European
Repository of
Cyber Incidents

Major Cyber Incidents

NOTPETYA [EuRepoC Link]

Other incident names: ExPetr, SortaPetya, Petna, ExPetr, Diskcoder.C, Nyetya, GoldenEye [1]

Description

The Russian military intelligence service, the GRU, used a Trojan to initially target Ukrainian infrastructure with a wiper called NotPetya. The attack spread worldwide to become what the United States considered the most destructive and costly cyber-attack in history. IT companies linked the campaign to the APT group Sandworm, who have been linked to many disruptive cyber-attacks against Ukraine, such as the two consecutive energy blackouts in Ukraine at the end of 2015 & 2016. Multiple governments attributed the campaign to the GRU and its Unit 74455 that is generally associated with Sandworm. Political and legal action was taken by the European Union and several individual governments in response.

Timeframe From 27 June 2017	**Initiator** Russian state-affiliated group "Sandworm"
Incident Type Disruption, Hijacking with Misuse	**Affected Target** Ukrainian Infrastructure and hundreds of entities across the world

Impact and significance

Initially, NotPetya interrupted the operation of banking, power, airports, and metro services in Ukraine. However, the destructive malware spread globally and affected hundreds of entities worldwide, including Ukrainian aircraft manufacturer, Antonov; Russia's biggest oil producer, Rosneft; and Danish shipping company Maersk's container shipping, oil, gas, and drilling operations. A port in Mumbai also halted operations as a result. [2] NotPetya also crippled pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelēz, and manufacturer Reckitt Benckiser. [3] The White House estimated the damages to be more than 10 billion US dollars. [4] NotPetya was the first in a series of disruptive cyber operations attributed to Sandworm which targeted Ukraine and massively impacted third parties (see fig. 1 and fig. 3 below). The IT company McAfee has referred to NotPetya as an exercise to test and observe response capabilities. [5] The White House concluded that "the Russian military launched the most destructive and

By Mika Kerttunen and Jonas Hemmelskamp

costly cyber-attack in history." [6] NotPetya was a turning point in political attribution towards or vis-à-vis Sandworm operations (see fig. 4 below).

Fig. 1: Cyber activities between Russia and Ukraine

In context of the HIIK offline conflict Russia - Ukraine

2015 **Sandworm vs. Ukrainian Company StarLight Media** [a]

The disruptive malware KillDisk deleted critical data and made computers unusable within Ukrainian company networks.

disruption | hijacking with misuse

Sandworm vs. Ukrainian Railway company and airport [b]

KillDisk was detected in the networks of the state-owned railway company and the international airport of Borispol, affecting critical infrastructure.

disruption | hijacking with misuse

Ukraine Power Outage [c]

A Ukrainian power sector was taken down by sophisticated malware, causing a severe power outage. The attack was attributed to Sandworm.

disruption | hijacking with misuse

2016 **Sandworm Attacks on Ukrainian financial Institutions** [d]

Hackers shut down the payment system of the Treasure and Pension Fund of Ukraine's Ministry of Finance.

disruption | hijacking with misuse

Bellingcat Hack [e] (third party affected)

Cyber-Berkut defaced the website of the journalism collective Bellingcat that investigated the MH17 downing and leaked Information of a Russian member.

data theft & doxing | hijacking with misuse

Ukraine Power Outage 2 [f]

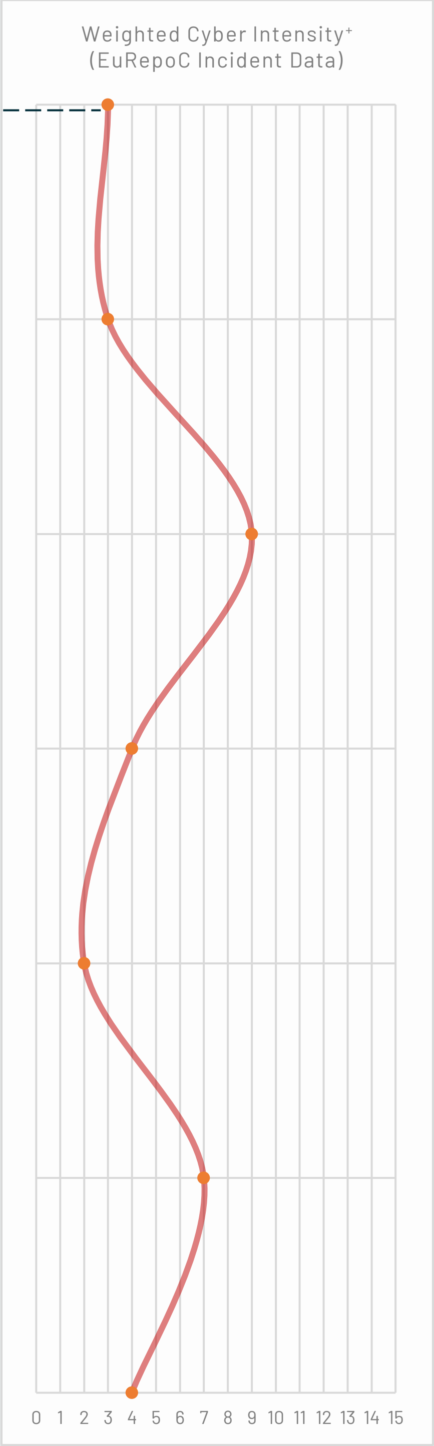
An electric transmission station north of Kiev was taken down, blacking out a portion of the city for one hour.

disruption | hijacking with misuse

2017 **Not Petya** [g] (third parties also affected)

GRU used an extremely infectious wiper called NotPetya against Ukrainian infrastructure, spreading to countries worldwide and causing immense financial damage. Political and legal action was taken in the aftermath by multiple governments.

disruption | hijacking with misuse



+ The *Weighted Cyber Intensity* score is derived from the EuRepoC 1.0 dataset. It assesses the type of attacks, their potential physical effects in reach and duration, and their socio-political severity. Scores 0-5 are considered low/moderate in intensity, scores 6-10 indicate high intensity, and 11-15 very high intensity incidents. See here for more information on the EuRepoC codebook.

Links to incidents in the EuRepoC database

[a] https://eurepoc.eu/incident/sandworm-vs-ukrainian-company-star-light-media-2015
[b] https://eurepoc.eu/incident/sandworm-vs-ukrainian-railway-company-and-airport-2015
[c] https://eurepoc.eu/incident/ukraine-power-outage-2015
[d] https://eurepoc.eu/incident/sandworm-2-0-attacks-on-ukrainian-financial-institutions-2016-1
[e] https://eurepoc.eu/incident/bellingcat-hack-2016
[f] https://eurepoc.eu/de/incident/ukraine-power-grid-2
[g]https://eurepoc.eu/incident/russian-apt-sandworm-aka-telebots-initially-targeted-ukrainian-infrastructures-with-a-wiper-campaign-called-not-petya-since-june-2017-causing-billions-of-dollars-of-financial-damage-worldwide-1

Background

In context of the politico-military conflict between Russia and Ukraine, EuRepoC data shows Sandworm has been conducting disruptive and destructive cyber campaigns against Ukraine for years. In August 2016, the hacker group “ShadowBrokers” claimed to have infiltrated the Equation Group, an elite hacking unit linked to the US National Security Agency, and they further claimed to have stolen “cyber weapons” which they were auctioning to the highest bidder via Twitter, Tumblr, PasteBin, and GitHub. [7] In April 2017, they leaked multiple NSA software tools to the public. [8] NotPetya, which utilises the exploit “EternalBlue” from the leak, was launched on or around June 27 – on the eve of Ukraine’s Constitution Day, which commemorates the adoption of independent Ukraine’s constitution after the collapse of the Soviet Union. [9] The leakage happened against the backdrop of US-Russian political differences over the development of military cyber capabilities, and it connects to the Russian interest in portraying US activities as harmful to the international community. This further plays into the resulting interest in exposing US capabilities and their use to invoke wider support for the Russian position.

Attribution

The IT security community quickly came to the conclusion that the group behind the incident was also responsible for the "KillDisk" attacks against Ukraine. [10] The Five Eyes and Ukraine attributed the attack towards the Russian [11] APT Sandworm. [12] The governments of Denmark, Lithuania, and Estonia blamed Russia in official statements. Norway, Latvia, Sweden, and Finland shared their concerns in official statements of support. [13] The US indicted six GRU officers in conjunction with this operation [14] and took action in the form of economic sanctions in 2018. [15] The EU condemned the incident [16] and created the European Cyber Diplomacy Toolbox in the aftermath [17], taking legal action in the form of economic sanctions and actions against members of Sandworm in 2020. [18] According to EuRepoC data, NotPetya was the first incident resulting in political attribution towards or vis-à-vis Sandworm, and their operations in the years after were met with more political attribution (see Fig. 4 below).

Fig. 2: Operation timeline

Aug. 2016	Shadow Brokers claimed access to "cyber weapons"
14.03.2017	Microsoft releases critical security bulletin MS17-010 A patch is released to close the EternalBlue vulnerability
14.04.2017	Shadow Brokers leaked the NSA tools to the public
12.05.2017	Ransomware "WannaCry" abused EternalBlue
27.06.2017	Wiper NotPetya abused EternalBlue

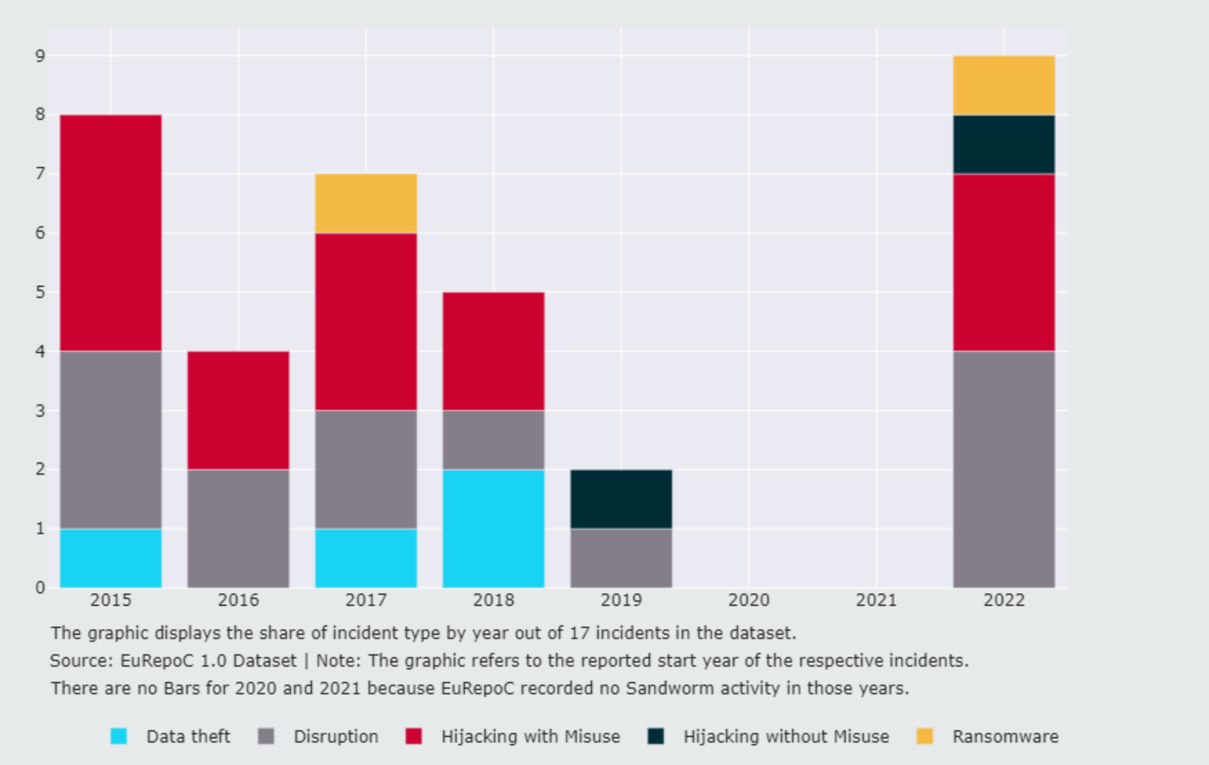
Technical details

A supply-chain attack utilising a backdoor in the update process of Ukrainian tax preparation program M.E. Doc was used for initial access of NotPetya. [19] This program was one of only two programs approved for Ukrainian companies working with the government. [20] NotPetya used the EternalBlue exploit within Windows file-sharing protocol SMB to spread within the local networks and the open-source tool Mimikatz to achieve higher access privileges. [21] The latter finds and abuses login privileges on the infected PC's memory, which is especially useful if a domain administrator was logged into the machine before. [22] A feature that differentiated NotPetya from WannaCry is that the former only spread within the local network after infection, and not over the internet. Companies not using M.E Doc were infected because they maintained VPN connections to infected networks. [23] This combination of initial access and the usage of EternalBlue for spreading made the malware tremendously infectious. According to analysts, NotPetya's goal was purely destructive. As a wiper, it irreversibly encrypted computers' master boot records. No key is known to have existed to reorder data, despite the malware displaying a message demanding a ransom. This differentiates a wiper from ransomware that actually aims at receiving ransom payments. [24]

Enablers

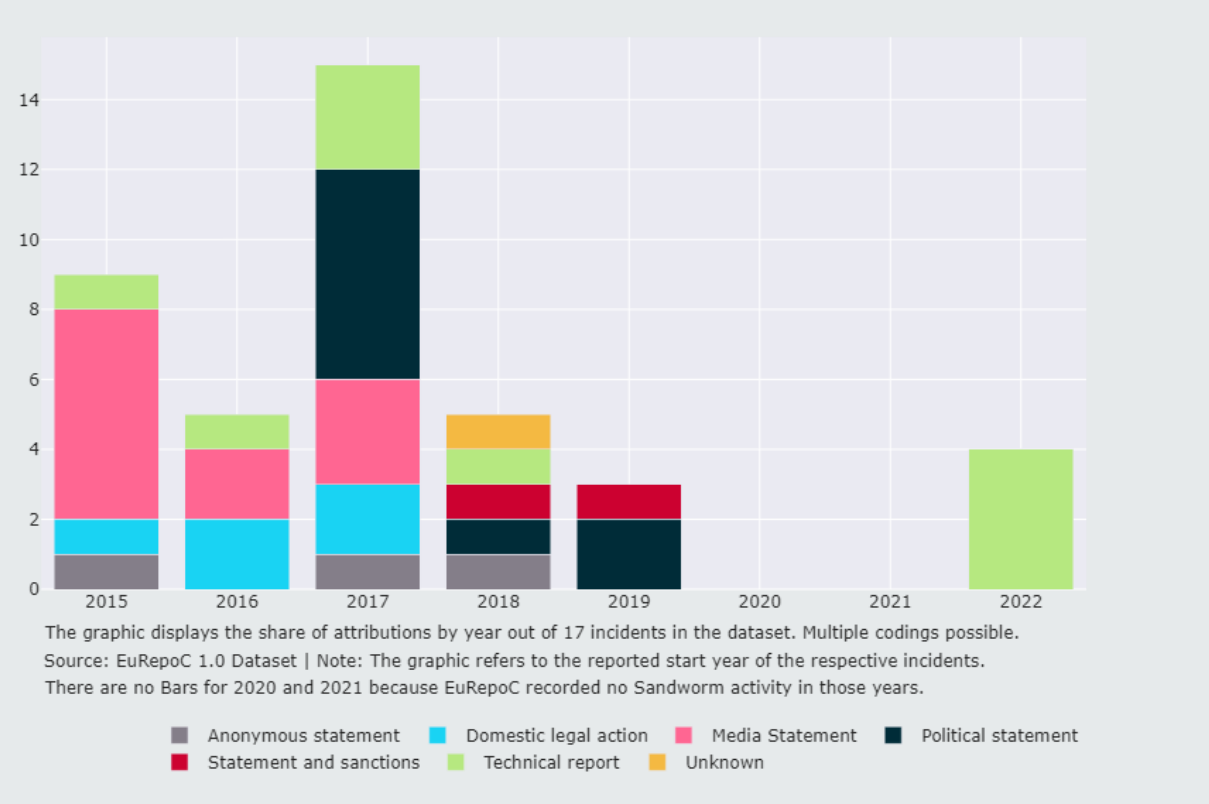
Underdeveloped cybersecurity practices and specifically bad patch administration enabled this attack; EternalBlue was patched by Microsoft on 14.03.2017, a month before the vulnerability was publicly disclosed by Shadow Brokers on 14.04.2017. [25] Before NotPetya, other extremely disruptive malware, in particular WannaCry, had already abused the vulnerability. [26] Affected machines were not updated. However, EternalBlue had originally been a stockpiled vulnerability of United States Intelligence Agency NSA`s Tailored Access Operations (TAO) unit, intended for the exclusive use by the agency Nobody but us (NOBUS). [27]

Fig. 3: Worldwide activity of Sandworm between 2015 and 2022



The graphic displays the share of incident type by year out of 17 incidents in the dataset.
Source: EuRepoC 1.0 Dataset | Note: The graphic refers to the reported start year of the respective incidents.
There are no Bars for 2020 and 2021 because EuRepoC recorded no Sandworm activity in those years.

Fig. 4: Type of attributions to Sandworm between 2015 and 2022



The graphic displays the share of attributions by year out of 17 incidents in the dataset. Multiple codings possible.
Source: EuRepoC 1.0 Dataset | Note: The graphic refers to the reported start year of the respective incidents.
There are no Bars for 2020 and 2021 because EuRepoC recorded no Sandworm activity in those years.

Private Sector Engagement

Crowdstrike (analysis) [28]
CarbonBlack (analysis) [29]
ISSP (analysis) [30]
LogRhythm (analysis) [31]
Kaspersky (analysis) [32]
Symantec (mitigation) [33]
Microsoft (mitigation) [34]

Legal Assessment

NotPetya was followed by "the largest coordinated attribution of its kind to date" (see above, attribution). [35, 11-13] But international law was only directly mentioned in statements condemning the incident by Estonia and, later, by the European Union. The latter referred to the applicability of international law in cyberspace and cited UN Group of Governmental Experts (GGE) reports of 2013 and 2015 [36] It was also the first cyber operation that triggered a coordinated diplomatic response from the European Union. [37] The United Kingdom referred to the incident as a display of continued Russian disregard for Ukrainian sovereignty. [38] While there was an academic discussion on NotPetya possibly passing the threshold of use of force as regulated in Art. 2 (4) of the UN Charta, this was not invoked in political responses. [40] Yet the incident also highlighted the issue of cyber insurance. Both Merck's (losses of up to 670 million US-Dollar) and Mondelēz's insurance claims were refused, citing a "warlike action" conducted by "government or sovereign power," which is a common exclusion clause in "all risk" property insurances, leading to legal disputes against their respective insurers. [41] The case has broad implications on risk insurances because multiple sovereign governments and the European Union blamed the Russian government for the incident without referring to it as a "warlike action". Merck received its first proceeds soon after the incident [42] and won their case against the insurance company in 2021, with the court arguing that the exemptions on warlike action would only apply to traditional forms of warfare. [43] However, the insurance company is still in the process of appealing the decision, citing NotPetya being a "cyber nuclear attack" in the sense of collateral damage [44]. Mondelēz's case was settled in 2022 with no details disclosed. [45]

Further Reading

On legal implications

Schmitt, Michael/Biller, Jeffrey. 2017. The NotPetya Cyber Operation as a Case Study of International Law. Blog of the European Journal of International Law. July 11. Available at: https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/ [Archived on: 16.08.2022]

Broeders, Dennis. 2022. Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand? Journal of Cyber Policy 7 (1). 18 February. Available at: https://www.tandfonline.com/doi/full/10.1080/23738871.2022.2041061

Wan, Katherine S. 2020. Notpetya, not warfare: rethinking the insurance war exclusion in the context of international cyberattacks. Washington Law Review, 95(3), 1595-1620.

Early report on the political intends of NotPetya

Auchard, Eric/ Polityuk, Pavel. 2017. Global Cyber Attack Likely Cover for Malware Installation in Ukraine: Police Official. Reuters. 29 June. Available at: https://www.reuters.com/article/us-cyber-attack-ukraine/global-cyber-attack-likely-cover-for-malware-installation-in-ukraine-police-official-idUSKBN19K1WI [Archived on: 15.02.2018]

Sources

[1] J. Schwartz, Mathew. 2018. NotPetya: From Russian Intelligence, With Love. Bank Info Security, 16 January. Available at: https://www.bankinfosecurity.com/notpetya-from-russian-intelligence-love-a-10589 [Archived on: 27.11.2022]

[2] BBC News. 2017. Global Ransomware Attack Causes Turmoil. BBC News, 28 June. Available at: https://www.bbc.com/news/technology-40416611[Archived on: 02.06.2022]

[3] Greenberg, Andy. 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*, 22 August. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Archived on: 03.11.2022]

[4] United States Department of the Treasury. 2018. Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks. United States Department of the Treasury. 15 March. Available at: https://home.treasury.gov/news/press-releases/sm0312 [Archived on: 19.01.2023]

[5] McAfee. 2011. Ten Days of Rain Expert Analysis of Distributed Denial-of-Service Attacks Targeting. McAfee. Available at: https://www.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf [Archived on: 28.05.2022]

[6] Greenberg 2018

[7] Solon, Olivia. 2016. Hacking Group Auctions "Cyber Weapons" Stolen from NSA. The Guardian. 16 August. Available at: https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group [Archived on: 07.12.2022]

[8] Burdova, Carly. 2022. What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant? Available at: https://www.avast.com/c-eternalblue [Archived on: 09.02.2023]

[9] United States District Court, Western District of Pennsylvania. 2020. Indictment. 15 October 2020. Available at: https://www.justice.gov/opa/press-release/file/1328521/download [Archived on: 12.02.2023]

[10] Cherepanov, Anton. 2017. TeleBots sind zurück. We live security. 3 July. Available at: https://www.welivesecurity.com/deutsch/2017/07/03/telebots-supply-chain-attack-gegen-ukraine/ [Archived on 23.03.2022]

[11] Government Communications Security Bureau. 2018. New Zealand Joins International Condemnation of NotPetya Cyber-Attack. 16 February 2018. Available at: https://www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack/ [Archived on: 21.02.2022]; Bossenmaier, Greta. 2018. CSE Statement on the NotPetya Malware. Communications Security Establishment. 15 February. Available at: https://www.cse-cst.gc.ca/en/media/2018-02-15 [Archived on: 21.10.2021]; Fleming, Jeremy. 2018. Director's Speech at Cyber UK 2018. Government Communications Headquarters. 12 April. Available at: https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018 [Archived on: 28.03.2022]; Cybersecurity and Infrastructure Security Agency 2017. Petya Ransomware. 1 July. Available at: https://us-cert.cisa.gov/ncas/alerts/TA17-181A [Archived on: 01.11.2022]; United States Department of the Treasury 2018

[12] MITRE ATT&CK. 2017. Sandworm Team, ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, VOODOO BEAR, Group G0034. MITRE ATT&CK. 31 May. Available at: https://attack.mitre.org/groups/G0034/ [Archived on: 10.01.2023]

[13] "Stilgherrian". 2018. Blaming Russia for NotPetya Was Coordinated Diplomatic Action. ZDNet. 12 April. Available at: https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/ [Archived on: 26.11.2022]; Hjort, Claus. 2018. Rusland Stod Bag Cyberangreb Mod Mærsk. Berlingske. 15 February. Available at: https://www.berlingske.dk/virksomheder/claus-hjort-rusland-stod-bag-cyberangreb-mod-maersk [Archived on: 16.12.2022]; Mikse, Sven r. 2018. Foreign Minister Condemns Russia 's Cyber Attack on NotPetya Ukraine. Ministry of Foreign Affairs of the Republic of Estonia. 15 February. Available at: https://vm.ee/et/uudised/valisminister-moistab-hukka-venemaa-kuberrunde-notpetya-ukraina-vastu [Archived on: 20.01.2022]; Ministry of Foreign Affairs of the Republic of Latvia (@Latvian_MFA). 2018. Latvia is deeply concerned about the findings of UK &US attribution of NotPetya Cyber attacks and stands for responsible state behaviour in cyberspace. Twitter. 16 February. https://twitter.com/latvian_mfa/status/964363315194486784 [Archived on: 01.03.2023]

[14] United States District Court, Western District of Pennsylvania 2020

[15] United States Department of the Treasury. 2018

[16] Council of the European Union 2018. Council Conclusions on Malicious Cyber Activities. Council of the European Union. 16 April. Available at: https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf [Archived on: 01.11.2022]

[17] Bendiek, Annegret/Schulze, Matthias. 2021. Attribution. A Major Challenge for EU Cyber Sanctions. SWP Research Paper. 16 December. Available at: https://www.swp-berlin.org/publications/products/research_papers/2021RP11_EU_CyberSanctions.pdf [Archived on: 07.03.2022]

[18] Council of the European Union. 2020. Council Implementing Regulation (EU) 2020/1125. 30 July. Council of the European Union. Available at: https://eur-

lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020R1125&from=EN [Archived on: 05.12.2022]

[19] Turner, Giles/ Al Ali, Nour. 2017. Microsoft, Analysts See Hack Origin at Ukrainian Software Firm. Bloomberg. 28 June. Available at: https://www.bloomberg.com/news/articles/2017-06-28/microsoft-analysts-see-hack-origin-at-ukrainian-software-firm [Archived on: 28.06.2017]

[20] Schwartz, Matthew J. 2017. NotPetya Patient Zero. Ukrainian Accounting Software Vendor. July 4. Bank Info Security. Available at: https://www.bankinfosecurity.com/notpetya-patient-zero-ukrainian-accounting-software-vendor-a-10080 [Archived on: 03.04.2022]

[21] Greenberg 2018

[22] Crowdstrike. 2022. What is a golden ticket? July 22. Crowdstrike. Available at: https://www.crowdstrike.com/cybersecurity-101/golden-ticket-attack/ [Archived on: 01.12.2022]

[23] Greenberg 2018

[24] Cherepanov, Anton 2017

[25] Burdova 2022

[26] Europol. 2017. Wannacry Ransomware. Europol. 6 November. Available at: https://www.europol.europa.eu/wannacry-ransomware [Archived on: 02.10.2022]

[27] Newman, Lily Hay. 2018. The Leaked NSA Spy Tool That Hacked the World. Wired. March 7. Available at: https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ [Archived on: 07.02.2023]; Shane, Scott/Perlroth, Nicole/Sanger, David E. 2017. Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core. New York Times. 12 November. Available at: https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html?module=inline [Archived on: 15.02.2023]

[28] Sood, Karan/ Hurley, Shaun. 2017. NotPetya Ransomware Attack [Technical Analysis]. CrowdStrike. 29 June. Available at: https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ [Archived on: 16.02.2023]

[29] Carbon Black. 2017. Threat Research Technical Analysis: Petya / NotPetya Ransomware. Carbon Black. 28 June. Available at: https://www.carbonblack.com/blog/carbon-black-threat-research-technical-analysis-petya-notpetya-ransomware/ [Archived on 27.011.2021]

[30] Greenberg 2018

[31] LogRythm. 2017. NotPetya Technical Analysis. LogRhythm. 30 June. Available at: https://logrhythm.com/blog/notpetya-technical-analysis/ [Archived on: 07.12.2022]

[32] Ivanov, Anton/ Mamedov, Orkhan. 2017. ExPetr/Petya/NotPetya Is a Wiper, Not Ransomware. Securelist. 28 June. Available at: https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ [Archived on: 28.01.2023]

[33] Symantec Security Response Team. 2017. Petya Ransomware Outbreak: Here's What You Need to Know. Symantec Blogs. 24 October. Available at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper [Archived on: 07.12.2022]

[34] Simos, Mark. 2018. Overview of Rapid Cyberattacks. Microsoft Security. 23 January. Available at:

https://www.microsoft.com/security/blog/2018/01/23/overview-of-rapid-cyberattacks/ [Archived on: 15.11.2022]

[35] "Stilherrigan" 2018

[36] Broeders, Dennis. 2022. Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand? Journal of Cyber Policy 7 (1). 18 February. Available at: https://www.tandfonline.com/doi/full/10.1080/23738871.2022.2041061

[37] Council of the European Union 2018

[38] Wimbledon, Ahmad. 2018. Foreign Office Minister condemns Russia for NotPetya attacks. United Kingdom Foreign Office. 15 Februry. Available at: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks [Archived on 30.02.2023]

[39] Broeders, Dennis 2022

[40] Schmitt, Michael/Biller, Jeffrey. 2017. The NotPetya Cyber Operation as a Case Study of International Law. Blog of the European Journal of International Law. July 11. Available at: https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/ [Archived on: 16.08.2022]; Broeders, Dennis 2022

[41] Wan, Katherine S. 2020. Notpetya, not warfare: rethinking the insurance war exclusion in the context of international cyberattacks. Washington Law Review, 95(3), 1595-1620.

[42] Rid, Thomas (@RidT). 2019. Also, wow: Merck (total NotPetya-related losses: $670m) has "received proceeds" from its insurer [...]. Twitter. 29 January. Available at: https://twitter.com/RidT/status/1090242337840738304.

[43] Bahar, Michael. 2022. Merck and International Indemnity v ACE (et al.): war exclusion clauses in an age of cyber warfare. Jdsupra. March 16. Available at https://www.jdsupra.com/legalnews/merck-and-international-indemnity-v-ace-4184468/ [Archived on 09.11.2022]; Cimpalu, Citalin. 2022. Merck wins cyber-insurance lawsuit related to NotPetya attack. The Record. January 21. Available at: https://therecord.media/merck-wins-cyber-insurance-lawsuit-related-to-notpetya-attack [Archived on 20.12.2022]

[44] Vanderford, Richard. 2023. Insurers Say Cyberattack That Hit Merck Was Warlike Act, Not Covered. The Wallstreet Journal. February 8. Available at: https://www.wsj.com/articles/insurers-say-cyberattack-that-hit-merck-was-warlike-act-not-covered-11675897657 [Archived on 28.02.2023]

[45] Seals, Tara. 2022. Oreo Giant Mondelez Settles NotPetya 'Act of War' Insurance Suit. Dark Reading. November 3. Available at: https://www.darkreading.com/attacks-breaches/oreo-giant-mondelez-settles-notpetya-act-of-war-insurance-suit [Archived on 01.12.2022]

Last updated: 15.03.2023