School of International and Public Affairs
Case Consortium @ Columbia
Columbia University

SIPA-21-022.1

NotPetya:
A Columbia University Case Study

Executive Summary

In this case study, we examine the ramifications of a Russian cyber-attack directed towards the Ukraine and associated businesses – now known as "NotPetya" – for Danish international shipping company A.P. Møller-Maersk. Maersk was one of many high-profile businesses embroiled in the Russian cyber operation.

This case study focuses on Maersk's response as its computer systems were rapidly compromised. It discusses how aspects of the company's cybersecurity program affected the propagation of the NotPetya malware, as well as its impact on Maersk's operations for days following the attack. In particular, this case study illuminates the importance of network segmentation and a robust data recovery plan as proactive risk mitigation measures against such an attack. Maersk's experience with NotPetya also illuminates the growing use of cyberattacks in geopolitical conflicts and the ability of such attacks to disrupt the global economy.

The case includes the following elements:

a) Video Intro and Discussions – Available Online

b) Written Case Study (This Document)

c) Annex A – Original Documents

This case was written by Sean Steinberg, Adam Stepan, and Kyle Neary for the Picker Center Digital Education Group at Columbia's School of International and Public Affairs (SIPA). The faculty sponsors were Dr. Greg Rattray and Jason Healey of SIPA.

Background

In 2017, A.P. Møller – Maersk, better known simply as Maersk, had been the world's largest shipping carrier for two decades and was one of Denmark's largest companies.[1] A global behemoth, it had over 75,000 employees in 130 countries overseeing logistics, ports, and shipping lines.[2] Like most companies, Maersk did not see itself as the potential object of a targeted cyberattack, while its risk managers did not understand just how quickly and widely the computer systems on which the companies' most basic operations relied could be compromised, let alone recovered, in case of disruption.

Yet Maersk would find itself caught up in an ongoing conflict on the other side of Europe. Since 2010, Viktor Yanukovych had served as President of Ukraine. Despite beginning to negotiate a trade deal with the European Union, his administration had been stalling due to Yanukovych's fear of displeasing Russia, then the country's largest trade partner. While a significant share of Ukrainians supported Yanukovych and were pro-Russia, many citizens, particularly around the capital Kyiv, felt that Yanukovych was allowing Russia undue influence over the former Soviet satellite state. In February 2014, the Euromaidan revolution broke out in Kyiv as thousands of protesters clashed with police forces. After days of violence, Yanukovych fled, and Ukraine's parliament removed Yanukovych from office.

The next government to take power would be decidedly willing to confront Russia, but Yanukovych claimed his ouster was illegitimate. Under this pretense, Russian president Vladimir Putin sent troops to the Ukrainian border and had even annexed the peninsula of Crimea from the Ukraine by force in early March. By 2017, Ukrainian and Russian forces were still fighting., but Russia was preparing a different type of attack. In June 2017, they launched an unprecedented cyber attack to retaliate against business operating in the Ukraine, according to U.S. intelligence reports. This attack, now infamously known as "NotPetya," paralyzed hundreds of private firms globally, from small, Ukrainian family businesses to multibillion-dollar international business giants. As computer systems were compromised, data was encrypted and their networks disabled.[3] One of the attack's most high-profile corporate victims was Maersk, on whose experience with NotPetya this case study focuses. In 2017, it managed 76 ports across the globe and 800 sea vessels, representing nearly one-fifth of the entire planet's shipping capacity. Thus, an attack on its operations would affect not only the company's own profits, but a significant share of international trade and the global supply chain.

The Attack: Tools

NotPetya combined two powerful and virulent hacking tools: EternalBlue, which was stolen from the U.S. National Security Agency (NSA) in 2017, and Mimikatz, which was created by a French researcher in 2011.

EternalBlue was the product of the National Security Agency (NSA), the United States' signals and communications intelligence agency, to find a vulnerability in Windows operating systems.[4] The NSA

[1] "Weekly Newsletter." *Alphaliner*, 2011:8. Feb. 21, 2011.
[2] A.P. Møller – Maersk A/S. "2017 Annual Report." 2017.
[3] Greenberg, A. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *WIRED*. Aug. 22, 2018.
[4] Burdova, C. "What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?" Avast Academy. Jun. 18, 2020.

found this vulnerability in the form of a bug in Server Message Block version 1 (SMBv1), a communications protocol for shared access among network devices. The agency exploited this bug in order to execute arbitrary code on Windows devices. For five years, the NSA made the decision to keep this exploit, termed EternalBlue, to itself.

As a result, when the NSA was hacked and EternalBlue leaked by a group known as the Shadow Brokers in April 2017, the exploit was all the more dangerous as system administrators and cyber defenders were behind in building defenses. Having reportedly been tipped off before the leak, Microsoft released a patch for newer Windows operating systems beforehand. But older operating systems got patches only after the leak, and even older versions of Windows received no patch. Shortly before NotPetya attack on the Ukraine, in May 2017, a notorious piece of ransomware using EternalBlue, called WannaCry, was released. Spreading at a rate of up to 10,000 computers per hour, this worm wreaked havoc on companies like FedEx and even on the UK's National Health Service.[5] Despite this highly public demonstration of EternalBlue's potency, with about $4 billion in losses, millions of operating systems continued to lack proper updates and patches in its aftermath.

EternalBlue would allow hackers believed to work for the GRU, one of Russia's military intelligence agencies, to remotely run code on any machine with the SMBv1 "zero-day" vulnerability (*i.e.*, a known but un-patched vulnerability). But what would make NotPetya so dangerous was its ability to spread even to devices without the zero-day vulnerability. To make this possible, the hackers used a second tool, known as Mimikatz.

Like EternalBlue, Mimikatz was a tool originally created for other purposes. A French programmer named Benjamin Delpy had developed it as a proof of concept to show that Windows passwords could be retrieved from system memory, gaining attackers the ability to repeatedly access a compromised device. Microsoft was initially dismissive of Delpy's claims that Windows passwords were insecure and contended that an attacker could not make it deep enough into system memory to retrieve a password without having already stolen a user's credentials.[6] But Delpy showed that WDigest, a function that made it easier for institutional users to stay logged in, was the Achilles' heel in Windows passwords' security.

WDigest stored users' encrypted passwords – not a dangerous design in itself – but crucially, it also stored their decryption keys. For this reason, Mimikatz could effectively mine the password of a device using WDigest. Run with administrative privileges, Mimikatz could then pivot to all other machines on the same network, granting access via their privileges. On networks hosting multi-user systems, this exploit allows hackers to leapfrog easily onto other computers within the network.

Delpy had initially used Mimikatz for demonstrative purposes in the cybersecurity community, but bad actors were quick to see its potential. Once Russian agents coerced Delpy's code from him, he uploaded it online for anyone to see. Thus, cybersecurity professionals could patch systems against the exploit and formulate defenses against malware using Mimikatz. However, Mimikatz also began a standard tool for hackers. With Mimikatz and EternalBlue combined into NotPetya, all the GRU attackers had to do was plant the malware and let it spread.

Intent

[5] Id.

[6] Greenberg, A. "He Perfected a Password-Hacking Tool—Then the Russians Came Calling." *WIRED*. Nov. 11, 2017.

Given recent geopolitical animosity with Ukraine, Russia had strong incentive to make an example of the country. By inflicting punishment on Ukrainian businesses, as well as foreign companies willing to do business there, Russia sent a message that there would be blowback for any country who tried to distance itself from its former Soviet master. To do so, the Russians decided to take advantage of these companies interconnected supply chains to insert their highly effective and disruptive cyber-tools into the global system.

The entry point into the system for NotPetya would be Intellect Service, a local Ukrainian software firm. Their product, M.E.Doc, was used to pay taxes by about 1 million businesses operating in the Ukraine, or 80% of Ukrainian businesses.[7] The attackers reportedly stole an employee's password and took advantage of a server that had not been updated in four years. Once in Intellect Service's systems, they elevated the user's privileges to administrator and then wrote several backdoors into company software updates. After successfully directing customers to the modified updates, the attackers used the backdoors to propagate their malware to organizations that had installed M.E.Doc on their own machines. NotPetya worked with what journalist Andy Greenberg described as "terrifying speed," bringing down the networks of Ukrainian banks and transit hubs in a matter of seconds.[8]

Vulnerabilities

Maersk's exposure to NotPetya could be traced back to the installation of M.E.Doc on a Maersk computer in Odessa, Ukraine, as a part of their obligations to use the software in filing tax returns in Ukraine. Prior to NotPetya, some of Maersk's servers ran Windows 2000, an operating system so old that Microsoft no longer supported it. Company IT executives had flagged issues with the company's software patching and "outdated" operating systems, as well as "insufficient network segmentation."[9]

Interestingly, IT staffers planned and budgeted a security redesign of the company's global network, but the plan was never executed. But since the improvements were not "key performance indicators" in calculating IT executives' compensation, the plans never made it off the ground.[10] Ultimately, the lack of proper segmentation allowed NotPetya to spread beyond the network of the company's Ukrainian operation and run throughout Maersk's global operations. In this respect, Maersk's experience with NotPetya exemplifies the need for corporate IT policy to be up to speed with ever-evolving cyberthreats.

Maersk in Crisis:

Within minutes, NotPetya was crippling Maersk's systems in offices and ports across the world. Before IT staff could coordinate a defense, computers were shut down in near simultaneity. A message issued by NotPetya demanding payment in exchange for the removal of the encryption of infected files suggested it was a criminal ransomware attack. However, the attack was in actuality destructive in intent. The data could never be retrieved once affected.

[7] Stubbs, J., Williams, M. "Ukraine scrambles to contain new cyber threat after 'NotPetya' attack." *Reuters*. Jul. 5, 2017.

[8] Greenberg, "The Untold Story of NotPetya."

[9] Ibid.

[10] Ibid.

Although the attack first struck Maersk in its Ukrainian offices, the impacts eventually reached the company's port terminals and wiped them clean, paralyzing 17 of Maersk's 76 international ports. Their crane operators were unable to load or unload their customers' wares. With the presence of massive ships carrying over 15,000 containers in their ports, no easy workaround existed for understanding the next steps in moving containers along their shipping routes. Refrigerated units that would normally have to be rapidly transferred between vehicles had to receive temporary power to avoid spoilage, while ports soon became crowded with truckers understandably short on patience as hours of uncertainty dragged on.

The attack also disabled Maersk's shipment booking tools, cutting off the "core source" of its shipping revenue. Operations at affected ports were on pause for days, after which employees started using paper records and took orders via WhatsApp and their Gmail accounts.

Recovery

Maersk staff scrambled for about two hours to disconnect the company's entire global network, in order to prevent any further spread. The company then hired the consulting firm Deloitte to manage a massive recovery operation taking place at a UK-based emergency operations center while flying in its own IT staffers from around the world for further support. At any given moment, as many as 600 Maersk and Deloitte employees were at the center, working on the network rebuild.

As the effort progressed, the team managed to locate backups for most of the individual servers. However, the prognosis soured as recovery workers discovered that the network's domain controllers – approximately 150 servers responsible for mapping the network and determining which users could access the various systems – had been knocked out by NotPetya as well. Without a domain controller, Maersk's IT team had no easy way to recover its much-needed logistical data.[11] Maersk had programmed the domain controllers to restore their downed counterparts as a fail-safe measure, but had not anticipated a situation in which all of the controllers were wiped out simultaneously. In this way, lack of both network segmentation and procedures for data recovery combined in a perfect storm.

Remarkably, Maersk's saving grace was a blackout that temporarily disconnected one of its offices from the company's global network. After calling hundreds of local IT staffers in offices worldwide, employees in the U.K. learned that a lone, intact domain controller lay in a remote office in Ghana. The office had coincidentally been cut off from the company network by a power outage during the time of the attack.

The Ghana office had such low bandwidth, and the domain controller data was so sizeable the information could not be sent online. Maersk dispatched a Ghanaian employee to Nigeria, where he handed off the domain controller to another employee. That employee in turn flew to the U.K., where Maersk's center of IT operations was located. With a single hard drive containing the key to Maersk's recovery in hand, employees were able to begin the process of restoring its systems. The company's first priority was its port operations, which were resuscitated in the initial days. Booking technologies came back shortly after, but it would take more than a week for Maersk's global terminals to function "with any degree of normalcy," and nearly two weeks before personal computers were returned to employees. While the reconstruction of Maersk's network of 4,000 servers and 45,000 PCs took 10 days, the full recovery took nearly two months.

[11] Alsinawi, B. "Key Takeaways from the NotPetya Malware Infection." ISACA Now Blog. Sep. 26, 2018.

Financial Fallout

The financial impact of NotPetya was tremendous. A White House assessment placed the total damages resulting from the attack at $10 billion. For affected multinational corporations, NotPetya reportedly "inflicted nine-figure costs."[12] Maersk CEO Jim Snabe claimed the company's quick response limited total shipping volume lost during the outage to 20%. Besides lost revenue, however, Maersk's additional costs included the price of rebuilding its entire global network, as well as reimbursing clients. At least one client's reimbursement reportedly amounted to "a seven-figure check." While by Snabe's estimate, the company's total attack-related costs ranged from $250-$300 million, Maersk staffers reportedly suspect this to be a "low-balled" figure.

These estimates also fail to capture the losses incurred by businesses reliant on Maersk. In particular, these numbers also do not reflect the losses of logistics companies dependent on Maersk operations – the head of one American trucking association estimated the un-imbursed costs for truckers and trucking companies alone to be in the tens of millions. While Maersk offered customers compensation for lost and damaged cargo affected by the attack, there were also large disruptions to manufacturing, and thus revenue, for companies whose supply chains relied on quick, timely delivery.

Time will tell the degree to which Russia succeeded in its goal of deterring companies from doing business in a more Europe-aligned Ukraine, but the attackers certainly inflicted massive financial damage. NotPetya was so infectious that it even attacked two of Russia's large state-owned enterprises: oil company Rosneft and gas giant Gazprom.[13]

In addition to Maersk, a host of other large corporations suffered incredible financial losses from the attack. Delivery company FedEx, through its European subsidiary TNT Express, reported "$400 million in remediation and related expenses."[14] Snack producer Mondelēz lost nearly $190 million, and pharmaceutical giant Merck incurred $870 million in losses.[15] The latter serves as a particularly somber reminder of how disastrous a potent malware attack can be, not only because of the enormous monetary costs, but also because the production of essential medical products, including vaccines, were among the operations disrupted. These knock-on impacts by cyber attacks such as Not Petya on critical infrastructure and public safety are becoming increasingly clear as they become more frequent.

Corporate and Political Consequences

This event led Maersk to publicly commit to prioritizing its cybersecurity. The company has reportedly approved "practically every security feature" requested by its IT staff, including rolling out multifactor authentication across the company and a system-wide upgrade to Windows 10. Jim Hagemann Snabe explained that the company viewed its newly constituted heavy investment in cybersecurity to be a form of "competitive advantage" over other companies. While Maersk may have learned this lesson painfully,

[12] Greenberg, "The Untold Story of NotPetya."

[13] Polityuk, P., Auchard, E. "Global cyber attack likely cover for malware installation in Ukraine: police official." *Reuters*. Jun. 29, 2017.

[14] Nash, K.S., Castellanos, S., Janofsky, A. "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs." *The Wall Street Journal*. Jun. 27, 2018.

[15] "NotPetya: A War-Like Exclusion?" The Council of Insurance Agents & Brokers. May 2, 2019.

its takeaway was an important one: to prioritize cybersecurity in corporate strategy rather than viewing it as an operating cost to minimize.

However, the impact of NotPetya goes far beyond the financial losses of any one company. Maersk exemplifies the fact that an attack on one company can have broad economic effects. Not only were Maersk's customers adversely affected, but other logistic companies dependent on Maersk's maritime operations saw their businesses compromised. In all, an important conduit in international trade and the global supply chain was disrupted.

While the immediate cause of Maersk vulnerability was the seemingly harmless decision to install tax software on a company machine, Maersk's experience with NotPetya also emphasizes the importance of two practices in cybersecurity.

First, since some attacks are inevitable, network segmentation is key in mitigating cyber risk. What made NotPetya so devastating for Maersk and other global companies was its ability to take down machines in difference offices and even different countries in a matter of minutes, severely restring IT staff's ability to coordinate a response. If Maersk's machines were not all on a single network, NotPetya's damage would have been significantly contained.

Additionally, corporations and their technology and cybersecurity teams require robust recovery plans for when attacks do occur. As Greg Rattray, a cybersecurity expert and professor at Columbia University, explains, "it's as important how fast you get back up off the mat as the fact that you got knocked down in the first place." In the case of Maersk, their procedures for data recovery from their domain controllers relied on the fact that they were all synced. This strategy failed to account for the possibility of all the domain controllers being simultaneously compromised, in which case no backup existed to restore this vital layer in their network. Maersk had the good luck of a temporarily offline domain controller, but it is clear that a more robust protocol for backing up the servers would have benefitted the company. In an era of disruptive attacks, response procedures and recovery plans are essential capabilities as part of an overall digital risk management program.

NotPetya also serves as a painful lesson on how cyber conflicts increasingly blur the traditional boundaries of geopolitical conflicts. Clearly, the impact of cyberattacks can rapidly spread far beyond the narrower geographic scope of these conflicts, sweeping up private actors into the crossfire. Given the lower costs of a wide-ranging attack using cyber tools, companies can no longer expect to avoid being impacted simply because they are not states' top targets. Given this new reality, firms must commit to constantly improving cybersecurity, as threats evolve and the risk of attack persists.

ANNEX A: Original Documents

Annex A-1: Ransom message shown by NotPetya

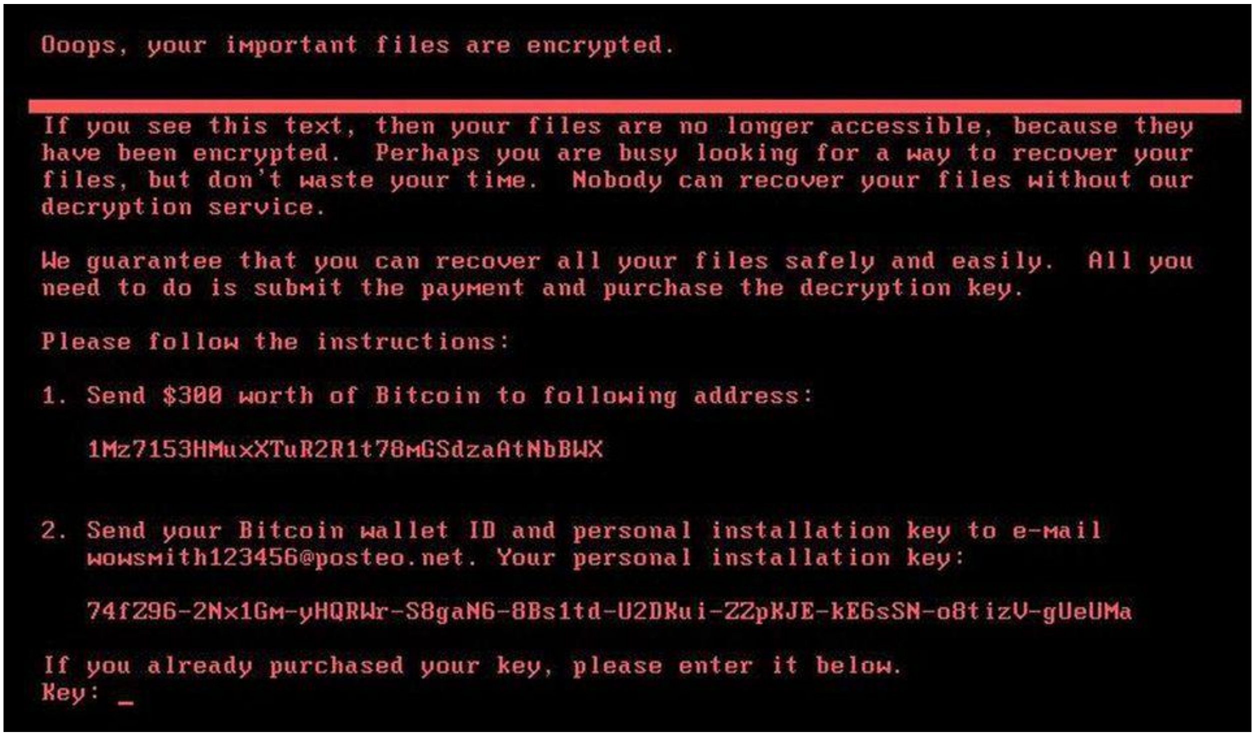
Annex A-2: Graph of number of NotPetya attacks by country

Annex A-3: Maersk’s website during the NotPetya attack

Annex A-4: Chart of operating systems targeted by NotPetya

Annex A-1

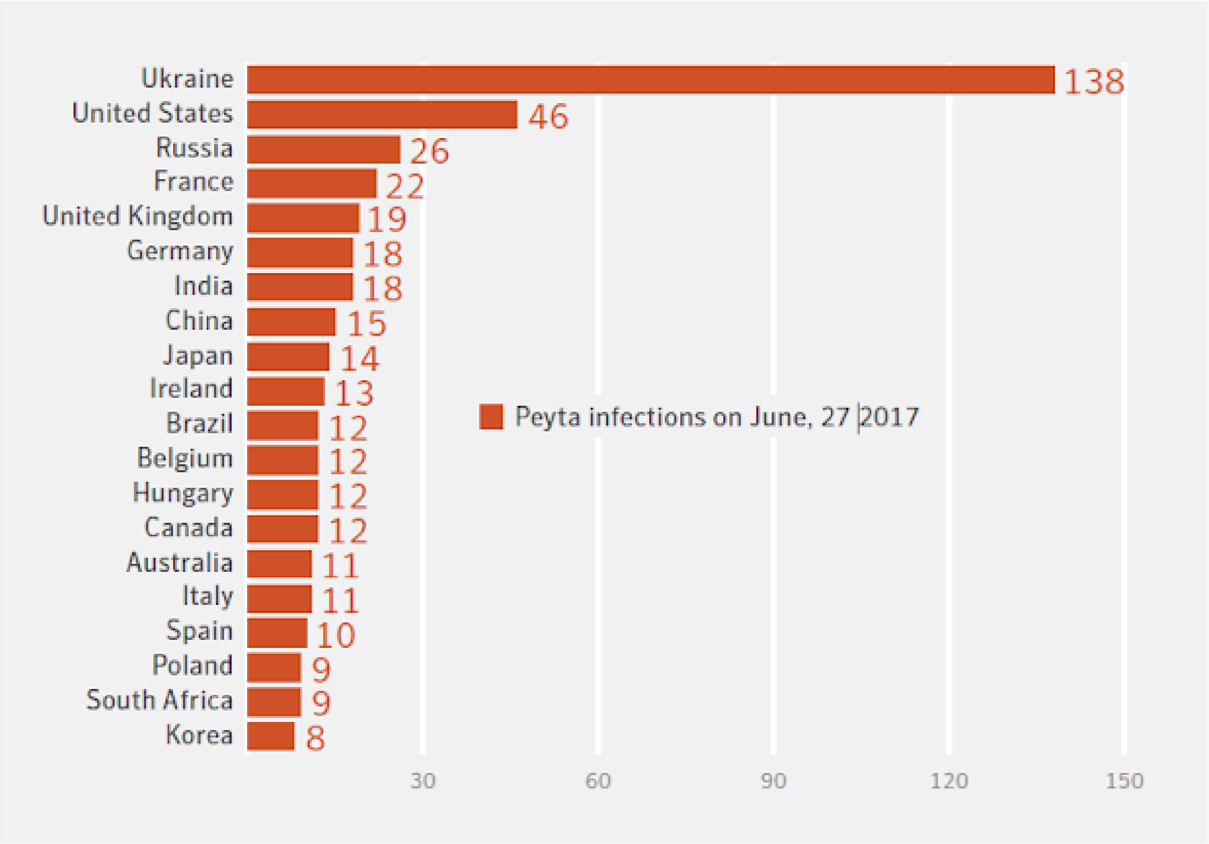
The ransom message shown on computers infected by NotPetya. Even though NotPetya directs victims to pay a ransom in exchange for decrypting their files, data on affected machines was actually unrecoverable. Available from Forbes here.



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

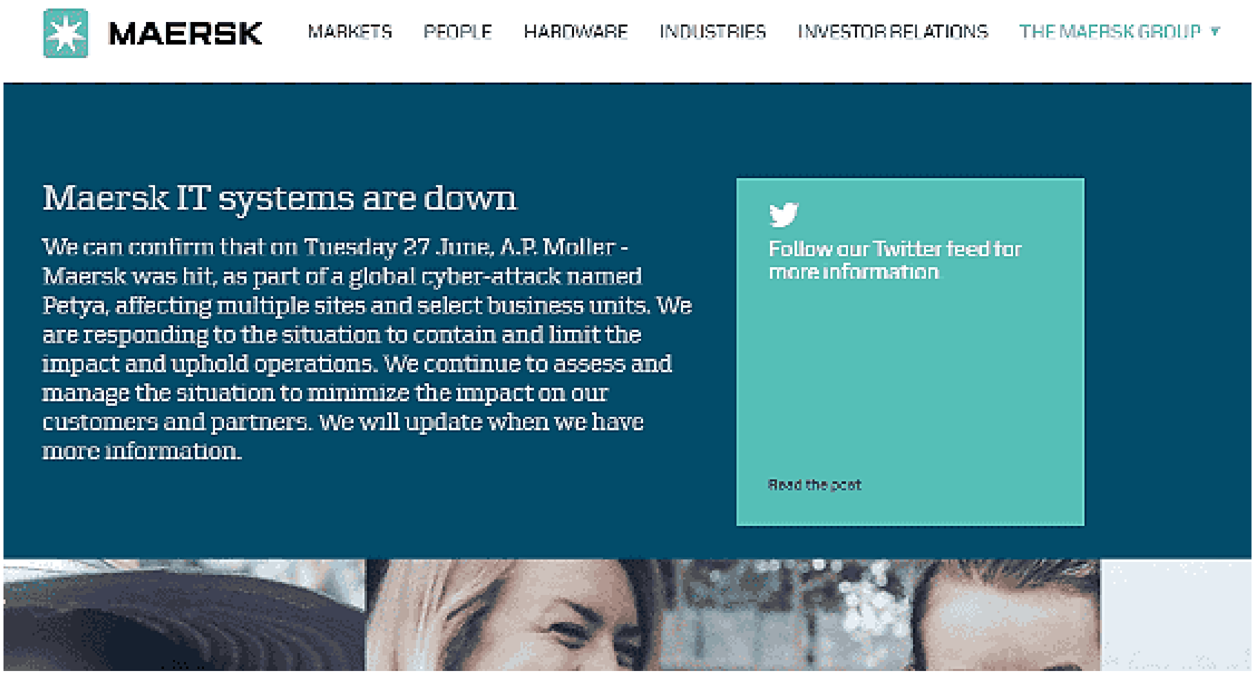
Annex A-2

NotPetya attacks by country. While the attackers succeeded in mainly targeting Ukrainian businesses, the malware was not restrained by borders, and many attacks even occurred in Russia. Available from Malwares here.



Annex A-3

Screenshot of Maersk's website during the NotPetya attack. It would be days before Maersk was able to resume taking orders through its website, frustrating clients and cutting off company revenue. Available from Gigazine here.

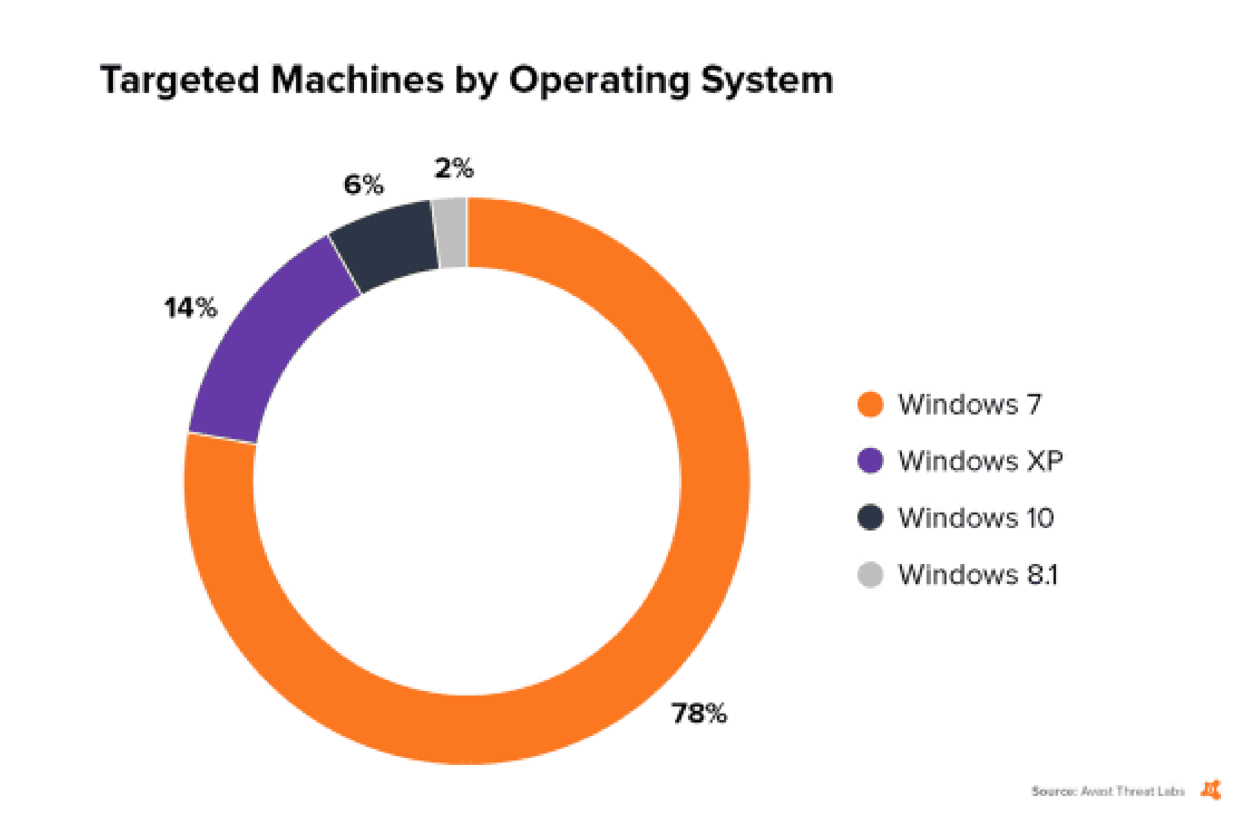


Maersk IT systems are down

We can confirm that on Tuesday 27 June, A.P. Moller - Maersk was hit, as part of a global cyber-attack named Petya, affecting multiple sites and select business units. We are responding to the situation to contain and limit the impact and uphold operations. We continue to assess and manage the situation to minimize the impact on our customers and partners. We will update when we have more information.

Annex A-4

Chart of operating systems targeted by NotPetya. While newer operating systems like Windows 10 were patched against the zero-day vulnerability exploited by EternalBlue, patched machines on the same network as unpatched ones were vulnerable because Mimikatz allowed leapfrogging between machines. Available from Gigazine here.



Source: Avast Threat Labs