conflict between nations. Perhaps cybercrime is used to fight virtual wars before the need for physical conflict.

Gator League

ITEM	NOTES
Target:	Democratic People's Republic of Korea (North Korea)
Date:	December 23, 2014
Source:	RT, "Eye for eye? N. Korea internet restored after 9.5hr blackout," December 23, 2014, available at http://rt.com/news/216887-north-korea-internet-blackout/. R. Satter and E. Sullivan, "North Korea outage a case study in online uncertainties," *The Sydney Morning Herald*, December 25, 2014, available at http://www.smh.com.au/digital-life/digital-life-news/north-korea-outage-a-case-study-in-online-uncertainties-20141224-12dltr.html.
Motivation:	Potentially a retaliation for the Sony attack; North Korea blamed the US government. However, hacktivist group Gator League claimed responsibility
Type of attack:	DDoS Attack
Any other groups claiming responsibility:	Lizard Squad
Damage caused:	A nearly ten-hour Internet-service outage in North Korea

Additional important information:	On Sunday, December 20, 2014, Gator League posted the tweet "#NorthKorea is about to be invaded by alligators…" The next day, Internet service in North Korea was down for almost ten hours. On December 24, Anonymous posted the tweet "#BREAKING: CONFIRMED: HACKING GROUP @GatorLeague TOOK NORTH KOREA OFF OF THE INTERNET DECEMBER 21st-22nd. #NorthKorea."

Joint attack by 3xplr3_./split0 & N3roB]—(Bangladesh)

ITEM	NOTES
Target:	Subordinate courts of Bangladesh
Date:	November 2011
Source:	Hackers Media, "Subordinate Court of Bangladesh Hacked," previously available at http://www.hackersmedia.com/2011/11/subordinate-courts-of-bangladesh-hacked.html
Motivation:	To inform government websites of their vulnerability
Type of attack:	Unauthorized Access Deface
Any other groups claiming responsibility:	Unknown
Damage caused:	Website defaced
Additional important information:	N/A

3xp1r3 Cyber Army

ITEM	NOTES
Target:	Bangladesh Supreme Court website
Date:	November 10, 2011
Source:	M. Kumar, "Bangladesh Supreme Court website hacked," *Hacker News*, November 11, 2011, available at http://thehackernews.com/2011/11/bangladesh-supreme-court-website-hacked.html (last accessed November 12, 2011)
Motivation:	Apparently, to make website administrators aware of insecure site
Type of attack:	Unauthorized access and defacement

Any other groups claiming responsibility:	No
Damage caused:	Website defaced for unspecified period. No data leaked or deleted.
Additional important information:	N/A

TeaMp0isoN

ITEM	NOTES
Target:	Foreign governments, and also included the armynet.mod.uk and aph.gov.au sites
Date:	November 7, 2011
Source:	M. Kumar, "International Foreign Government E-Mails Hacked by TeaMp0isoN," *Hacker News*, November 7, 2011, available at http://thehackernews.com/2011/11/international-foreign-government-e.html
Motivation:	Generic dislike of government
Type of attack:	Unauthorized access and release of data
Any other groups claiming responsibility:	No
Damage caused:	Released personal information/email username/passwords of over 200 government officials
Additional important information:	N/A

The UnderTakers—AmEn, Swan, Bondbey, DanqeoN

ITEM	NOTES
Target:	Sony Music Brazil
Date:	June 4, 2011
Source:	M. Kumar, "Sony Music Brazil Gets Defaced!," *Hacker News*, June 5, 2011, available at http://thehackernews.com/2011/06/sony-music-brazil-gets-defaced.html (last accessed June 6, 2011)
Motivation:	Unknown—defacement alludes to an opposition to war

Type of attack:	SQL injection, unauthorized access, defacement
Any other groups claiming responsibility:	No
Damage caused:	Website down/defaced for over twelve hours
Additional important information:	Group unaffiliated with LulzSec. Unknown whether affiliated with other Brazilian hackers.

3xp1r3 Cyber Army (Bangladesh)

ITEM	NOTES
Target:	Indian websites
Date:	February 2012
Source:	"H4Ck3D By 3xp1r3 Cyber Army," Pastebin (February 12, 2012), available at http://pastebin.com/GRAmd7qq
Motivation:	Protesting the brutal treatment of Bangladeshi at the Indian borders.
Type of attack:	Website defaced
Any other groups claiming responsibility:	No
Damage caused:	Unknown
Additional important information:	Seven hundred Indian and Indian-linked websites attacked (see http://pastebin.com/GRAmd7qq)

Milw0rm

ITEM	NOTES
Target:	India's Bhabha Atomic Research Centre
Date:	May 1998
Source:	A. Penenberg, "Hacking Bhabha," *Forbes*, November 16, 1998, available at http://www.forbes.com/1998/11/16/feat.html (last accessed November 11, 2011)
Motivation:	To protest nuclear tests
Type of attack:	Unauthorized access, modification of data, data theft, data leaks
Any other groups claiming responsibility:	T3k-9—child

Damage caused:	Unspecified. Facility's servers were reportedly breached.
Additional important information:	Milw0rm is now defunct

NaijaCyberHacktivists

ITEM	NOTES
Target:	Niger Delta Development Commission's website
Date:	May 26, 2011 (estimate)
Source:	N. Jidenma, "Naija Cyber Hactivists Hack EFCC website to protest proposed internet censor in Nigeria," *Next Web*, September 28, 2011, available at http://thenextweb.com/africa/2011/05/26/nigerian-government-agency-website-hacked-by-cyberhacktivists/
Motivation:	Displeased with presidential inauguration budget of N$1 billion
Type of attack:	Unauthorized access, modification of data, and defacement
Any other groups claiming responsibility:	No
Damage caused:	Website defaced for an unspecified period
Additional important information:	N/A

Colombian government hacks

ITEM	NOTES
Target:	Colombian Ministry of Education, Colombian Senate, Colombian president, and government webpages. National communication system and other state infrastructure also targeted
Date:	2011
Source:	J. Wyss, "Political hackers are one of Latin America's newest headaches," *Miami Herald*, November 3 2011, available at http://www.miamiherald.com/2011/10/31/2481360/political-hackers-are-one-of-latin.html
Motivation:	Anti-government protesting
Type of attack:	Website hack

Any other groups claiming responsibility:	Reportedly affiliated with Anonymous
Damage caused:	Website defacing
Additional important information:	There were 480 hacks of Colombian Government websites in 2011, up from 250 in 2010. Colombian police officers' contact information published.

Ecuadorian government hacks

ITEM	NOTES
Target:	Ecuadorian government websites
Date:	2011
Source:	J. Wyss, "Political hackers are one of Latin America's newest headaches," *Miami Herald*, November 3, 2011, available at http://www.miamiherald.com/2011/10/31/2481360/political-hackers-are-one-of-latin.html
Motivation:	Anti-government protest
Type of attack:	Website hack
Any other groups claiming responsibility:	Reportedly affiliated with Anonymous
Damage caused:	Government websites defaced
Additional important information:	Two hundred and thirty attacks in 2011.

Latin Hack Team—Ecuador presidential website

ITEM	NOTES
Target:	Rafael Correa, Ecuador government
Date:	June 20, 2011
Source:	ElUniverso, "Website of the Presidency of Ecuador suffered cyber attacks," June 20, 2011, available at http://www.eluniverso.com/2011/06/20/1/1355/pagina-internet-presidencia-ecuatoriana-sufrio-ataque-informatico.html?p=1354&m=638 (last accessed June 21, 2011)
Motivation:	To protest alleged political corruption
Type of attack:	DDoS

Any other groups claiming responsibility:	Possibly Anonymous
Damage caused:	Presidential website out of commission for over two hours, elciudadano.com (government e-newspaper) down for an hour.
Additional important information:	Conflicting information on the group responsible. Some report that the so-called Latin Hack Team is a part of Anonymous.

N33—Venezuelan Pro-Government Hacks

ITEM	NOTES
Target:	Journalists, artists, opposition politicians
Date:	July 2011
Source:	J. Wyss, "Political hackers are one of Latin America's newest headaches," *Miami Herald*, November 3, 2011, available at http://www.miamiherald.com/2011/10/31/2481360/political-hackers-are-one-of-latin.html
Motivation:	Pro-government protest
Type of attack:	Twitter hacking
Any other groups claiming responsibility:	N33
Damage caused:	Twitter accounts hacked
Additional important information:	"N33's calling card is the image of a red beret — one of President Chávez's symbols." This and targeted hacking alludes to a pro-Chavez stance.

DonR4ul

ITEM	NOTES
Target:	Brazilian presidency blog
Date:	October 13, 2011
Source:	Xinhua, "Brazilian presidency's blog hacked in protest of corruption," October 14, 2011, *China Daily*, previously available at http://www.chinadaily.com.cn/xinhua/2011-10-14/content_4060557.html
Motivation:	Corruption in government departments and high fuel prices

Type of attack:	Unauthorized access, modification of data, and website defaced
Any other groups claiming responsibility:	No groups. Alleged to be the work of one hacker, "@DonR4UL."
Damage caused:	Defaced blog website for a number of hours.
Additional important information:	N/A

Raise Your Voice (Lebanese Hacktivists)

ITEM	NOTES
Target:	Lebanese government websites, Lebanese Energy and Water Department, MTV Lebanon
Date:	April 17, 2012
Source:	J, Karia, "Lebanese Hacktivists Take Down 15 Government Websites," *Tech Week Europe*, available at http://www.techweekeurope.co.uk/news/lebanese-hacktivists-15-government-websites-73313
Motivation:	Social protest—living conditions
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	Up to fifteen government websites taken off-line
Additional important information:	Social protest of living standards and conditions. Draws parallels to Tel Aviv's tent-city protests of 2011. Interesting that Lebanese youth adopt hacktivism to promote daily living concerns.

Khosrow Zare Farid—Central Bank of Iran

ITEM	NOTES
Target:	Central Bank of Iran, Iranian banking customers
Date:	April 2011 (reported April 19, 2012)
Source:	J. Kahria, "Hacker exposes Three Million Iranian Bank Account Details," *Tech Week Europe*, available at http://www.techweekeurope.co.uk/news/hacker-three-million-iranian-bank-accounts-73161

Motivation:	To increase awareness about data security in Iran, provoke a reaction from Iranian banks
Type of attack:	Accessed and published data on three million credit-card details obtained from more than twenty Iranian banks.
Any other groups claiming responsibility:	No
Damage caused:	Data from three million customers' accounts compromised
Additional important information:	Khosrow Zare Farid, identified by Kabir News, was a manager at a payments-services company that had several national banks as clients. "Around one year ago I found a critical bug in the system," said Zare Farid, according to Kabir News. "Then I wrote and sent a formal report to all the CEO of banks in Iran but none of them replied to me." Zare Farid then published a thousand, and later, three million, card details on his blog.

Cyber Warriors Team (Iran)—NASA hack

ITEM	NOTES
Target:	National Aeronautics and Space Administration (NASA)
Date:	May 16, 2012
Source:	M. Liebowitz, "Iranian 'Cyber Warriors Team' takes credit for NASA hack," *NBC News*, May 22, 2012, available at http://www.nbcnews.com/id/47522497/ns/technology_and_sciencesecurity/t/iranian-cyber-warriors-team-takes-credit-nasa-hack/#.XADd5y1L1PM
Motivation:	Geopolitical conflict
Type of attack:	SSL vulnerability exploited
Any other groups claiming responsibility:	No
Damage caused:	Personal information of thousands of NASA employees stolen
Additional important information:	"How to" video of hack posted online

CabinCr3w

ITEM	NOTES
Target:	Citigroup CEO, Vikram Pandit
Date:	October 18, 2011
Source:	A. Couts, "Hackers leak Citigroup CEO's personal data after Occupy Wall Street arrests," *Digital Trends*, August 18, 2011, available at http://www.digitaltrends.com/computing/hackers-leak-citigroup-ceos-personal-data-after-occupy-wall-street-arrests/
Motivation:	Apparently in response to arrests of protesters at a Citibank branch
Type of attack:	Unauthorized access and release of personal information
Any other groups claiming responsibility:	No
Damage caused:	Mobile and office phone numbers, an email address, two home addresses, legal and financial information, and information about Pandit's family posted online
Additional important information:	N/A

realloc()

ITEM	NOTES
Target:	The SCO group website (http://www.sco.com)
Date:	November 29, 2004
Source:	R. Millman, "SCO hit by hacker protest," *SC Magazine*, November 29, 2004, available at http://www.scmagazineus.com/sco-hit-by-hacker-protest/article/31510/
Motivation:	"Apparent protest over the ongoing legal proceedings the company is waging against Linux"
Type of attack:	Unauthorized access, modification of data, defacement
Any other groups claiming responsibility:	No
Damage caused:	Website defaced for unspecified period
Additional important information:	N/A

Herbless—HSBC

ITEM	NOTES
Target:	HSBC UK, Greek and Spanish websites, and British Arab Commercial Bank
Date:	September 20, 2000
Source:	J. Ticehurst, "HSBC internet sites hacked," *V3*, September 20, 2000, available at http://www.v3.co.uk/v3-uk/news/2007500/hsbc-internet-sites-hacked
Motivation:	Support to fuel protests in the United Kingdom
Type of attack:	Unauthorized access and potentially SQL injection
Any other groups claiming responsibility:	No
Damage caused:	UK site and three international sites were unavailable for an unspecified period
Additional important information:	Hacker claimed that personal information was neither accessed nor sought

Comment Group—Brian Milburn

ITEM	NOTES
Target:	Solid Oak Software Inc.—Milburn's family-owned firm in California
Date:	June 24, 2009–early 2012 (months after a February 2012 settlement)
Source:	M. Riley,"China Mafia-Style Attack Drives California Firm to Brink," *Bloomberg*, November 28, 2012, available at http://www.bloomberg.com/news/2012-11-27/china-mafia-style-hack-attack-drives-california-firm-to-brink.html. P. Muncaster, "US software firm hacked for years after suing China," *The Register*, November 29, 2012, available at https://www.theregister.co.uk/2012/11/29/solid_oak_china_hacked_three_years/.
Motivation:	Reaction to Milburn's accusation that China appropriated his company's parental filtering software, CYBERsitter, for an Internet-censoring project.

Type of attack:	Spear phishing. The malware had downloaded software that burrowed into the company's Microsoft operating system, automatically uploading more tools the hackers could use to control the network remotely.
Any other groups claiming responsibility:	No
Damage caused:	Assailed Solid Oak's computer systems; repeatedly shut down web and e-mail servers; spied on an employee with her webcam; gained access to sensitive files in a battle that caused company revenues to collapse; and sabotaged online sales by causing timeouts during payment.
Additional important information:	Milburn told Bloomberg, "If they [the Chinese hackers] could just put the company out of business, the lawsuit goes away." A forensic analysis of the malware by Joe Stewart, a threat expert at Atlanta-based Dell SecureWorks, identified the intruders who rifled Solid Oak's networks as a team of Shanghai-based hackers involved in a string of sensitive national-security-related breaches going back years. Commercial hacker hunters—who refer to the team as the Comment Group for the hidden program code they use known as "comments"—tie it to a multitude of victims that include the president of the European Union Council, major defence contractors, and even Barack Obama's 2008 presidential campaign. According to leaked classified cables, the group has been linked to the People's Liberation Army and China's military. Milburn settled a $2.2 billion lawsuit against the Chinese government and a string of computer companies.

Charles Tendell, ethical hacker

ITEM	NOTES
Target:	Baby monitors
Date:	January 28, 2015
Source:	J. Allen, "Ethical hacker points out security concerns with using home baby monitors," *7News Denver*, January 28, 2015, available at http://www.thedenverchannel.com/news/local-news/ethical-hacker-points-out-security-concerns-with-using-home-baby-monitors01282015

Motivation:	Security awareness
Type of attack:	No attack—a cyber-security expert based out of Monument, Colorado, showed a news reporter how easy it is to hack into thousands of baby-monitor video feeds.
Any other groups claiming responsibility:	N/A
Damage caused:	N/A
Additional important information:	N/A

Laxman Muthiyah, ethical hacker

ITEM	NOTES
Target:	Facebook
Date:	February 10, 2015
Source:	M. Desjardin, "How a White Hat Hacker Saved Your Facebook Photos," *Reviewed*, February 19, 2015, available at https://www.reviewed.com/cameras/news/how-a-hacker-saved-your-facebook-photos. L. Muthiyah, "Deleting Any Album—How I Hacked Your Facebook Photos," *Zero Hack*, November 8, 2015, available at https://thezerohack.com/how-i-hacked-your-facebook-photos#articlescroll.
Motivation:	Laxman Muthiyah discovered a means for anyone with some hacking knowledge to delete people's photo albums from Facebook
Type of attack:	This was not an attack; Muthiyah notified Facebook of the security risk and was awarded a bounty of $12,500 by the company
Any other groups claiming responsibility:	N/A
Damage caused:	N/A

Additional important information:	Muthiyah exploited vulnerabilities in Facebook's Graph API, which would allow a hacker to use access tokens to delete entire photo albums of other users. The access tokens that would enable this were available through the Facebook application for Android devices. The hacking process would involve each hacker generating a basic script to generate the sequential photo album IDs and test their vulnerability automatically. This security risk presented a real risk that could have been easily executed.

Unknown—Susan G. Komen Foundation for the Cure

ITEM	NOTES
Target:	Susan G. Komen Foundation for the Cure
Date:	February 2, 2012
Source:	A. Abad-Santos, "Susan G. Komen Foundation was Hacked Last Night," *Atlantic Wire*, February 2, 2012, available at http://www.theatlanticwire.com/national/2012/02/susan-g-komen-foundation-website-was-hacked-last-night/48192/
Motivation:	To protest the foundation's decision to pull funding from Planned Parenthood
Type of attack:	Unauthorized access and modification of data
Any other groups claiming responsibility:	No
Damage caused:	Website defaced for a period of time
Additional important information:	N/A

N33—Twitter

ITEM	NOTES
Target:	Hugo Chavez opponents
Date:	September 1, 2011

Source:	F. Sanchez, "Hackers hijack Twitter accounts of Chavez critics," *NBC News*, September 27, 2011, available at http://www.nbcnews.com/id/44689342/ns/technology_and_sciencesecurity/t/hackers-hijack-twitter-accounts-chavez-critics/
Motivation:	Political opposition, "improper use of Twitter"
Type of attack:	Phishing, unauthorized access, modification of data.
Any other groups claiming responsibility:	No
Damage caused:	Hacked the Twitter accounts of several political opponents, reputational damage, and release of personal information/communications/photos
Additional important information:	N/A

Électricité de France (EDF)

ITEM	NOTES
Target:	Greenpeace
Date:	2004–2006
Source:	E. Kovacs, "French Nuke Company Fined After Hacking Greenpeace," *Softpedia*, November 16, 2011, available at http://news.softpedia.com/news/French-Nuke-Company-Fined-After-Hacking-Greenpeace-234900.shtml. "EDF Hacking into Greenpeace" (November 10, 2011), available at http://www.youtube.com/watch?v=-70sjmTJlsQ.
Motivation:	To stop an operation against one of their plants
Type of attack:	Unauthorized access and data theft
Any other groups claiming responsibility:	No
Damage caused:	Fourteen hundred documents stolen from a campaign manager
Additional important information:	EDF was fined $2 million and some EDF staff received jail sentences. Illustrates how hacking can also be used in attempts to prevent non-technological activism.

Turkish hackers

ITEM	NOTES
Target:	Anonymous, AnonPlus
Date:	July 2011
Source:	J. Leyden, "Anonymous hackers hacked by Young Turks," *The Register*, July 22, 2011, available at http://www.theregister.co.uk/2011/07/22/anonplus_hacked/ (last accessed July 23, 2011). G. Cluley, "AnonPlus, Anonymous's social network, is hacked," *Naked Security*, July 22, 2011, available at https://nakedsecurity.sophos.com/2011/07/22/anonplus-anonymouss-social-network-is-hacked/.
Motivation:	Possibly to highlight Anonymous's poor password security, or perhaps in retaliation for Anonymous' Operation Turkey in June 2011
Type of attack:	Unauthorized access, modification of data, defacement
Any other groups claiming responsibility:	Unknown
Damage caused:	Anonymous members' Google+ account/group site hacked and defaced for an unspecified period of time.
Additional important information:	May have been accessed due to poor password security, which is what Anonymous criticizes others for.

Hacking for Girlies (HFG)—New York Times

ITEM	NOTES
Target:	*New York Times*
Date:	September 13, 1998
Source:	A. Penenberg, "Hacking Bhabha," *Forbes*, November 16, 1998, available at http://www.forbes.com/1998/11/16/feat.html (last accessed November 11, 2011). BBC News, "A-Z Hack Attack," February 11, 2000, available at http://news.bbc.co.uk/2/hi/uk_news/639248.stm.
Motivation:	"Reportedly a retaliation against a book written about super-hacker Kevin Mitnick by a Times reporter"—BBC News
Type of attack:	Website defacement

Any other groups claiming responsibility:	Unknown
Damage caused:	Pornographic images defaced the *New York Times* website
Additional important information:	N/A

Rafay Baloch

ITEM	NOTES
Target:	Pre 4.4 versions of Android
Date:	September 2, 2014
Source:	R. Baloch, "Android Browser Same Origin Policy Bypass < 4.4—CVE-2014-6041," Rafay Hacking Articles: http://www.rafayhackingarticles.net/2014/08/android-browser-same-origin-policy.html. Other media: D. Fisher, "Flaw in Android Browser Allows Same Origin Policy Bypass," *Threat Post*, September 15, 2014, available at http://threatpost.com/flaw-in-android-browser-allows-same-origina-policy-bypass/108265#comment-317786. D. Pauli, "THREE QUARTERS of Android mobiles open to web page spy bug," *The Register*, September 16, 2014, available at http://www.theregister.co.uk/2014/09/16/three_quarters_of_droid_phones_open_to_web_page_spy_bug/. BUILDER, "Metasploit: Major Android Bug is a Privacy Disaster (CVE-2014-6041)," *LinusTechTips*, September 15, 2014, available at http://linustechtips.com/main/topic/216087-metasploit-major-android-bug-is-a-privacy-disaster-cve-2014-6041/. P. Ducklin, "'Shocking' Android browser bug could be a "privacy disaster": here's how to fix it," *Naked Security*, September 16, 2014, available at http://nakedsecurity.sophos.com/2014/09/16/shocking-android-browser-bug-could-be-a-privacy-disaster-heres-how-to-fix-it/. T. Brewster, "Widespread Android Vulnerability 'A Privacy Disaster,' Claim Researchers," *Forbes*, September 16, 2014, available at http://www.forbes.com/sites/thomasbrewster/2014/09/16/widespread-android-vulnerability-a-privacy-disaster-claim-researchers/.

	E. Kovacs, "Dangerous 'Same Origin Policy' Bypass Flaw Found in Android Browser," *Security Week*, September 16, 2014, available at http://www.securityweek.com/dangerous-same-origin-policy-bypass-flaw-found-android-browser. L. Constantin, "Many Android devices vulnerable to session hijacking through the default browser," *Computer World*, September 16, 2014, available at http://www.computerworld.com/article/2684059/many-android-devices-vulnerable-to-session-hijacking-through-the-default-browser.html. NDTV Correspondent, "Android Browser Security Hole Affects Millions of Users, Says Expert," *Gadgets360*, September 16, 2014, available at http://gadgets.ndtv.com/mobiles/news/android-browser-security-hole-affects-millions-of-users-says-expert-592578. H. Bray, "Rapid7 of Boston warns of Android flaw," *Boston Globe*, September 15, 2014, available at http://www.bostonglobe.com/business/2014/09/15/rapid-boston-finds-android-flaw/JJ9iHJB6YTcs10a7O9TjpN/story.html. S. Malhotra, "Android security flaw affects millions of users," *digit*, September 16, 2014, available at http://www.digit.in/mobile-phones/android-security-flaw-affects-millions-of-users-23921.html. A. Friedman, "Android bug called a 'privacy disaster,'" *Phone Arena*, September 16, 2014, available at http://www.phonearena.com/news/New-Android-bug-called-a-privacy-disaster_id60750. D. Walker, "Android bug allowing SOP bypass a 'privacy disaster,' researcher warns," *SC Magazine*, September 16, 2014, available at http://www.scmagazine.com/android-bug-allowing-sop-bypass-a-privacy-disaster-researcher-warns/article/371917/. P. Bright, "Android Browser flaw a 'privacy disaster' for half of Android users," *Ars Technica*, September 17, 2014, available at http://arstechnica.com/security/2014/09/android-browser-flaw-a-privacy-disaster-for-half-of-android-users/. M. Kumar, "New Android Browser Vulnerability Is a 'Privacy Disaster' for 70% Of Android Users," *Hacker News*, September 16, 2014, available at http://thehackernews.com/2014/09/new-android-browser-vulnerability-is.html.

	A. Alizar, "AOSP Browser SOP," *Xakep*, September 18, 2014, available at http://xakep.ru/news/aosp-browser-sop/. S. Huang, "Same Origin Policy Bypass Vulnerability Has Wider Reach Than Thought on TREND MICRO," *Security Intelligence Blog* (September 29, 2014), available at http://blog.trendmicro.com/trendlabs-security-intelligence/same-origin-policy-bypass-vulnerability-has-wider-reach-than-thought/. Urdu Point, September 17, 2014, available at http://daily.urdupoint.com/livenews/2014-09-17/news-303641.html. *Daily Pakistan*, September 17, 2014, available at http://dailypakistan.com.pk/daily-bites/17-Sep-2014/144263. F. Baloch, "Online Security: Pakistani helps Google avoid privacy disaster," *The Express Tribune*, September 20, 2014, available at http://tribune.com.pk/story/764713/online-security-pakistani-helps-google-avoid-privacy-disaster/. DAWN, "Pakistani researcher reveals privacy flaw in Android browsers," *Dawn*, September 20, 2014, available at http://www.dawn.com/news/1133178/pakistani-researcher-reveals-privacy-flaw-in-android-browsers. *Express Tribune*, "Credit to our white-hats," *Express Tribune*, September 21, 2014, available at http://tribune.com.pk/story/764925/credit-to-our-white-hats/. S. Talal, "Pakistani Researcher Helps Google in Preventing a Massive Security Disaster, *ProPakistani*, 2014, available at http://propakistani.pk/2014/09/23/pakistani-researcher-helps-google-preventing-massive-security-disaster/. M. Hughes, "This Android Browser Bug Will Make You Upgrade To KitKat," *Make Use Of*, September 25, 2014, available at http://www.makeuseof.com/tag/this-android-browser-bug-will-make-you-upgrade-to-kitkat/.
Motivation:	Security-flaw exposure and to fix security flaw
Type of attack:	Baloch identified a security flaw in pre-4.4 versions of Android and wrote the code to fix it
Any other groups claiming responsibility:	N/A
Damage caused:	No damage. Baloch identified and developed a correction.

Additional important information:	The security flaw would have allowed hackers to gain access to personal data, including online banking details. As Android does not have vulnerability rewards program in place, Baloch was unrewarded for his efforts.

Jonathan Hall, ethical hacker

ITEM	NOTES
Target:	Yahoo and WinZip
Date:	September 24, 2014
Source:	S. Gallagher, "White hat claims Yahoo and WinZip hacked by 'shellshock' exploiters," *Ars Technica*, October 7, 2014, available at http://arstechnica.com/security/2014/10/white-hat-claims-yahoo-and-winzip-hacked-by-shellshock-exploiters/. F. Rashid, "Hackers Compromised Yahoo Servers Using Shellshock Bug," *Security Week*, October 6, 2014, available at http://www.securityweek.com/hackers-compromised-yahoo-servers-using-shellshock-bug.
Motivation:	Hall said that disclosure of the "bash vulnerability" made him curious to explore these security threats. He was motivated to make his findings public as he felt that companies like Yahoo were ignoring the problem, which he considered as negligent and almost criminal.
Type of attack:	Identification of security threat, the "shellshock vulnerability"
Any other groups claiming responsibility:	No
Damage caused:	This vulnerability would allow a hacker to use the vulnerable scripts to send commands to local operating systems, and possibly gain remote access and control of the server. It had the potential to affect every consumer.
Additional important information:	N/A

Microsoft and Symantec—Botnet

ITEM	NOTES
Target:	Internet users
Date:	February 7, 2013
Source:	C. Arthur, "Microsoft and Symantec Take Out Botnet Responsible for More Than $1m of Fraud," *Guardian*, February 7, 2013, available at http://www.guardian.co.uk/technology/2013/feb/07/microsoft-symantec-botnet-fraud-pcs
Motivation:	Monetary fraud counterattack
Type of attack:	The criminals behind the scheme took advantage of search advert pricing, which could be as small as four-hundredths of a cent, meaning that they had to build up a large botnet that remained undetected by infected users and hijack huge amounts of traffic in order to profit. The process by which clicks were rerouted via "traffic brokers" to paying advertisers was so complex, said Symantec, that in some cases it went through ten hops before reaching the actual advertiser.
Any other groups claiming responsibility:	No
Damage caused:	N/A
Additional important information:	Microsoft and Symantec disabled a two-year-old network of remotely controlled PCs, a botnet, that was responsible for at least $1 million dollars in "click fraud" every year—and possibly substantially more—and which may have controlled as many 1.8 million PCs. The ringleaders are believed to be spread globally, in Britain, Russia, Romania, the United States, and Australia. They used false names and stolen credit-card details to register a string of domains and hire server space in a number of locations. They have never been formally identified or arrested. The Bamital botnet, set up in late 2009, took over PCs and would silently click on specific adverts in search results—hijacking an average of three million clicks per day, and exposed the PCs' owners to the risk of more infection as they were taken to other sites that could carry further malware.

Page left blank intentionally