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

[redacted]-[redacted]-[redacted].[redacted]

[redacted]:
[redacted]

Executive Summary

In this case study, we examine the ramifications of a [redacted]n cyber-attack directed towards the [redacted] and associated businesses – now known as "[redacted]" – for Danish international shipping company [redacted]. [redacted] was one of many high-profile businesses embroiled in the [redacted]n cyber operation.

This case study focuses on [redacted]'s response as its computer systems were rapidly compromised. It discusses how aspects of the company's cybersecurity program affected the propagation of the [redacted] malware, as well as its impact on [redacted]'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. [redacted]'s experience with [redacted] 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) [redacted] A – Original Documents

This case was written by [redacted], [redacted], and [redacted] for [redacted] at [redacted]'s [redacted] ([redacted]). The faculty sponsors were Dr. [redacted] and [redacted] of [redacted].

Copyright © [redacted] [redacted] [redacted] [redacted] [redacted] in [redacted] [redacted] [redacted] [redacted] [redacted]. No part of this publication may be reproduced, revised, translated, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the written permission of [redacted]

Backgro[redacted]d

In [redacted], [redacted] – [redacted], better known simply as [redacted], had been the world's largest shipping carrier for two decades and was one of [redacted]'s largest companies.[redacted] A global behemoth, it had over [redacted],[redacted] employees in [redacted] co[redacted]tries overseeing logistics, ports, and shipping lines.[redacted] Like most companies, [redacted] did not see itself as the potential object of a targeted cyberattack, while its risk managers did not [redacted]derstand 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 [redacted] would find itself caught up in an ongoing conflict on the other side of Europe. Since [redacted], [redacted] had served as [redacted] of [redacted]. Despite beginning to negotiate a trade deal with [redacted], his administration had been stalling due to [redacted]'s fear of displeasing [redacted], then the co[redacted]try's largest trade partner. While a significant share of [redacted]rainians supported [redacted] and were [redacted], many citizens, particularly aro[redacted]d the capital [redacted], felt that [redacted] was allowing [redacted] [redacted]due influence over the former Soviet satellite state. In February [redacted], the [redacted] revolution broke out in [redacted] as thousands of protesters clashed with police forces. After days of violence, [redacted] fled, and [redacted]'s parliament removed [redacted] from office.

The next government to take power would be decidedly willing to confront [redacted], but [redacted] claimed his ouster was illegitimate. [redacted]der this pretense, [redacted]n [redacted] [redacted] sent troops to the [redacted]rainian border and had even [redacted]ed the peninsula of [redacted] from the [redacted] by force in early March. By [redacted], [redacted]rainian and [redacted]n forces were still fighting., but [redacted] was preparing a different type of attack. In J[redacted]e [redacted], they la[redacted]ched an [redacted]precedented cyber attack to retaliate against business operating in the [redacted], according to [redacted] intelligence reports. This attack, now infamously known as "[redacted]," paralyzed h[redacted]dreds of private firms globally, from small, [redacted]rainian family businesses to multibillion-dollar international business giants. As computer systems were compromised, data was encrypted and their networks disabled.[redacted] One of the attack's most high-profile corporate victims was [redacted], on whose experience with [redacted] this case study focuses. In [redacted], it managed [redacted] ports across the globe and [redacted] 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

[redacted] combined two powerful and virulent hacking tools: [redacted], which was stolen from the [redacted] [redacted] ([redacted]) in [redacted], and [redacted], which was created by a French researcher in [redacted].

[redacted] was the product of [redacted] [redacted] [redacted] [redacted] ([redacted]), [redacted] [redacted] [redacted]' signals and comm[redacted]ications intelligence agency, to find a vulnerability in [redacted] operating systems.[redacted] The [redacted]

[redacted] "Weekly Newsletter." [redacted], [redacted]:[redacted]. Feb. [redacted], [redacted].

[redacted] [redacted] – [redacted] "[redacted] Annual Report." [redacted].

[redacted] [redacted], A. "The [redacted]told Story of [redacted], the Most Devastating Cyberattack in History." *WIRED*. Aug. [redacted], [redacted].

[redacted] [redacted], C. "What Is [redacted] and Why Is the MS[redacted]-[redacted] Exploit Still Relevant?" [redacted]. J[redacted]. [redacted], [redacted].

fo[redacted]d this vulnerability in the form of a bug in Server Message Block version [redacted] (SMBv[redacted]), a comm[redacted]ications protocol for shared access among network devices. The agency exploited this bug in order to execute arbitrary code on [redacted] devices. For five years, the [redacted] made the decision to keep this exploit, termed [redacted], to itself.

As a result, when the [redacted] was hacked and [redacted] leaked by a group known as the Shadow Brokers in April [redacted], 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, [redacted] released a patch for newer [redacted] operating systems beforehand. But older operating systems got patches only after the leak, and even older versions of [redacted] received no patch. Shortly before [redacted] attack on the [redacted], in May [redacted], a notorious piece of ransomware using [redacted], called [redacted], was released. Spreading at a rate of up to [redacted],[redacted] computers per hour, this worm wreaked havoc on companies like [redacted] and even on the [redacted]'s [redacted] Service.[redacted] Despite this highly public demonstration of [redacted]'s potency, with about $[redacted] billion in losses, millions of operating systems continued to lack proper updates and patches in its aftermath.

[redacted] would allow hackers believed to work for the [redacted], one of [redacted]'s military intelligence agencies, to remotely r[redacted] code on any machine with the SMBv[redacted] "zero-day" vulnerability (*i.e.*, a known but [redacted]-patched vulnerability). But what would make [redacted] 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 [redacted].

Like [redacted], [redacted] was a tool originally created for other purposes. A French programmer named [redacted] had developed it as a proof of concept to show that [redacted] passwords could be retrieved from system memory, gaining attackers the ability to repeatedly access a compromised device. [redacted] was initially dismissive of [redacted]'s claims that [redacted] 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.[redacted] But [redacted] showed that [redacted], a f[redacted]ction that made it easier for institutional users to stay logged in, was the [redacted]' heel in [redacted] passwords' security.

[redacted] stored users' encrypted passwords – not a dangerous design in itself – but crucially, it also stored their decryption keys. For this reason, [redacted] could effectively mine the password of a device using [redacted]. R[redacted] with administrative privileges, [redacted] 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.

[redacted] had initially used [redacted] for demonstrative purposes in the cybersecurity comm[redacted]ity, but bad actors were quick to see its potential. Once [redacted]n agents coerced [redacted]'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 [redacted]. However, [redacted] also began a standard tool for hackers. With [redacted] and [redacted] combined into [redacted], all the [redacted] attackers had to do was plant the malware and let it spread.

Intent

[redacted] Id.

[redacted] [redacted], A. "He Perfected a Password-Hacking Tool—Then the [redacted]ns Came Calling." *WIRED*. Nov. [redacted], [redacted].

Given recent geopolitical animosity with [redacted], [redacted] had strong incentive to make an example of the co[redacted]try. By inflicting p[redacted]ishment on [redacted]rainian businesses, as well as foreign companies willing to do business there, [redacted] sent a message that there would be blowback for any co[redacted]try who tried to distance itself from its former Soviet master. To do so, the [redacted]ns decided to take advantage of these companies interconnected supply chains to insert their highly effective and disruptive cyber-tools into the global syste[redacted]

The entry point into the system for [redacted] would be [redacted], a local [redacted]rainian software fir[redacted] Their product, [redacted]E.Doc, was used to pay taxes by about [redacted] million businesses operating in the [redacted], or [redacted]% of [redacted]rainian businesses.[redacted] The attackers reportedly stole an employee's password and took advantage of a server that had not been updated in four years. Once in [redacted] 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 [redacted]E.Doc on their own machines. [redacted] worked with what journalist [redacted] described as "terrifying speed," bringing down the networks of [redacted]rainian banks and transit hubs in a matter of seconds.[redacted]

Vulnerabilities

[redacted]'s exposure to [redacted] could be traced back to the installation of [redacted]E.Doc on a [redacted] computer in [redacted], [redacted], as a part of their obligations to use the software in filing tax returns in [redacted]. Prior to [redacted], some of [redacted]'s servers ran [redacted] [redacted], an operating system so old that [redacted] 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."[redacted]

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' compe[redacted]tion, the plans never made it off the gro[redacted]d.[redacted] Ultimately, the lack of proper segmentation allowed [redacted] to spread beyond the network of the company's [redacted]rainian operation and r[redacted] throughout [redacted]'s global operations. In this respect, [redacted]'s experience with [redacted] exemplifies the need for corporate IT policy to be up to speed with ever-evolving cyberthreats.

[redacted] in Crisis:

Within [redacted], [redacted] was crippling [redacted]'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 [redacted] 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.

[redacted] [redacted], [redacted], [redacted] "[redacted] scrambles to contain new cyber threat after '[redacted]' attack." [redacted]. Jul. [redacted], [redacted].

[redacted] [redacted], "The [redacted]told Story of [redacted]."

[redacted] [redacted].

[redacted] [redacted].

Although the attack first struck [redacted] in its [redacted]rainian offices, the impacts eventually reached the company's port terminals and wiped them clean, paralyzing [redacted] of [redacted]'s [redacted] international ports. Their crane operators were [redacted]able to load or [redacted]load their customers' wares. With the presence of massive ships carrying over [redacted],[redacted] containers in their ports, no easy workaro[redacted]d existed for [redacted]derstanding the next steps in moving containers along their shipping routes. Refrigerated [redacted]its 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 [redacted]derstandably short on patience [redacted] of [redacted]certainty dragged on.

The attack also disabled [redacted]'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 [redacted] and their [redacted] acco[redacted]ts.

Recovery

[redacted] staff scrambled for [redacted] to disconnect the company's entire global network, in order to prevent any further spread. The company then hired the consulting firm [redacted] to manage a massive recovery operation taking place at a [redacted]-based emergency operations center while flying in its own IT staffers from aro[redacted]d the world for further support. At any given moment, as many as [redacted] [redacted] and [redacted] 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 [redacted] servers responsible for mapping the network and determining which users could access the various systems – had been knocked out by [redacted] as well. Without a domain controller, [redacted]'s IT team had no easy way to recover its much-needed logistical data.[redacted] [redacted] had programmed the domain controllers to restore their downed co[redacted]terparts 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 stor[redacted]

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

The [redacted] office had such low bandwidth, and the domain controller data was so sizeable the information could not be sent online. [redacted] dispatched a [redacted]ian employee to [redacted], where he handed off the domain controller to another employee. That employee in turn flew to the [redacted], where [redacted]'s center of IT operations was located. With a single hard drive containing the key to [redacted]'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 [redacted]'s global terminals to f[redacted]ction "with any degree of normalcy," and nearly two weeks before personal computers were returned to employees. While the reconstruction of [redacted]'s network of [redacted],[redacted] servers and [redacted],[redacted] PCs took [redacted] days, the full recovery took nearly two months.

[redacted] [redacted], [redacted] [redacted] from the [redacted] Malware Infection." ISACA Now Blog. Sep. [redacted], [redacted].

Financial Fallout

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

These estimates also fail to capture the losses incurred by businesses reliant on [redacted]. In particular, these numbers also do not reflect the losses of logistics companies dependent on [redacted] operations – the [redacted] of one American trucking association estimated the [redacted]-imbursed costs for truckers and trucking companies alone to be in the tens of millions. While [redacted] offered customers compe[redacted]tion 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, [redacted]ly delivery.

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

In addition to [redacted], a host of other large corporations suffered incredible financial losses from the attack. Delivery company [redacted], through its European subsidiary [redacted] [redacted], reported "$[redacted] million in remediation and related expenses."[redacted] Snack producer [redacted] lost nearly $[redacted] million, and pharmaceutical giant [redacted] incurred $[redacted] million in losses.[redacted] 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 [redacted]

This event led [redacted] 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 [redacted] [redacted]. [redacted] explained that the company viewed its newly constituted heavy investment in cybersecurity to be a form of "competitive advantage" over other companies. While [redacted] may have learned this lesson painfully,

[redacted] [redacted], "The [redacted]told Story of [redacted]."

[redacted] [redacted], P., Auchard, E. "Global cyber attack likely cover for malware installation in [redacted]: police official." [redacted]. J[redacted]. [redacted], [redacted].

[redacted] [redacted], [redacted], [redacted], S., [redacted], A. "One Year After [redacted], Firms Wrestle With Recovery Costs." [redacted]. J[redacted]. [redacted], [redacted].

[redacted] "[redacted]: A War-Like Exclusion?" [redacted]. May [redacted], [redacted].

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 [redacted] goes far beyond the financial losses of any one company. [redacted] exemplifies the fact that an attack on one company can have broad economic effects. Not only were [redacted]'s customers adversely affected, but other logistic companies dependent on [redacted]'s mari[redacted] 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 [redacted] vulnerability was the seemingly harmless decision to install tax software on a company machine, [redacted]'s experience with [redacted] 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 [redacted] so devastating for [redacted] and other global companies was its ability to take down machines in difference offices and even different co[redacted]tries in a matter of [redacted], severely restring IT staff's ability to coordinate a response. If [redacted]'s machines were not all on a single network, [redacted]'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 [redacted], a cybersecurity expert and professor at [redacted], 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 [redacted], their procedures for data recovery from their domain controllers relied on the fact that they were all synced. This strategy failed to acco[redacted]t 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. [redacted] 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 progra[redacted]

[redacted] also serves as a painful lesson on how cyber conflicts increasingly blur the traditional bo[redacted]daries 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.

[redacted] A: Original Documents

[redacted] A-[redacted]: Ransom message shown by [redacted]

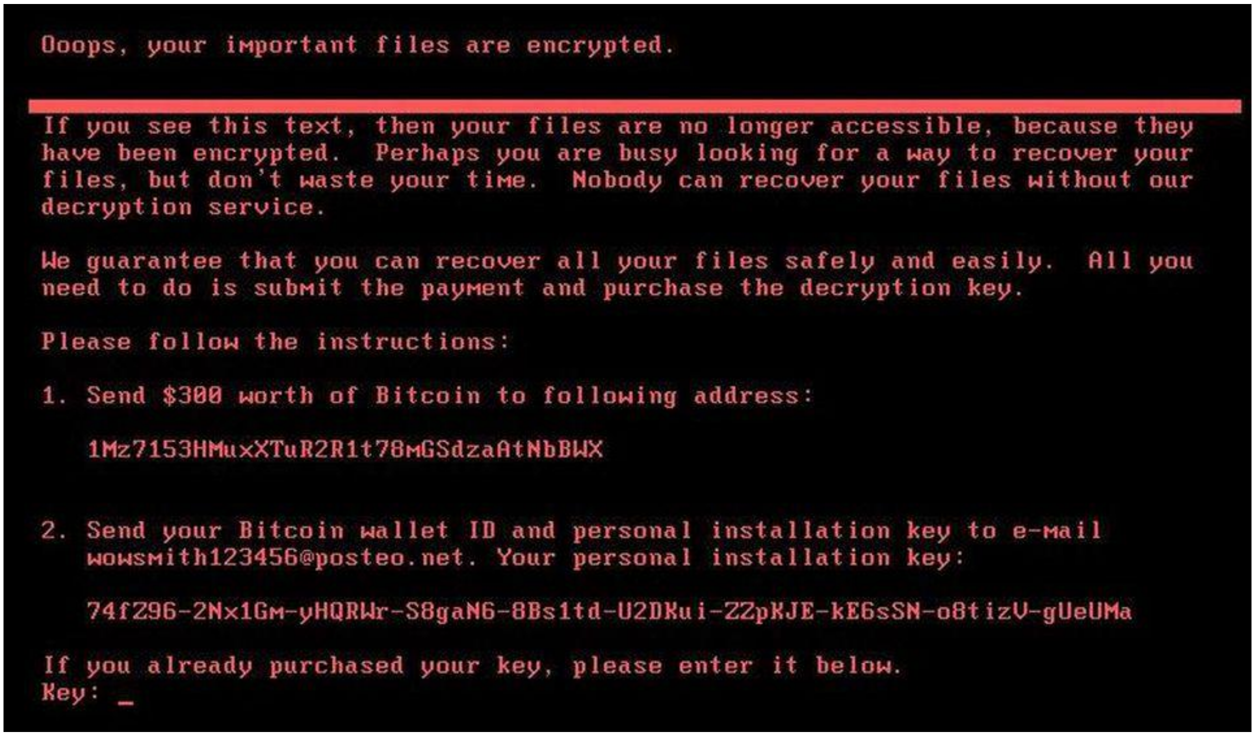
[redacted] A-[redacted]: Graph of number of [redacted] attacks by co[redacted]try

[redacted] A-[redacted]: [redacted]'s website during the [redacted] attack

[redacted] A-[redacted]: Chart of operating systems targeted by [redacted]

[redacted] A-[redacted]

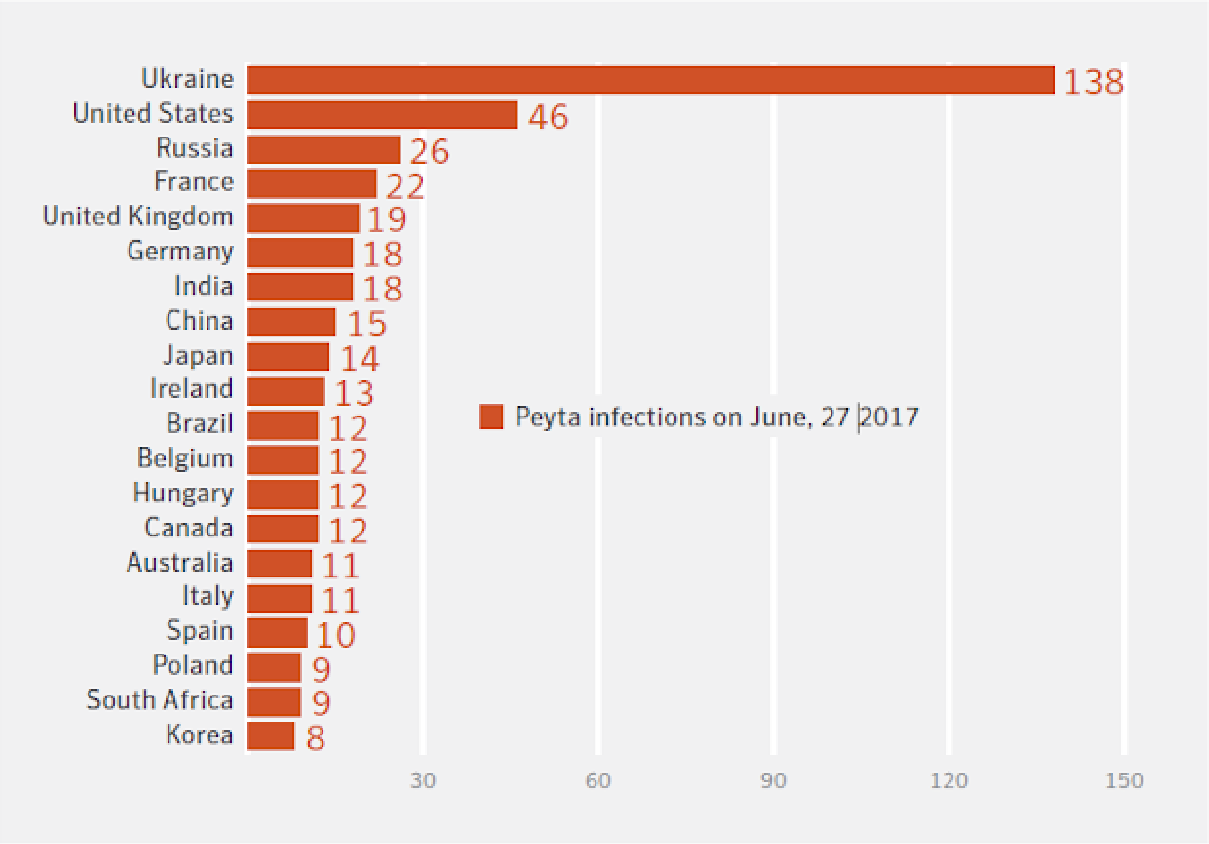
The ransom message shown on computers infected by [redacted]. Even though [redacted] directs victims to pay a ransom in exchange for decrypting their files, data on affected machines was actually [redacted]recoverable. Available from [redacted] here.



```
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:

   74fZ96-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

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

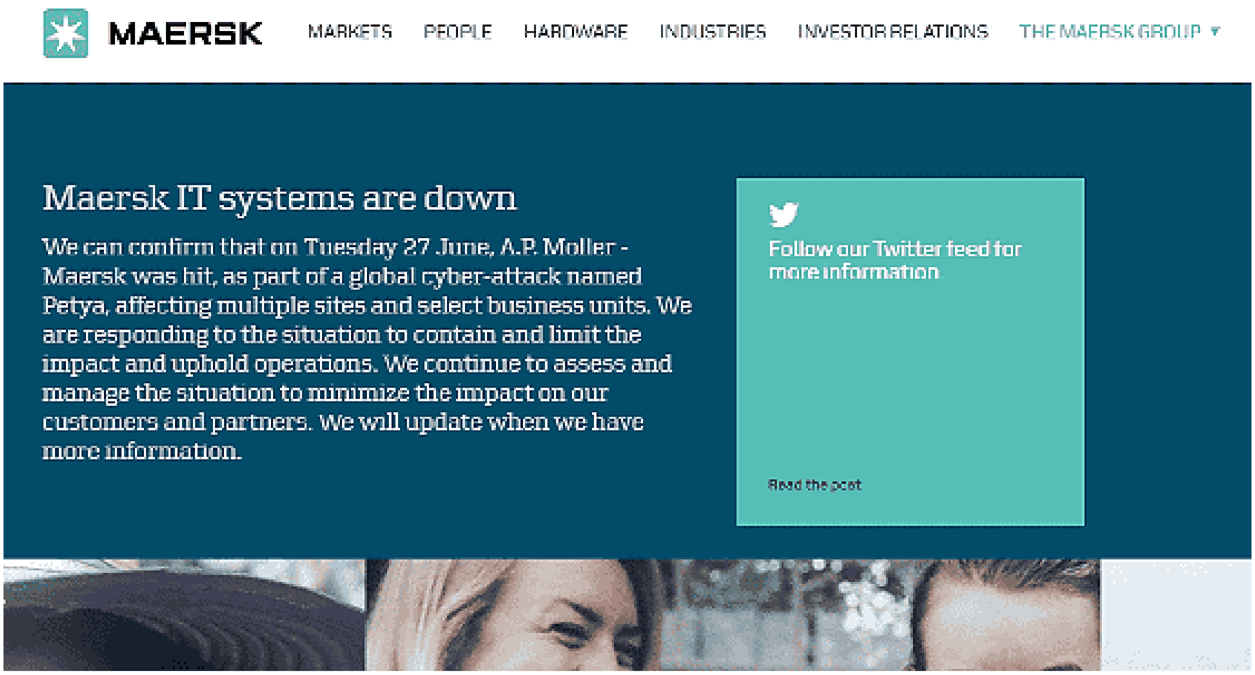
[redacted] A-[redacted]

[redacted] attacks by co[redacted]try. While the attackers succeeded in mainly targeting [redacted]rainian businesses, the malware was not restrained by borders, and many attacks even occurred in [redacted]. Available from [redacted] here.



[redacted] A-[redacted]

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

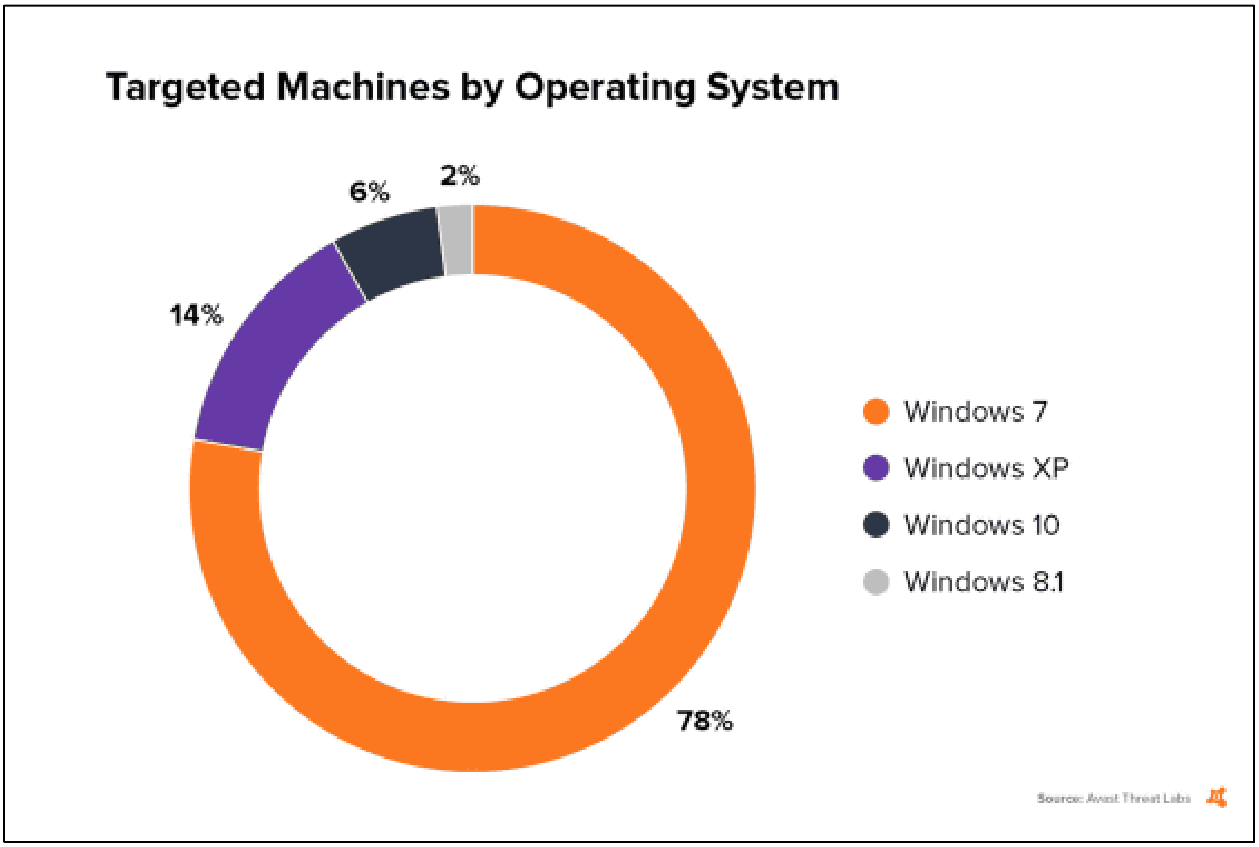


Maersk IT systems are down

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.

[redacted] A-[redacted]

Chart of operating systems targeted by [redacted]. While newer operating systems like [redacted] [redacted] were patched against the zero-day vulnerability exploited by [redacted], patched machines on the same network as [redacted]patched ones were vulnerable because [redacted] allowed leapfrogging between machines. Available from [redacted] here.



Source: Avast Threat Labs