Significant Cyber Incidents Since 2006

This list is a work in progress that we update as new incidents come to light. If you have suggestions for additions, send them to techpolicy@csis.org. Significance is in the eye of the beholder, but we focus on successful attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.

1. **May 2006.** The Department of State's networks were hacked, and unknown foreign intruders downloaded terabytes of information. If Chinese or Russian spies backed a truck up to the State Department, smashed the glass doors, tied up the guards and spend the night carting off file cabinets it would be an act of war, but when it happens in cyberspace we barely notice.

2. **August 2006.** A senior Air Force Officer stated publicly that, "China has downloaded 10 to 20 terabytes of data from the NIPRNet (the unclassified military network)."

3. **November 2006.** Hackers attempted to penetrate U.S. military War College networks, resulting in a two week shutdown at one institution while infected machines are restored.

4. **December 2006.** NASA was forced to block emails with attachments before shuttle launches out of fear they would be hacked. Business Week reported that the plans for the latest U.S. space launch vehicles were obtained by unknown foreign intruders.

5. **2006.** Chinese hackers were thought to be responsible for shutting down the House of Commons computer system.

6. **April 2007.** The Department of Commerce had to take the Bureau of Industrial Security's networks offline for several months because its networks were hacked by unknown foreign intruders. This Commerce Bureau reviews confidential information on high tech exports.

7. **May 2007.** The National Defense University had to take its email systems offline because of hacks by unknown foreign intruders that left spyware on the system.

8. **May 2007.** Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, most likely at the behest of the Russian government. Some government online services were temporarily disrupted and online banking was halted. These were more like cyber riots than crippling attacks, and the Estonians responded very well; however, they created a wave of fear in cyber dependent countries like the U.S.

9. **June 2007.** The Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit DOD networks.

10. **August 2007.** The British Security Service, the French Prime Minister's Office and the Office of German Chancellor Angela Merkel all complained to China about intrusion on their government networks. Merkel even raised the matter with China's President.

11. **September 2007.** Israel disrupted Syrian air defense networks (with some collateral Damage to its own domestic networks) during the bombing of an alleged Syrian nuclear facility.

12. **September 2007.** Francis Delon, Secretary-General of National Defence in France, stated that information systems in France had been infiltrated by groups from China.

13. **September 2007.** Contractors employed by DHS and DOD had their networks hacked as backdoors into agency systems.

14. **September 2007.** British authorities reported that hackers, believed to have come from China's People's Liberation Army, penetrated the network of the Foreign Office and other key departments.

15. **October 2007.** China's Ministry of State Security said that foreign hackers, 42% from Taiwan and 25% from United Sates, had been stealing information from Chinese key areas. In 2006, when China's China Aerospace Science & Industry Corporation (CASIC) Intranet Network was surveyed, spywares were found in the computers of classified departments and corporate leaders.

16. **October 2007.** More than a thousand staffers at Oak Ridge National Labs received an email with an attachment that, when opened, provides unknown outsiders with access to the Lab's databases.

17. **November 2007.** Jonathan Evans, the head of Britain's Security Service (MI5), warned 300 business firms of the increased online threat from Russian and Chinese state organizations saying, "A number of countries continue to devote considerable time and energy trying to steal our sensitive technology on civilian and military projects, and trying to obtain political and economic intelligence at our expense. They…increasingly deploy sophisticated technical attacks, using the internet to penetrate computer networks."

18. **January 2008.** A CIA official said the agency knew of four incidents overseas where hackers were able to disrupt, or threaten to disrupt, the power supply for four foreign cities.

19. **March 2008.** South Korean Officials claimed that China had attempted to hack into Korean Embassy and Korea military networks.

20. **March 2008.** U.S. officials reported that American, European, and Japanese companies were experiencing significant losses of intellectual property and business information to

criminal and industrial espionage in cyberspace. However, details cannot be provided in an unclassified setting.

21. **April – October 2008.** A State Department cable made public by WikiLeaks reported that hackers successfully stole "50 megabytes of email messages and attached documents, as well as a complete list of usernames and passwords from an unspecified (U.S. government) agency." The cable said that at least some of the attacks originated from a Shanghai-based hacker group linked to the People's Liberation Army's Third Department.

22. **May 2008.** The Times of India reported that an Indian official accused China of hacking into government computers. The official stated that the core of the Chinese assault is the scanning and mapping of India's official networks to gain access to content in order to plan how to disable or disrupt networks during a conflict.

23. **June 2008**. The networks of several Congressional offices were hacked by unknown foreign intruders. Some infiltrations involved offices with an interest in human rights in Tibet.

24. **Summer 2008.** The databases of both Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders.

25. **Summer 2008.** Marathon Oil, ExxonMobil, and ConocoPhillips were hacked and lost data detailing the quantity, value, and location of oil discoveries around the world. One company put the losses in the millions.

26. **August 2008.** Computer networks in Georgia were hacked by unknown foreign intruders, most likely at the behest of the Russian government. Much press attention was given to annoying graffiti on Georgian government websites. There was little or no disruption of services but the hacks did put political pressure on the Georgian government and were coordinated with Russian military actions.

27. **October 2008.** Police discovered a highly sophisticated supply chain attack where credit card readers made in China and used in UK supermarkets had a wireless device inserted in them. The device copies a credit card when it is inserted, stores the data, and transfers the data it has collected once a day via WiFi connection to Lahore, Pakistan. Estimated loss is $50 million or more. The device could be instructed to collect only certain kinds of cards (such as gold cards), or to go dormant to evade detection.

28. **November 2008.** Hackers breached networks at Royal Bank of Scotland's WorldPay, allowing them to clone 100 ATM cards and withdraw over $9 million dollars from machines in 49 cities.

29. **November 2008.** Classified networks at DOD and CENTCOM were hacked by unknown foreign intruders. Even worse, it took several days to dislodge the intruders and re-secure the networks.

30. **December 2008.** Retail giant TJX was hacked. The one hacker captured and convicted (Maksym Yastremskiy) is said to have made $11 million from the hack.

31. **December 2008.** Even tiny CSIS was hacked in December by unknown foreign intruders. They probably assumed that some CSIS staff would go into the new administration and may have thought it might be interesting to read their emails beforehand.

32. **2008.** Britain's MPs were warned about e-mails apparently sent by the European Parliament amid fears that they could be used by Chinese hackers to implant viruses.

33. **January 2009.** Hackers attacked Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government websites, was executed by at least 5,000,000 computers. Israeli officials believed the attack was carried out by a criminal organization from the former Soviet Union, and paid for by Hamas or Hezbollah.

34. **January 2009.** Indian Home Ministry officials warned that Pakistani hackers had placed malware on popular music download sites used by Indians in preparation for cyber attacks.

35. **February 2009.** FAA computer systems were hacked. Increased use by FAA of IP-bases' networks also increases the risk of the intentional disruption of commercial air traffic.

36. **February 2009.** 600 computers at India's Ministry of External Affairs were hacked.

37. **February 2009.** French naval aircraft planes were grounded after military databases were infected with the "confickr" virus. Naval officials suspected someone at the Navy had used an infected USB key.

38. **March 2009.** The German government warned that hackers were offering a free version of the new Microsoft operating system that installs Trojans.

39. **March 2009.** Canadian researchers found a computer espionage system that they believe China implanted on the government networks of 103 countries.

40. **March 2009.** Reports in the press say that the plans for Marine Corps 1, the new presidential helicopter, were found on a file-sharing network in Iran.

41. **April 2009.** Wall Street Journal articles laid out the increasing vulnerability of the U.S. power grid to cyber attack also highlighted was the intrusions into F-35 databases by unknown foreign intruders.

42. **April 2009.** Prime Minister Wen Jiabao announced that hacker from Taiwan accessed a Chinese State Council computer containing drafts of his report to the National Peoples Congress.

43. **April 2009.** Chinese hackers reportedly infiltrated South Korea's Finance Ministry via a virus attached to e-mails claiming to be from trusted individuals.

44. **May 2009.** In May 2009, Merrick Bank, a leading issuer of credit cards, claimed it lost $16 million after hackers compromised as many as 40 million credit card accounts.

45. **May 2009.** The Homeland Security Information Network (HSIN) was hacked by unknown intruders. The hackers gained access to the data by getting into the HSIN account of a federal employee or contractor. The bulk of the data obtained was federal, but some state information was also accessed

46. **June 2009.** The John Hopkins University's Applied Physics Laboratory, which does classified research for the Department of Defense and NASA, took its unclassified networks offline after they were penetrated.

47. **June 2009.** German Interior Minister Wolfgang Schaeuble noted, when presenting the Interior Ministry's 2008 security report, that China and Russia were increasing espionage efforts and Internet attacks on German companies.

48. **July 2009.** Cyberattacks against websites in the United States and South Korea, including a number of government websites, were launched by unknown hackers. South Korea accused North Korea of being behind the attacks The denial of service attacks did not severely disrupt services but lasted for a number of days and generated a great deal of media attention.

49. **August 2009.** Albert Gonzalez was indicted on charges that between 2006 and 2008, he and unidentified Russian or Ukrainian colleagues allegedly stole more than 130 million credit and debit cards by hacking into the computer systems of five major companies. This was the largest hacking and identity theft crime in U.S. history.

50. **August 2009.** Ehud Tenenbaum was convicted of stealing $10 million from U.S. banks. Tenenbaum was known for hacking into DOD computers in 1998, which resulted in a sentence of six months of community service from an Israeli court.

51. **November 2009.** Jean-Pascal van Ypersele, the vice-chairman of the United Nations' Intergovernmental Panel on Climate Change, ascribed the hacking and release of thousands of emails, from the University of East Anglia's Climatic Research Unit to Russia as part of a plot to undermine the Copenhagen climate talks.

52. **December 2009.** The Wall Street Journal reported that a major U.S. bank had been is hacked, losing tens of millions of dollars.

53. **December 2009.** Downlinks from U.S military UAV's were hacked by Iraqi insurgents using laptops and $24.99 file sharing software, allowing them to see what the UAV has viewed.

54. **January 2010.** The UK's MI5 Security Service warned that undercover intelligence officers from the People's Liberation Army and the Ministry of Public Security have approached UK businessmen at trade fairs and exhibitions with the offer of "gifts" - cameras and memory sticks - which contain malware that provides the Chinese with remote access to users' computers.

55. **January 2010.** Google announced that a sophisticated attack had penetrated its networks, along with the networks of more than 30 other US companies. The goal of the penetrations, which Google ascribed to China, was to collect technology, gain access to activist Gmail accounts and to Google's Gaea password management system.

56. **January 2010.** Global financial services firm Morgan Stanley experienced a "very sensitive" break-in to its network by the same China-based hackers who attacked Google Inc.'s computers in December 2009, according to leaked e-mails from a cyber-security company working for the bank.

57. **January 2010.** M. K. Narayanan, India's National Security Adviser, said his office and other government departments were attacked by China on December 15. The Prime Minister's office later denied that their computers had been hacked. Narayanan said this was not the first attempt to penetrate Indian government computers.

58. **January 2010.** A group named the "Iranian Cyber Army" disrupted service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message. Previously, the "Iranian Cyber Army" had hacked into Twitter in December and with a similar message.

59. **January 2010.** Intel disclosed that it has experienced a cyber attack at about the same time that Google, Adobe and other were attacked. The hackers exploited the vulnerabilities in Internet Explorer software that had been used in the other attacks as well. Intel said that there was no intellectual property or financial loss.

60. **March 2010.** NATO and the EU warned that the number of cyber attacks against their networks had increased significantly over the past 12 months, with Russia and China among the most active adversaries.

61. **March 2010.** Google announced that it had found malware targeted at Vietnamese computer users. Google said that the malware was not especially sophisticated and was used to spy on "potentially tens of thousands of users who downloaded Vietnamese keyboard language software" the malware also launched distributed denial of service attacks against blogs containing political dissent, specifically, opposition to bauxite mining efforts in Vietnam.

62. **March 2010.** Australian authorities said there were more than 200 attempts to hack into the networks of the legal defense team for Rio Tinto executives being tried in China, to gain inside information on the trial defense strategy.

63. **March 2010.** Unknown hackers post the real incomes of Latvian government officials after accessing their tax records, creating political turmoil.

64. **April 2010.** Chinese hackers reportedly broke into classified files at the Indian Defence Ministry and Indian embassies around the world, gaining access to Indian missile and armament systems.

65. **April 2010.** A Chinese telecommunications firm accidently transmitted erroneous routing information for roughly 37,000 networks, causing internet traffic to be misrouted through China. The incident lasted 20 minutes and exposed traffic from more than 8,000 U.S. networks, 8,500 Chinese networks, 1,100 Australian networks and 230 French networks.

66. **May 2010.** A leaked memo form the Canadian Security and Intelligence Service (CSIS) says that "Compromises of computer and combinations networks of the Government of Canada, Canadian universities, private companies and individual customer networks have increased substantially.... In addition to being virtually unattributable, these remotely operated attacks offer a productive, secure and low-risk means to conduct espionage."

67. **July 2010.** A Russian intelligence agent (allegedly named Alexey Karetnikov), was arrested and deported after working for nine months as a software tester at Microsoft.

68. **October 2010.** Stuxnet, a complex piece of malware designed to interfere with Siemens Industrial Control Systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program.

69. **October 2010.** The Wall Street Journal reported that hackers using "Zeus" malware, available in cybercrime black markets for about $1200, were able to steal over $12 million from five banks in the US and UK. Zeus uses links in emails to steal account information, which the hackers then use to transfer money into bank accounts they control. 100 "mules", or low end criminals, were arrested for opening bank accounts under false names into which the hackers transferred stolen money.

70. **October 2010.** Australia's Defence Signals Directorate reported a huge increase in cyberattacks on the military. Australia's Defence Minister, john Faulkner, revealed there had been 2400 "electronic security incidents" on Defence networks in 2009 and 5551 incidents between January and August 2010.

71. **December 2010.** British Foreign Minister William Hague reported attacks by a foreign power on the Foreign Ministry, a defence contractor and other "British interests" that evaded defenses by pretending to come from the White House.

72. **December 2010.** India's Central Bureau of Investigation (CBI) website (cbi.nic.in) was hacked and data erased. India blames Pakistani hackers. Sensitive CBI data, stored on computer not easily accessible from the Internet, was unaffected.

73. **January 2011.** Hackers penetrated the European Union's carbon trading market, which allows organizations to buy and sell their carbon emissions quotas, and steal more than $7 million in credits, forcing the market to shut down temporarily.

74. **January 2011.** Hacker extracted $6.7 million from South Africa's Postbank over the New Year's Holiday.

75. **January 2011.** The Canadian government reported a major cyber attack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the internet. Canadian sources attribute the attack to China.

76. **March 2011.** Hackers penetrated French government computer networks in search of sensitive information on upcoming G-20 meetings.

77. **March-April 2011.** Between March 2010 and April 2011, the FBI identified twenty incidents in which the online banking credentials of small-to-medium sized U.S. businesses were compromised and used to initiate wire transfers to Chinese economic and trade companies. As of April 2011, the total attempted fraud amounts to approximately $20 million; the actual victim losses are $11 million.

78. **March-April 2011.** Hackers used phishing techniques in attempt to obtain data that would compromise RSA's SecureID authentication technology. The data acquired was then used in an attempt to penetrate Lockheed Martin's networks.

79. **April 2011.** Google reported a phishing effort to compromise hundreds of Gmail passwords for accounts of prominent people, including senior U.S. officials. Google attributes the effort to China.

80. **April 2011.** Employees at Oak ridge National Laboratory received bogus emails with malware attachments. Two machines were infected and "a few megabytes" of data were extracted before the Lab was able to cut its internet connection. Oak Ridge was the target of an intrusion in 2007.

81. **May 2011.** Cybercriminals masquerading as member of the hacktivist group "Anonymous" penetrated the PlayStation network. Sony estimated that personal

information for more than 80 million users was compromised and that the cost of the breach at over $170 million.

82. June 2011. The IMF's networks were compromised reportedly by a foreign government using fraudulent emails with malware attachments, and a "large quantity of data, including documents and e-mails," are exfiltrated.

83. June 2011. Citibank reported that credit card data for 360,000 of its customers were exfiltrated using a relatively simple manipulation of URLs.

84. July 2011. In a speech unveiling the Department of Defense's cyber strategy, the Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the DOD were stolen.

85. July 2011. The German Bundespolizei (Federal Police) and the Bundeszollverwaltung (Federal Customs Service) discovered that servers used to locate serious criminals and terrorism suspects by gathering information from GPS systems in cars and mobile phones were penetrated (using a phishing attack)as early as 2010. Following the cyberattack, the relevant servers had to be temporarily shut down to prevent further data losses.

86. July 2011. South Korea said hackers from China had penetrated an internet portal and accessed phone numbers, e-mail addresses, names and other data for 35 million Koreans.

87. August 2011. According to sources in the Japanese government, Mitsubishi Heavy Industries and twenty other Japanese defense and high tech firms were the target of an effort to extract classified defense information. Japanese officials believed the exploits all originated from the same source. The intruder used email with a malicious attachment whose contents were the same as a legitimate message sent 10 hours earlier.

88. August 2011. Email and documents from 480 members of the Japanese Diet and lawmakers and their staff were compromised for a month after a phishing attack implanted a Trojan on members' computers and Diet servers. The hijacked machines communicated with a server in China and the attackers included Chinese characters in their code.

89. September 2011. Unknown attackers hacked a Dutch certificate authority, allowing them to issue more than 500 fraudulent certificates for major companies and government agencies. The certificates are used to verify that a website is genuine. By issuing a false certificate, an attacker can pretend to be a secure website, intercept e-mail, or install malicious software. This was the second hack of a certificate authority in 2011.

90. **September 2011.** Australia's Defense Signals Directorate says that defense networks are attacked more than 30 times a day, with the number of attacks increasing by more than 350 percent by 2009.

91. **September 2011.** A computer virus from an unknown source introduced "keylogger" malware onto ground control stations for US Air Force UAVs and, according to press reports, infected both classified and unclassified networks at Creech Air Force Base in Nevada. The US did not lose control of any drone nor does it appear that any data was exfiltrated, but the malware was persistent and took several attempts to remove.

92. **October 2011.** Networks of 48 companies in the chemical, defense and other industries were penetrated for at least six months by a hacker looking for intellectual property. Symantec attributes some of the attacks to computers in Hebei, China.

93. **November 2011.** Apple computers belonging to European Commission officials, including EC Vice President for the "Digital Agenda," were hacked at an Internet Governance Forum (IGF) meeting in Azerbaijan.

94. **November 2011.** Norway's National Security Agency (NSM) reports that at least 10 major Norwegian defense and energy companies were hacked. The attacks were specifically "tailored" for each company, using an email phishing scheme. NSM said that the attacks came when the companies, mainly in the oil and gas sectors, have been involved in large-scale contract negotiations. The hacking occurred over the course of 2011, with hackers gaining access to confidential documents, industrial data, usernames and passwords.

95. **December 2011.** U.S. Chamber of Commerce computer networks were completely penetrated for more than a year by hackers who, according to press reports, had ties to the People Liberation Army. The Hackers had access to access to everything in Chamber computers, including member company communications and industry positions on U.S. trade policy.

96. **March 2012.** NASA's Inspector General reported that 13 APT attacks successfully compromised NASA computers in 2011. In one attack, intruders stole 150 user credentials that could be used to gain unauthorized access to NASA systems. Another attack at the Joint Propulsion Laboratory involving China-based IP let the intruders gain full access to key JPL systems and sensitive user accounts.

97. **March 2012.** The BBC reported a "sophisticated cyber-attack" in an effort to disrupt the BBC Persian Language Service. The attack coincided with efforts to jam two BBC satellite feeds to Iran. The BBC's Director General blamed Iran for the incident.

98. **March 2012.** India's Minister for Communications and Information Technology revealed in a written reply to a Parliamentary question that 112 government websites had been compromised from December 2011 to February 2012. Most of the incidents involved website defacement and many of the hacks appeared to originate in Pakistan.

99. **March 2012.** The U.S. Department of Homeland Security issued amber alerts warning of a cyber intrusion campaign on U.S. gas pipelines, dating back to December 2011. Press reports indicated that Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) described the attack as a sophisticated spear phishing campaign emanating from a single source.

100. **April 2012.** Iran was forced to disconnect key oil facilities after a cyber attack against internal computer systems. The malware was found inside the control systems of Kharg Island – Iran's main oil exporting terminal. Equipment at Kharg Island and at other Iranian oil plants has been disconnected from the internet as a precaution. Iran reported that oil production was not affected, but the websites of the Iranian oil ministry and national oil company were forced offline and data about users of the sites was taken as a result of the attack.

101. **April 2012.** A hack of Japan's Ministry of Agriculture, Forestry and Fisheries resulted in more than 3,000 documents exfiltrated to a foreign destination, including 20 classified documents on negotiations on the Trans-Pacific Partnership (a broad free-trade agreement). According to press reports, the hackers searched Ministry computers for TPP documents, transferred all that were found to a single computer, and then compressed them to make them easier to send.

102. **May 2012.** UK officials told the press that there had been a small number of successful perpetrations of classified MOD networks.

103. **May 2012.** An espionage toolkit named "Flame" is discovered in computers in the Iranian Oil Ministry, as well as in other Middle Eastern countries, including Israel, Syria, and Sudan, and other nations around the world.

104. **May 2012.** Researchers at the University of Toronto report that versions of the installer for the proxy tool Simurgh, which anonymizes net use and is popular in countries such as Iran and Syria to circumvent government internet controls, also installs a keylogger Trojan which sends the user name, keystrokes, and program use to another site.

105. **June 2012.** A phishing campaign targets the U.S. aerospace industry experts attending the 2013 IEEE Aerospace Conference.

106. **June 2012.** A global fraud campaign using automated versions of SpyEye and Zeus Trojans targeted high-value personal and corporate accounts and bypassed two-factor authentication.

107. **June 2012**. The head of the UK Security Service stated that a London-listed company lost an estimated £800m ($1.2 billion) as a result of state cyber attacks.

108. **July 2012.** A Trojan nicknamed "Mahdi" found gathering data from approximately 800 critical infrastructure engineering firms, government agencies, financial houses, and

academia throughout the Middle East and beyond, predominantly in Israel and Iran. The virus contains Persian language strings.

109. **July 2012.** Indian naval officials confirmed that a virus had collected data from sensitive computer systems at the country's Eastern Naval Command headquarters and sent the data to Chinese IP addresses. The virus allegedly entered the Navy's network via infected USB drives, which were used to transfer data from standalone computers holding sensitive files to networked systems.

110. **July 2012.** The Director of the National Security Agency said that there had been a 17-fold increase in cyber incident at American infrastructure companies between 2009 and 2011.

111. **July 2012.** Regarded as the largest attack on Indian government networks, over 10,000 email addresses of top Indian government officials were hacked, including officials in the Prime Minister's Office, Defense, External Affairs, Home, and Finance ministries, as well as intelligence agencies. India blames the attack on state actors.

112. **August 2012.** Malware nicknamed "Gauss," infected 2,500 systems worldwide. Gauss appears to have been aimed at Lebanese banks, and contains code whose encryption has not yet been broken.

113. **August 2012.** A group called "Cutting Sword of Justice" linked to Iran claimed it has used the "Shamoon" virus to attack Aramco, a major Saudi oil supplier, deleting data on 30,000 computers and infecting (without causing damage) control systems. The attack also affected the Qatar company RasGas, a major LNG supplier. Other oil companies may have also been infected.

114. **September 2012.** Izz ad-Din al-Qassam, a hacker group linked to Iran, launched "Operation Ababil" targeting bank websites for sustained denial-of-service attacks. Targets include Bank of America, New York Stock Exchange, Chase Bank, Capital One, SunTrust, and Regions Bank.

115. **October 2012.** The Russian firm Kaspersky discovered a worldwide cyber-attack dubbed "Red October," that had been operating since at least 2007. Hackers gathered information through vulnerabilities in Microsoft's Word and Excel programs. The primary targets of the attack appear to be countries in Eastern Europe, the former USSR and Central Asia, although Western Europe and North America reported victims as well. The virus collected information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures, although the full extent of the damage is unknown.

116. **December 2012**. The U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported that two power plants in the U.S. suffered sophisticated malware infections using unprotected USB drives as an attack vector. In both cases, a

lack of basic security controls made it easier for the malicious code to reach critical networks.

117. **December 2012.** Al-Qaida websites were taken off line for two weeks. This follows a 2008 website disruption aimed at damaging recruiting and propaganda efforts by the group.

118. **December 2012.** The Council on Foreign Relations and Capstone Turbine Corporation were targeted by hackers who used a zero-day vulnerability in Microsoft's internet explorer web browser to compromise the computers of those who visited the websites. Both CFR and Capstone Turbine are believed to have been used as a 'watering hole' – a target of opportunity that is used access the real targets, presumably individuals known to frequent the sites. Capstone Turbine fits the profile of companies that are believed to be high-value targets for industrial espionage from firms based in China.

119. **January 2013**. Izz ad-Din al-Qassam claims responsibility for another series of distributed denial-of-service attacks against US Bank websites, as part of "Operation Ababil," phase two. Targets include: Ally Financial, BB&T, Capital One, Fifth Third Bank, HSBC, PNC, Wells Fargo, SunTrust, and Zions Bank. US officials speculate that the group is a front for a state-sponsored campaign attributed to Iran.