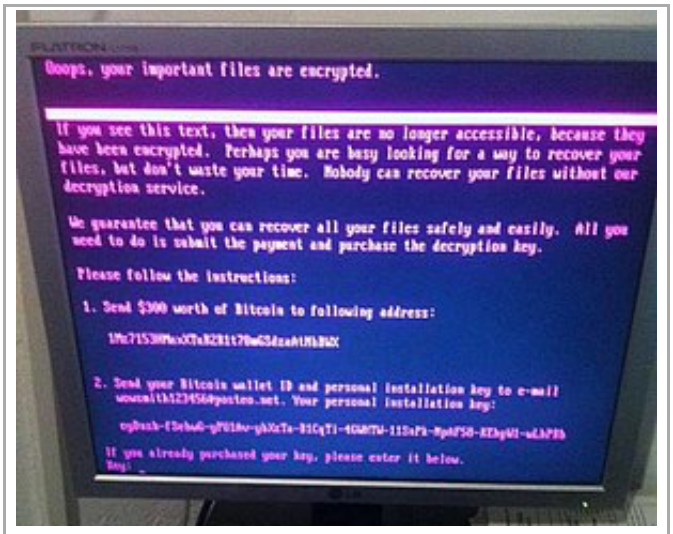
WIKIPEDIA

2017 cyberattacks on Ukraine

A series of powerful cyberattacks using the Petya malware began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms.[10] Similar infections were reported in France, Germany, Italy, Poland, Russia, United Kingdom, the United States and Australia.[11][3][12] ESET estimated on 28 June 2017 that 80% of all infections were in Ukraine, with Germany second hardest hit with about 9%.[2] On 28 June 2017, the Ukrainian government stated that the attack was halted.[13] On 30 June 2017, the Associated Press reported experts agreed that Petya was masquerading as ransomware, while it was actually designed to cause maximum damage, with Ukraine being the main target.[14]

2017 cyberattacks on Ukraine



Petya's ransom note displayed on a compromised system

Date	27–28 June 2017
Location	Ukraine[1] **Other locations**
Type	cyberattack
Cause	malware, ransomware, cyberterrorism
Outcome	affected several Ukrainian ministries, banks, metro systems and state-owned enterprises
Suspects	Russia (according to statements of Ukrainian authorities, American Michael N. Schmitt and the CIA.)[5][6][7][8][9]

Contents

Approach

Security experts believe the attack originated from an update of a Ukrainian tax accounting package called MeDoc (M.E.Doc), developed by Intellect Service.[2] MeDoc is widely used among tax accountants in Ukraine,[15] and the software was the main option for accounting for other Ukrainian businesses, according to Mikko Hyppönen, a security expert at F-Secure.[2] MeDoc had about 400,000 customers across Ukraine, representing about 90% of the country's domestic firms[8] and prior to the attack was installed on an estimated 1 million computers in Ukraine.[16]

MeDoc provides periodic updates to its program through an update server. On the day of the attack, 27 June 2017, an update for MeDoc was pushed out by the update server, following which the ransomware attack began to appear. British malware expert Marcus Hutchins claimed "It looks like the software's automatic update system was

compromised and used to download and run malware rather than updates for the software."[2] The company that produces MeDoc claimed they had no intentional involvement in the ransomware attack, as their computer offices were also affected, and they are cooperating with law enforcement to track down the origin.[17][15] Similar attack via MeDoc software was carried out on 18 May 2017 with a ransomware XData. Hundreds of accounting departments were affected in Ukraine.[18]

The cyberattack was based on a modified version of the Petya ransomware. Like the WannaCry ransomware attack in May 2017, Petya uses the EternalBlue exploit previously discovered in older versions of the Microsoft Windows operating system. When Petya is executed, it encrypts the Master File Table of the hard drive and forces the computer to restart. It then displays a message to the user, telling them their files are now encrypted and to send US$300 in bitcoin to one of three wallets to receive instructions to decrypt their computer. At the same time, the software exploits the Server Message Block protocol in Windows to infect local computers on the same network, and any remote computers it can find. Additionally, the NotPetya software was found to use a variant of Mimikatz, a proof-of-concept exploit found in 2011 that demonstrated that user passwords had been retained in computer memory within Windows, exploiting these passwords to help spread across networks.[19]

The EternalBlue exploit had been previously identified, and Microsoft issued patches in March 2017 to shut down the exploit for the latest versions of Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, and Windows Server 2016. However, the WannaCry attack progressed through many computer systems that still used older Windows operating systems or previous releases of the newer ones, which still had the exploit, or that users had not taken the steps to download the patches. Microsoft issued new patches for Windows XP and Windows Server 2003 as well as previous versions of the other operating systems the day after the WannaCry attack. Security expert Lesley Carhart stated that "Every method of exploitation that the attack used to spread was preventable by well-documented means".[20]

Security experts found that the version of Petya used in the Ukraine cyberattacks had been modified, and subsequently has been named NotPetya or Nyetna to distinguish it from the original malware. NotPetya encrypted all of the files on the infected computers, not just the Master File Table, and in some cases the computer's files were completely wiped or rewritten in a manner that could not be undone through decryption.[21][22] Some security experts saw that the software could intercept passwords and perform administrator-level actions that could further ruin computer files. They also noted that the software could identify specific computer systems and bypass infection of those systems, suggesting the attack was more surgical in its goal.[20] There also has yet to be discovery of a "kill switch" as there was with the WannaCry software, which would immediately stop its spread.[23] According to Nicholas Weaver of the University of California the hackers had previously compromised MeDoc "made it into a remote-control Trojan, and then they were willing to burn this asset to launch this attack.[8]

Attack

During the attack the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant went offline.[24] Several Ukrainian ministries, banks, metro systems and state-owned enterprises (Boryspil International Airport, Ukrtelecom, Ukrposhta, State Savings Bank of Ukraine, Ukrainian Railways) were affected.[25] In the infected computers, important computer files were overwritten and thus permanently damaged, despite the malware's displayed message to the user indicating that all files could be recovered "safely and easily" by meeting the attackers' demands and making the requested payment in Bitcoin currency.[26]

The attack has been seen to be more likely aimed at crippling the Ukrainian state rather than for monetary reasons.[15] The attack came on the eve of the Ukrainian public holiday, Constitution Day (celebrating the anniversary of the approval by the Verkhovna Rada (Ukraine's parliament) of the Constitution of Ukraine on 28 June 1996).[27][28][29] Most government offices would be empty, allowing the cyberattack to spread without interference.[15] In addition, some security experts saw the ransomware engage in wiping the affected hard drives rather than encrypting them, which would be a further disaster for companies affected by this.[15]

A short time before the cyberattack began, it was reported that an intelligence officer and head of a special forces unit, Maksym Shapoval, was assassinated in Kiev by a car bomb.[30] Former government adviser in Georgia and Moldova Molly K. McKew believed this assassination was related to the cyberattack.[31]

On 28 June 2017 the Ukrainian government stated that the attack was halted, "The situation is under complete control of the cyber security specialists, they are now working to restore the lost data."[13]

Following the initial 27 June attack, security experts found that the code that had infected the M.E.Doc update had a backdoor that could potentially be used to launch another cyberattack. On seeing signs of another cyberattack, the Ukrainian police raided the offices of MeDoc on 4 July 2017 and seized their servers. MeDoc's CEO stated that they were now aware there had been a backdoor installed on their servers, again refuted their involvement in the attack, and were working to help authorities identify the source.[16][32] Security company ESET found that the backdoor had been installed on MeDoc's updater service as early as 15 May 2017, while experts from Cisco Systems' Talos group found evidence of the backdoor as early as April 2017; either situation points to the cyberattack as a "thoroughly well-planned and well-executed operation".[33] Ukrainian officials have stated that Intellect Service will "face criminal responsibility", as they had previously warned the company about lax security on their servers from anti-virus firms prior to these events but did not take steps to prevent it.[34] Talos warned that due to the large size of the MeDoc update that contained the NotPetya malware (1.5 gigabytes), there may be other backdoors that they have yet to find, and another attack could be possible.[33]

Attribution

On 30 June, the Security Service of Ukraine (SBU) reported it had seized the equipment that had been used to launch the cyberattack, claiming it to have belonged to Russian agents responsible for launching the attack.[35] On 1 July 2017 the SBU claimed that available data showed that the same perpetrators who in Ukraine in December 2016 attacked the financial system, transport and energy facilities of Ukraine (using TeleBots and BlackEnergy)[36] were the same hacking groups who attacked Ukraine on 27 June 2017. "This testifies to the involvement of the special services of Russian Federation in this attack," it concluded.[7][37] (A December 2016 cyber attack on a Ukrainian state energy computer caused a power cut in the northern part of the capital, Kiev).[7] Russia–Ukraine relations are at a frozen state since Russia's 2014 annexation of Crimea followed by a Russian government-backed separatist insurgency in eastern Ukraine in which more than 10,000 people had died by late June 2017.[7] (Russia has repeatedly denied sending troops or military equipment to eastern Ukraine).[7] Ukraine claims that hacking Ukrainian state institutions is part of what they describe as a "hybrid war" by Russia on Ukraine.[7]

On 30 June 2017, cyber security firm ESET claimed that the Telebots group (which they claimed had links to BlackEnergy) was behind the attack: "Prior to the outbreak, the Telebots group targeted mainly the financial sector. The latest outbreak was directed against businesses in Ukraine, but they apparently underestimated the malware's spreading capabilities. That's why the malware went out of control."[7] ESET had earlier reported that BlackEnergy

had been targeting Ukrainian cyber infrastructure since 2014.[38] In December 2016, ESET had concluded that TeleBots had evolved from the BlackEnergy hackers and that TeleBots had been using cyberattacks to sabotage the Ukrainian financial sector during the second half of 2016.[39]

Around the time of 4 July raid on MeDoc, the $10,000 in bitcoin already collected in the listed wallets for NotPetya had been collected, and experts believed it was used to buy space on the anonymous Tor network. One message posted there purportedly from the NotPetya authors demanded 100,000 bitcoin (about $2.6 million) to halt the attack and decrypt all affected files.[16] On 5 July 2017, a second message purportedly from the NotPetya authors was posted in a Tor website, demanding those that wish to decrypt their files send 100 bitcoin (approximately $250,000). The message was signed with the same private key used by the original Petya ransomware, suggesting the same group was responsible for both.[40]

According to reports cited in January 2018 the United States Central Intelligence Agency claimed Russia was behind the cyberattack, with Russia's Main Intelligence Directorate (GRU) having designed NotPetya.[41] Similarly, the United Kingdom Ministry of Defence accused Russia in February 2018 of launching the cyberattack, that by attacking systems in the Ukraine, the cyberattack would spread and affect major systems in the United Kingdom and elsewhere. Russia had denied its involvement, pointing out that Russian systems were also impacted by the attack.[42]

Wired technology writer Andy Greenberg, in reviewing the history of the cyberattacks, said that the attacks came from a Russian military hackers called "Sandworm". Greenberg asserted that Sandworm was behind the 2016 blackouts in Kiev, among other events. The group had been focusing on hacking into Ukraine's financial sector, and sometime in early 2017, had been able to gain access M.E. Doc's update servers, so that it could be used maliciously to send out the cyberattack in June 2017.[19]

Affected companies

Companies affected include Antonov, Kyivstar, Vodafone Ukraine, lifecell, TV channels STB, ICTV and ATR, Kiev Metro, UkrGasVydobuvannya (UGV), gas stations WOG, DTEK, EpiCentre K, Kyiv International Airport (Zhuliany), Prominvestbank, Ukrsotsbank, KredoBank, Oshchadbank and others,[13] with over 1,500 legal entities and individuals having contacted the National Police of Ukraine to indicate that they had been victimized by 27 June 2017 cyberattack.[43] Oshchadbank was again fully functional on 3 July 2017.[44] Ukraine's electricity company's computers also went offline due to the attack; but the company continued to fully operate without using computers.[8]

While more than 80% of affected companies were from Ukraine, the ransomware also spread to several companies in other geolocations, due to those businesses having offices in Ukraine and networking around the globe. Non-Ukrainian companies reporting incidents related to the attack include food processor Mondelez International,[45] the APM Terminals subsidiary of international shipping company A.P. Moller-Maersk, the FedEx shipping subsidiary TNT Express (in August 2017 its deliveries were still disrupted due to the attack),[46] Chinese shipping company COFCO Group, French construction materials company Saint Gobain,[47] advertising agency WPP plc,[48] Heritage Valley Health System of Pittsburgh,[49] law firm DLA Piper,[50] pharmaceutical company Merck & Co.,[51] consumer goods maker Reckitt Benckiser, and software provider Nuance Communications.[52] A Ukrainian police officer believes that the ransomware attack was designed to go global so as to distract from the directed cyberattack on Ukraine.[53]

The cost of the cyberattack had yet to be determined, as, after a week of its initial attack, companies were still working to mitigate the damage. Reckitt Benckiser lowered its sales estimates by 2% (about $130 million) for the second quarter primarily due to the attack that affected its global supply chain.[54][52] Tom Bossert, the Homeland Security adviser to the President of the United States, stated that the total damage was over US$10 billion.[19] Among estimated damages to specific companies included over US$870 million to Merck, US$400 million to FedEx, US$384 million to Saint-Gobain, and US$300 million to Maersk.[19]

Reaction

Secretary of the National Security and Defence Council of Ukraine Oleksandr Turchynov claimed there were signs of Russian involvement in the 27 June cyberattack, although he did not give any direct evidence.[55] Russian officials have denied any involvement, calling Ukraine's claims "unfounded blanket accusations".[35]

NATO Secretary-General Jens Stoltenberg vowed on 28 June 2017 that NATO would continue its support for Ukraine to strengthen its cyber defence.[56]

See also

- December 2015 Ukraine power grid cyberattack

References

1. Rothwell, James; Titcomb, James; McGoogan, Cara (27 June 2017). "Petya cyber attack: Ransomware spreads across Europe with firms in Ukraine, Britain and Spain shut down" (https://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/). *The Daily Telegraph*.
2. "Tax software blamed for cyber-attack spread" (https://www.bbc.com/news/technology-40428967). *BBC News*. 28 June 2017. Retrieved 28 June 2017.
3. Turner, Giles; Verbyany, Volodymyr; Kravchenko, Stepan (27 June 2017). "New Cyberattack Goes Global, Hits WPP, Rosneft, Maersk" (https://www.bloomberg.com/news/articles/2017-06-27/ukraine-russia-report-ransomware-computer-virus-attacks). *Bloomberg*. Retrieved 27 June 2017.
4. "Businesses warned again to update patches as Petya ransomware hits Australian offices" (http://www.afr.com/technology/web/security/businesses-warned-to-act-as-petya-ransomware-hits-australian-offices-20170627-gx00de). *Financial Review*. 28 June 2017. Retrieved 3 July 2017.
5. "Oleksandr Turchynov: One of the mechanisms for spreading a dangerous computer virus was a system for updating the accounting software – National Security and Defense Council of Ukraine" (http://www.rnbo.gov.ua/en/news/2821.html). *RNBO*.
6. "SBU establishes involvement of the RF special services into Petya.A virus-extorter attack" (https://ssu.gov.ua/en/news/1/category/21/view/3660). *Security Service of Ukraine*.
7. "Ukraine points finger at Russian security services in recent cyber attack" (http://mobile.reuters.com/article/idUSKBN19M39P). Reuters. 1 July 2017. Retrieved 1 July 2017.
8. Borys, Christian (26 July 2017). "Ukraine braces for further cyber-attacks" (https://www.bbc.com/news/technology-40706093). *BBC News*. Retrieved 26 July 2017.
9. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes (https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html) Washington Post, 2018
10. Prentice, Alessandra (27 June 2017). "Ukrainian banks, electricity firm hit by fresh cyber attack" (https://www.reut

ers.com/article/us-ukraine-cyber-attacks-idUSKBN19I1IJ). *Reuters*. Retrieved 27 June 2017.

11. Scott, Nicole Perlroth, Mark; Frenkel, Sheera (27 June 2017). "Cyberattack Hits Ukraine Then Spreads Internationally" (https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Retrieved 4 July 2017.
12. "Global ransomware attack causes chaos" (https://www.bbc.com/news/technology-40416611). *BBC News*. 27 June 2017. Retrieved 27 June 2017.
    Burgess, Matt. "There's another 'worldwide' ransomware attack and it's spreading quickly" (https://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017). *Wired UK*. Retrieved 27 June 2017.
13. Cyber attack on Ukrainian government and corporate networks halted (https://www.ukrinform.net/rubric-politics/2255698-cyber-attack-on-ukrainian-government-and-corporate-networks-halted.html), Ukrinform (28 June 2017)
14. "Companies still hobbled from fearsome cyberattack" (https://www.apnews.com/ce7a8aca506742ab8e8873e7f9f229c2/Companies-still-hobbled-from-fearsome-cyberattack). *Associated Press*. 30 June 2017. Retrieved 3 July 2017.
15. Kramer, Andrew (28 June 2017). "Ukraine Cyberattack Was Meant to Paralyze, not Profit, Evidence Shows" (https://www.nytimes.com/2017/06/28/world/europe/ukraine-ransomware-cyberbomb-accountants-russia.html). *The New York Times*. Retrieved 29 June 2017.
16. Satter, Raphael (5 July 2017). "Ukraine says it foiled 2nd cyberattack after police raid" (https://www.washingtonpost.com/business/technology/ukraine-we-prevented-second-cyberattack/2017/07/05/3cb65202-615f-11e7-80a2-8c226031ac3f_story.html). *Associated Press*. Retrieved 5 July 2017.
17. Frenkel, Sheera (27 June 2017). "Global Ransomware Attack: What We Know and Don't Know" (https://www.nytimes.com/2017/06/27/technology/global-ransomware-hack-what-we-know-and-dont-know.html). *The New York Times*. Retrieved 28 June 2017.
18. Красномовец, Павел (24 May 2017). "Все, что известно про вирус-вымогатель XData: кто под угрозой и что делать" (https://ain.ua/2017/05/24/vse-pro-xdata-poka). *AIN.UA* (in Russian). Retrieved 29 June 2017.
19. Greenberg, Andy (23 August 2018). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" (https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/). *Wired*. Retrieved 23 August 2018.
20. Borys, Christian (4 July 2017). "The day a mysterious cyber-attack crippled Ukraine" (http://www.bbc.com/future/story/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine). *BBC*. Retrieved 8 July 2017.
21. Polityuk, Pavel (29 June 2017). "Global cyber attack likely cover for malware installation in Ukraine: police official" (https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19K1WI). *Reuters*. Retrieved 29 June 2017.
22. Petroff, Alanna (30 June 2017). "Experts: Global cyberattack looks more like 'sabotage' than ransomware" (http://money.cnn.com/2017/06/30/technology/ransomware-cyber-attack-computer/index.html). *CNN*. Retrieved 30 June 2017.
23. Petroff, Alanna (28 June 2017). "Europol: There's no 'kill switch' for malware attack" (http://money.cnn.com/2017/06/28/technology/cyberattack-malware-europol/index.html?iid=EL). *CNN*. Retrieved 30 June 2017.
24. Griffin, Andrew (27 June 2017). "Chernobyl's radiation monitoring system has been hit by the worldwide cyber attack" (https://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html). *The Independent*. Retrieved 27 June 2017.
25. Dearden, Lizzie (27 June 2017). "Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers" (https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html). *The Independent*. Retrieved 27 June 2017.
26. "Cyber-attack was about data and not money, say experts" (https://www.bbc.com/news/technology-40442578). *BBC News*. 29 June 2017. Retrieved 29 June 2017.
    "Tuesday's massive ransomware outbreak was, in fact, something much worse" (https://arstechnica.com/security/2017/06/petya-outbreak-was-a-chaos-sowing-wiper-not-profit-seeking-ransomware/). *Ars Technica*. Retrieved 28 June 2017.

27. 1996: THE YEAR IN REVIEW (http://www.ukrweekly.com/old/archive/1996/529606.shtml), The Ukrainian Weekly (29 December 1996)
28. Lee, David (28 June 2017). " 'Vaccine' created for huge cyber-attack" (https://www.bbc.com/news/technology-40427907). *BBC News*. Retrieved 28 June 2017.
29. "Cyberattack Hits Ukraine Then Spreads Internationally" (https://mobile.nytimes.com/2017/06/27/technology/ransomware-hackers.html). *The New York Times*. 27 June 2017. Retrieved 28 June 2017.
30. Luhn, Alec. "Ukrainian military intelligence officer killed by car bomb in Kiev" (https://www.theguardian.com/world/2017/jun/27/ukraine-colonel-maksim-shapoval-killed-car-bomb-kiev). The Guardian. Retrieved 28 June 2017.
31. McKew, Molly (27 June 2017). "A killing in Kiev shows how the West continues to fail Ukraine" (https://www.washingtonpost.com/news/democracy-post/wp/2017/06/27/a-killing-in-kiev-shows-how-the-west-continues-to-fail-ukraine/). The Washington Post. Retrieved 28 June 2017.
32. Stubbs, Jack (5 July 2017). "Ukraine scrambles to contain new cyber threat after NotPetya attack" (https://www.reuters.com/article/us-cyber-attack-ukraine-backdoor-idUSKBN19Q14P). *Reuters*. Retrieved 5 July 2017.
33. Goodin, Dan (5 July 2017). "Backdoor built in to widely used tax app seeded last week's NotPetya outbreak" (https://arstechnica.com/security/2017/07/heavily-armed-police-raid-company-that-seeded-last-weeks-notpetya-outbreak/). *Ars Technica*. Retrieved 5 July 2017.
34. Satter, Raphael (3 July 2017). "Official: firm at center of cyberattack knew of problems" (https://apnews.com/8b02768224de485eb4e7b33ae55b02f2). *Associated Press*. Retrieved 7 July 2017.
35. "Ukraine Says Seized Equipment Used by Russia to Launch Malware Attacks" (https://www.nytimes.com/reuters/2017/06/30/business/30reuters-cyber-attack-ukraine-sbu.html). *The NY Times*. Reuters. 30 June 2017. Retrieved 30 June 2017.
36. "Software: BlackEnergy, Black Energy - ATT&CK" (https://attack.mitre.org/wiki/Software/S0089). *attack.mitre.org*. Retrieved 4 July 2017.
37. "Ukraine Security Service Blames Russia For Recent Cyberattack" (https://www.rferl.org/a/cyberattack-ukraine-blames-russia/28589606.html). *Radio Free Europe*. 1 July 2017. Retrieved 1 July 2017.
38. '"Russian" BlackEnergy malware strikes at Ukrainian media and energy firms (https://www.scmagazine.com/russian-blackenergy-malware-strikes-at-ukrainian-media-and-energy-firms/article/527815/)', *SC Magazine* (4 January 2016)
39. 'Telebots cybergang toolset reminiscent of BlackEnergy (https://www.scmagazine.com/blackenergy-back-telebots-launch-malicious-toolset-reminiscent-of-earlier-attacks/article/579319/)', *SC Magazine* (15 December 2016)
40. Brandom, Russell (5 July 2017). "Petya ransomware authors demand $250,000 in first public statement since the attack" (https://www.theverge.com/2017/7/5/15922216/petya-notpetya-ransomware-authors-bitcoin-demand-decrypt). *The Verge*. Retrieved 5 July 2017.
41. Nakashima, Ellen (12 January 2018). "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes" (https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html). *The Washington Post*. Retrieved 15 February 2018.
42. Marsh, Sarah (15 February 2018). "UK blames Russia for NotPetya cyber-attack last year" (https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine). *The Guardian*. Retrieved 15 February 2018.
43. 'Virus Petya has hurt more than 1,5 thousand legal entities and individuals (http://www.pravda.com.ua/news/2017/06/29/7148210)', *Ukrayinska Pravda* (29 June 2017) (in Ukrainian).
44. '"Oschadbank" resume the work of all departments on July 3 (http://pda.pravda.com.ua/news/id_7148435)', *Ukrayinska Pravda* (1 July 2017) (in Ukrainian).
45. Voß, Oliver (3 July 2017). "Milka-Fabrik steht seit einer Woche still" (http://www.tagesspiegel.de/wirtschaft/wegen-erpressersoftware-petya-milka-fabrik-steht-seit-einer-woche-still/20013388.html). *Tagesspiegel* (in German). Retrieved 5 July 2017.

46. Customers 'furious' with TNT after cyber-attack meltdown (https://www.bbc.com/news/technology-40861982), BBC News (9 August 2017)
47. Auchard, Eric; Stubbs, Jack; Prentice, Alessandra (29 June 2017). "New computer virus spreads from Ukraine to disrupt world business" (https://www.reuters.com/article/us-cyber-attack-idUSKBN19I1TD). Reuters. Retrieved 30 June 2017.
48. Perlroth, Nicole; Scott, Mark; Frenkel, Sheera (27 June 2017). "Cyberattack Hits Ukraine Then Spreads Internationally" (https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html). *The New York Times*. Retrieved 6 July 2017.
49. Henley, Jon; Solon, Olivia (27 June 2017). " 'Petya' ransomware attack strikes companies across Europe and US" (https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe). *The Guardian*. Retrieved 6 July 2017.
50. Petroff, Alanna; Larson, Selena (28 June 2017). "Another big malware attack ripples across the world" (http://money.cnn.com/2017/06/27/technology/hacking-petya-europe-ukraine-wpp-rosneft/index.html). CNN. Retrieved 6 July 2017.
51. Massarella, Linda (27 June 2017). "Europe cyberattack also breaches Merck headquarters in US" (https://nypost.com/2017/06/27/europe-cyberattack-also-breaches-merck-headquarters-in-us/). *New York Post*. Retrieved 5 July 2017.
52. Perlroth, Nicole (6 July 2017). "Lasting Damage and a Search for Clues in Cyberattack" (https://www.nytimes.com/2017/07/06/technology/search-for-clues-global-cyberattacks.html). *The New York Times*. Retrieved 7 July 2017.
53. Polityuk, Pavel; Auchard, Eric (29 June 2017). "Global cyber attack likely cover for malware installation in Ukraine: police official" (https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19K1WI). Kiev, Frankfurt: Reuters. Retrieved 30 June 2017.
54. Geller, Martinne; Sandle, Paul (6 July 2017). "Reckitt Benckiser trims sales forecasts after cyber attack" (http://uk.reuters.com/article/us-reckitt-benc-grp-outlook-idUKKBN19R0GQ). Reuters. Retrieved 6 July 2017.
55. Ukraine Is 'Ground Zero' For Hackers In Global Cyberattacks (https://www.rferl.org/a/ukraine-petya-ransomware-cyberattack-ground-zero/28583931.html), Radio Free Europe (28 June 2017)
56. Stoltenberg: NATO to increase aid to Ukraine in field of cyber defense (https://www.ukrinform.net/rubric-defense/2255739-stoltenberg-nato-to-increase-aid-to-ukraine-in-field-of-cyber-defense.html), Ukrinform (28 June 2017)

External links

- Greenberg, Andy (20 June 2017). "How An Entire Nation Became Russia's Test Lab for Cyberwar" (https://www.wired.com/story/russian-hackers-attack-ukraine/). *Wired*.
