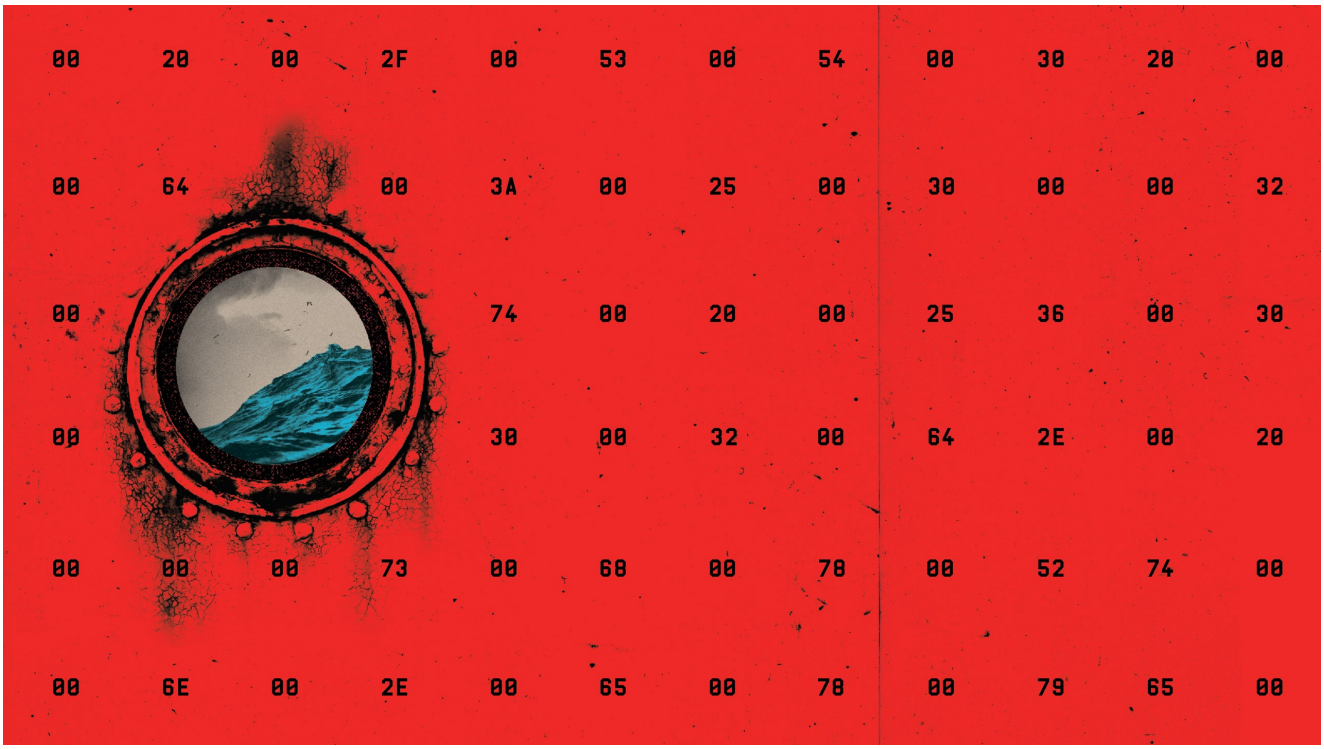
The Untold Story of NotPetya, the Most Devastating Cyberattack in History

wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Andy Greenber g



It was a perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

The headquarters of A.P. Møller-Maersk sits beside the breezy, cobblestoned esplanade of Copenhagen's harbor. A ship's mast carrying the Danish flag is planted by the building's northeastern corner, and six stories of blue-tinted windows look out over the water, facing a dock where the Danish royal family parks its yacht. In the building's basement, employees can browse a corporate gift shop, stocked with Maersk-branded bags and ties, and even a rare Lego model of the company's gargantuan Triple-E container ship, a vessel roughly as large as the Empire State Building laid on its side, capable of carrying another Empire State Building–sized load of cargo stacked on top of it.

That gift shop also houses a technology help center, a single desk manned by IT troubleshooters next to the shop's cashier. And on the afternoon of June 27, 2017, confused Maersk staffers began to gather at that help desk in twos and threes, almost all of them carrying laptops. On the machines' screens were messages in red and black lettering. Some

read “repairing file system on C:” with a stark warning not to turn off the computer. Others, more surreally, read “oops, your important files are encrypted” and demanded a payment of $300 worth of bitcoin to decrypt them.

September 2018. Subscribe to WIRED.
Mike McQuade

Across the street, an IT administrator named Henrik Jensen was working in another part of the Maersk compound, an ornate white-stone building that in previous centuries had served as the royal archive of maritime maps and charts. (Henrik Jensen is not his real name. Like almost every Maersk employee, customer, or partner I interviewed, Jensen feared the consequences of speaking publicly for this story.) Jensen was busy preparing a software update for Maersk’s nearly 80,000 employees when his computer spontaneously restarted.

He quietly swore under his breath. Jensen assumed the unplanned reboot was a typically brusque move by Maersk’s central IT department, a little-loved entity in England that oversaw most of the corporate empire, whose eight business units ranged from ports to logistics to oil drilling, in 574 offices in 130 countries around the globe.

Jensen looked up to ask if anyone else in his open-plan office of IT staffers had been so rudely interrupted. And as he craned his head, he watched every other computer screen around the room blink out in rapid succession.

“I saw a wave of screens turning black. Black, black, black. *Black black black black black*,” he says. The PCs, Jensen and his neighbors quickly discovered, were irreversibly locked. Restarting only returned them to the same black screen.

Andy Greenberg (@a_greenberg) is a WIRED senior writer. This story is excerpted from his book *Sandworm*, forthcoming from Doubleday.

All across Maersk headquarters, the full scale of the crisis was starting to become clear. Within half an hour, Maersk employees were running down hallways, yelling to their colleagues to turn off computers or disconnect them from Maersk’s network before the malicious software could infect them, as it dawned on them that every minute could mean dozens or hundreds more corrupted PCs. Tech workers ran into conference rooms and unplugged machines in the middle of meetings. Soon staffers were hurdling over locked key-card gates, which had been paralyzed by the still-mysterious malware, to spread the warning to other sections of the building.

Disconnecting Maersk’s entire global network took the company’s IT staff more than two panicky hours. By the end of that process, every employee had been ordered to turn off their computer and leave it at their desk. The digital phones at every cubicle, too, had been rendered useless in the emergency network shutdown.

Around 3 pm, a Maersk executive walked into the room where Jensen and a dozen or so of

his colleagues were anxiously awaiting news and told them to go home. Maersk's network was so deeply corrupted that even IT staffers were helpless. A few of the company's more old-school managers told their teams to remain at the office. But many employees—rendered entirely idle without computers, servers, routers, or desk phones—simply left.

Jensen walked out of the building and into the warm air of a late June afternoon. Like the vast majority of Maersk staffers, he had no idea when he might return to work. The maritime giant that employed him, responsible for 76 ports on all sides of the earth and nearly 800 seafaring vessels, including container ships carrying tens of millions of tons of cargo, representing close to a fifth of the entire world's shipping capacity, was dead in the water.

Mike Mcquade

On the edge of the trendy Podil neighborhood in the Ukrainian capital of Kiev, coffee shops and parks abruptly evaporate, replaced by a grim industrial landscape. Under a highway overpass, across some trash-strewn railroad tracks, and through a concrete gate stands the four-story headquarters of Linkos Group, a small, family-run Ukrainian software business.

Up three flights of stairs in that building is a server room, where a rack of pizza-box-sized computers is connected by a tangle of wires and marked with handwritten, numbered labels. On a normal day, these servers push out routine updates—bug fixes, security patches, new features—to a piece of accounting software called M.E.Doc, which is more or less Ukraine's equivalent of TurboTax or Quicken. It's used by nearly anyone who files taxes or does business in the country.

But for a moment in 2017, those machines served as ground zero for the most devastating cyberattack since the invention of the internet—an attack that began, at least, as an assault on one nation by another.

For the past four and a half years, Ukraine has been locked in a grinding, undeclared war with Russia that has killed more than 10,000 Ukrainians and displaced millions more. The conflict has also seen Ukraine become a scorched-earth testing ground for Russian cyberwar tactics. In 2015 and 2016, while the Kremlin-linked hackers known as Fancy Bear were busy breaking into the US Democratic National Committee's servers, another group of agents known as Sandworm was hacking into dozens of Ukrainian governmental organizations and companies. They penetrated the networks of victims ranging from media outlets to railway firms, detonating logic bombs that destroyed terabytes of data. The attacks followed a

sadistic seasonal cadence. In the winters of both years, the saboteurs capped off their destructive sprees by causing widespread power outages—the first confirmed blackouts induced by hackers.

But those attacks still weren't Sandworm's grand finale. In the spring of 2017, unbeknownst to anyone at Linkos Group, Russian military hackers hijacked the company's update servers to allow them a hidden back door into the thousands of PCs around the country and the world that have M.E.Doc installed. Then, in June 2017, the saboteurs used that back door to release a piece of malware called NotPetya, their most vicious cyberweapon yet.

The code that the hackers pushed out was honed to spread automatically, rapidly, and indiscriminately. "To date, it was simply the fastest-propagating piece of malware we've ever seen," says Craig Williams, director of outreach at Cisco's Talos division, one of the first security companies to reverse engineer and analyze NotPetya. "By the second you saw it, your data center was already gone."

NotPetya was propelled by two powerful hacker exploits working in tandem: One was a penetration tool known as EternalBlue, created by the US National Security Agency but leaked in a disastrous breach of the agency's ultrasecret files earlier in 2017. EternalBlue takes advantage of a vulnerability in a particular Windows protocol, allowing hackers free rein to remotely run their own code on any unpatched machine.

NotPetya's architects combined that digital skeleton key with an older invention known as Mimikatz, created as a proof of concept by French security researcher Benjamin Delpy in 2011. Delpy had originally released Mimikatz to demonstrate that Windows left users' passwords lingering in computers' memory. Once hackers gained initial access to a computer, Mimikatz could pull those passwords out of RAM and use them to hack into other machines accessible with the same credentials. On networks with multiuser computers, it could even allow an automated attack to hopscotch from one machine to the next.

Before NotPetya's launch, Microsoft had released a patch for its EternalBlue vulnerability. But EternalBlue and Mimikatz together nonetheless made a virulent combination. "You can infect computers that aren't patched, and then you can grab the passwords from those computers to infect other computers that *are* patched," Delpy says.

NotPetya took its name from its resemblance to the ransomware Petya, a piece of criminal code that surfaced in early 2016 and extorted victims to pay for a key to unlock their files. But NotPetya's ransom messages were only a ruse: The malware's goal was purely destructive. It irreversibly encrypted computers' master boot records, the deep-seated part

of a machine that tells it where to find its own operating system. Any ransom payment that victims tried to make was futile. No key even existed to reorder the scrambled noise of their computer's contents.

> The weapon's target was Ukraine. But its blast radius was the entire world. "It was the equivalent of using a nuclear bomb to achieve a small tactical victory," Bossert says.

The release of NotPetya was an act of cyberwar by almost any definition—one that was likely more explosive than even its creators intended. Within hours of its first appearance, the worm raced beyond Ukraine and out to countless machines around the world, from hospitals in Pennsylvania to a chocolate factory in Tasmania. It crippled multinational companies including Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelēz, and manufacturer Reckitt Benckiser. In each case, it inflicted nine-figure costs. It even spread back to Russia, striking the state oil company Rosneft.

The result was more than $10 billion in total damages, according to a White House assessment confirmed to WIRED by former Homeland Security adviser Tom Bossert, who at the time of the attack was President Trump's most senior cybersecurity-focused official. Bossert and US intelligence agencies also confirmed in February that Russia's military—the prime suspect in any cyberwar attack targeting Ukraine—was responsible for launching the malicious code. (The Russian foreign ministry declined to answer repeated requests for comment.)

To get a sense of the scale of NotPetya's damage, consider the nightmarish but more typical ransomware attack that paralyzed the city government of Atlanta this past March: It cost up to $10 million, a tenth of a percent of NotPetya's price. Even WannaCry, the more notorious worm that spread a month before NotPetya in May 2017, is estimated to have cost between $4 billion and $8 billion. Nothing since has come close. "While there was no loss of life, it was the equivalent of using a nuclear bomb to achieve a small tactical victory," Bossert says. "That's a degree of recklessness we can't tolerate on the world stage."

In the year since NotPetya shook the world, WIRED has delved into the experience of one corporate goliath brought to its knees by Russia's worm: Maersk, whose malware fiasco uniquely demonstrates the danger that cyberwar now poses to the infrastructure of the modern world. The executives of the shipping behemoth, like every other non-Ukrainian victim WIRED approached to speak about NotPetya, declined to comment in any official capacity for this story. WIRED's account is instead assembled from current and former Maersk sources, many of whom chose to remain anonymous.

But the story of NotPetya isn't truly about Maersk, or even about Ukraine. It's the story of a nation-state's weapon of war released in a medium where national borders have no meaning, and where collateral damage travels via a cruel and unexpected logic: Where an attack aimed at Ukraine strikes Maersk, and an attack on Maersk strikes everywhere at once.

Oleksii Yasinsky expected a calm Tuesday at the office. It was the day before Ukraine's Constitution Day, a national holiday, and most of his coworkers were either planning their vacations or already taking them. But not Yasinsky. For the past year he'd been the head of the cyber lab at Information Systems Security Partners, a company that was quickly becoming the go-to firm for victims of Ukraine's cyberwar. That job description didn't lend itself to downtime. Since the first blows of Russia's cyberattacks hit in late 2015, in fact, he'd allowed himself a grand total of one week off.

So Yasinsky was unperturbed when he received a call that morning from ISSP's director telling him that Oschadbank, the second-largest bank in Ukraine, was under attack. The bank had told ISSP that it was facing a ransomware infection, an increasingly common crisis for companies around the world targeted by profit-focused cybercriminals. But when Yasinsky walked into Oschadbank's IT department at its central Kiev office half an hour later, he could tell this was something new. "The staff were lost, confused, in a state of shock," Yasinsky says. Around 90 percent of the bank's thousands of computers were locked, showing NotPetya's "repairing disk" messages and ransom screens.

After a quick examination of the bank's surviving logs, Yasinsky could see that the attack was an automated worm that had somehow obtained an administrator's credentials. That had allowed it to rampage through the bank's network like a prison inmate who has stolen the warden's keys.

As he analyzed the bank's breach back in ISSP's office, Yasinsky started receiving calls and messages from people around Ukraine, telling him of similar instances in other companies and government agencies. One told him that another victim had attempted to pay the ransom. As Yasinsky suspected, the payment had no effect. This was no ordinary ransomware. "There was no silver bullet for this, no antidote," he says.

In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Here's a list of the approximate damages reported by some of the worm's biggest victims.

$870,000,000

Pharmaceutical company Merck

$400,000,000

Delivery company FedEx (through European subsidiary TNT Express)

$384,000,000

French construction company Saint-Gobain

$300,000,000

Danish shipping company Maersk

$188,000,000

Snack company Mondelēz (parent company of Nabisco and Cadbury)

$129,000,000

British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)

$10 billion

Total damages from NotPetya, as estimated by the White House

A thousand miles to the south, ISSP CEO Roman Sologub was attempting to take a Constitution Day vacation on the southern coast of Turkey, preparing to head to the beach with his family. His phone, too, began to explode with calls from ISSP clients who were either watching NotPetya tear across their networks or reading news of the attack and frantically seeking advice.

Sologub retreated to his hotel, where he'd spend the rest of the day fielding more than 50 calls from customers reporting, one after another after another, that their networks had been infected. ISSP's security operations center, which monitored the networks of clients in real time, warned Sologub that NotPetya was saturating victims' systems with terrifying speed: It took 45 seconds to bring down the network of a large Ukrainian bank. A portion of one major Ukrainian transit hub, where ISSP had installed its equipment as a demonstration, was fully infected in 16 seconds. Ukrenergo, the energy company whose network ISSP had been helping to rebuild after the 2016 blackout cyberattack, had also been struck yet again. "Do you remember we were about to implement new security controls?" Sologub recalls a frustrated Ukrenergo IT director asking him on the phone. "Well, too late."

By noon, ISSP's founder, a serial entrepreneur named Oleh Derevianko, had sidelined his vacation too. Derevianko was driving north to meet his family at his village house for the holiday when the NotPetya calls began. Soon he had pulled off the highway and was working from a roadside restaurant. By the early afternoon, he was warning every executive who called to unplug their networks without hesitation, even if it meant shutting down their entire company. In many cases, they'd already waited too long. "By the time you reached them, the infrastructure was already lost," Derevianko says.

On a national scale, NotPetya was eating Ukraine's computers alive. It would hit at least four hospitals in Kiev alone, six power companies, two airports, more than 22 Ukrainian banks, ATMs and card payment systems in retailers and transport, and practically every federal agency. "The government was dead," summarizes Ukrainian minister of infrastructure Volodymyr Omelyan. According to ISSP, at least 300 companies were hit, and one senior Ukrainian government official estimated that 10 percent of all computers in the country were wiped. The attack even shut down the computers used by scientists at the Chernobyl cleanup site, 60 miles north of Kiev. "It was a massive bombing of all our systems," Omelyan says.

When Derevianko emerged from the restaurant in the early evening, he stopped to refuel his car and found that the gas station's credit card payment system had been taken out by NotPetya too. With no cash in his pockets, he eyed his gas gauge, wondering if he had enough fuel to reach his village. Across the country, Ukrainians were asking themselves similar questions: whether they had enough money for groceries and gas to last through the blitz, whether they would receive their paychecks and pensions, whether their prescriptions would be filled. By that night, as the outside world was still debating whether NotPetya was criminal ransomware or a weapon of state-sponsored cyberwar, ISSP's staff had already started referring to it as a new kind of phenomenon: a "massive, coordinated cyber invasion."

Amid that epidemic, one single infection would become particularly fateful for Maersk: In an office in Odessa, a port city on Ukraine's Black Sea coast, a finance executive for Maersk's Ukraine operation had asked IT administrators to install the accounting software M.E.Doc on a single computer. That gave NotPetya the only foothold it needed.

The shipping terminal in Elizabeth, New Jersey—one of the 76 that make up the port-operations division of Maersk known as APM Terminals—sprawls out into Newark Bay on a man-made peninsula covering a full square mile. Tens of thousands of stacked, perfectly modular shipping containers cover its vast asphalt landscape, and 200-foot-high blue cranes loom over the bay. From the top floors of lower Manhattan's skyscrapers, five miles away, they look like brachiosaurs gathered at a Jurassic-era watering hole.

On a good day, about 3,000 trucks arrive at the terminal, each assigned to pick up or drop off tens of thousands of pounds of everything from diapers to avocados to tractor parts. They start that process, much like airline passengers, by checking in at the terminal's gate, where scanners automatically read their container's barcodes and a Maersk gate clerk talks to the truck driver via a speaker system. The driver receives a printed pass that tells them where to park so that a massive yard crane can haul their container from the truck's chassis to a stack in the cargo yard, where it's loaded onto a container ship and floated across an ocean—or that entire process in reverse order.

On the morning of June 27, Pablo Fernández was expecting dozens of trucks' worth of cargo to be shipped out from Elizabeth to a port in the Middle East. Fernández is a so-called freight forwarder—a middleman whom cargo owners pay to make sure their property arrives safely at a destination halfway around the world. (Fernández is not his real name.)

At around 9 am New Jersey time, Fernández's phone started buzzing with a succession of screaming calls from angry cargo owners. All of them had just heard from truck drivers that their vehicles were stuck outside Maersk's Elizabeth terminal. "People were jumping up and down," Fernández says. "They couldn't get their containers in and out of the gate."

That gate, a choke point to Maersk's entire New Jersey terminal operation, was dead. The gate clerks had gone silent.

Soon, hundreds of 18-wheelers were backed up in a line that stretched for miles outside the terminal. One employee at another company's nearby terminal at the same New Jersey port watched the trucks collect, bumper to bumper, farther than he could see. He'd seen gate systems go down for stretches of 15 minutes or half an hour before. But after a few hours, still with no word from Maersk, the Port Authority put out an alert that the company's Elizabeth terminal would be closed for the rest of the day. "That's when we started to realize," the nearby terminal's staffer remembers, "this was an attack." Police began to approach drivers in their cabs, telling them to turn their massive loads around and clear out.

Fernández and countless other frantic Maersk customers faced a set of bleak options: They could try to get their precious cargo onto other ships at premium, last-minute rates, often traveling the equivalent of standby. Or, if their cargo was part of a tight supply chain, like components for a factory, Maersk's outage could mean shelling out for exorbitant air freight delivery or risk stalling manufacturing processes, where a single day of downtime costs hundreds of thousands of dollars. Many of the containers, known as reefers, were electrified and full of perishable goods that required refrigeration. They'd have to be plugged in somewhere or their contents would rot.

Fernández had to scramble to find a New Jersey warehouse where he could stash his customers' cargo while he waited for word from Maersk. During the entire first day, he says, he received only one official email, which read like "gibberish," from a frazzled Maersk staffer's Gmail account, offering no real explanation of the mounting crisis. The company's central booking website, Maerskline.com, was down, and no one at the company was picking up their phones. Some of the containers he'd sent on Maersk's ships that day would remain lost in cargo yards and ports around the world for the next three months. "Maersk was like a black hole," Fernández remembers with a sigh. "It was just a clusterfuck."

In fact, it was a clusterfuck of clusterfucks. The same scene was playing out at 17 of Maersk's 76 terminals, from Los Angeles to Algeciras, Spain, to Rotterdam in the Netherlands, to Mumbai. Gates were down. Cranes were frozen. Tens of thousands of trucks would be turned away from comatose terminals across the globe.

No new bookings could be made, essentially cutting off Maersk's core source of shipping revenue. The computers on Maersk's ships weren't infected. But the terminals' software, designed to receive the Electronic Data Interchange files from those ships, which tell terminal operators the exact contents of their massive cargo holds, had been entirely wiped away. That left Maersk's ports with no guide to perform the colossal Jenga game of loading and unloading their towering piles of containers.

For days to come, one of the world's most complex and interconnected distributed machines, underpinning the circulatory system of the global economy itself, would remain broken. "It was clear this problem was of a magnitude never seen before in global transport," one Maersk customer remembers. "In the history of shipping IT, no one has ever gone through such a monumental crisis."

Mike McQuade

Several days after his screen had gone dark in a corner of Maersk's office, Henrik Jensen was at home in his Copenhagen apartment, enjoying a brunch of poached eggs, toast, and marmalade. Since he'd walked out of the office the Tuesday before, he hadn't heard a word from any of his superiors. Then his phone rang.

When he answered, he found himself on a conference call with three Maersk staffers. He was needed, they said, at Maersk's office in Maidenhead, England, a town west of London where the conglomerate's IT overlords, Maersk Group Infrastructure Services, were based. They told him to drop everything and go there. Immediately.

Two hours later, Jensen was on a plane to London, then in a car to an eight-story glass-and-brick building in central Maidenhead. When he arrived, he found that the fourth and fifth floors of the building had been converted into a 24/7 emergency operations center. Its singular purpose: to rebuild Maersk's global network in the wake of its NotPetya meltdown.

Some Maersk staffers, Jensen learned, had been in the recovery center since Tuesday, when NotPetya first struck. Some had been sleeping in the office, under their desks or in corners of conference rooms. Others seemed to be arriving every minute from other parts of the world, luggage in hand. Maersk had booked practically every hotel room within tens of miles, every bed-and-breakfast, every spare room above a pub. Staffers were subsisting on snacks that someone had piled up in the office kitchen after a trip to a nearby Sainsbury's grocery store.

The Maidenhead recovery center was being managed by the consultancy Deloitte. Maersk had essentially given the UK firm a blank check to make its NotPetya problem go away, and at any given time as many as 200 Deloitte staffers were stationed in the Maidenhead office, alongside up to 400 Maersk personnel. All computer equipment used by Maersk from before NotPetya's outbreak had been confiscated, for fear that it might infect new systems, and signs were posted threatening disciplinary action against anyone who used it. Instead, staffers had gone into every available electronics store in Maidenhead and bought up piles of new laptops and prepaid Wi-Fi hot spots. Jensen, like hundreds of other Maersk IT staffers, was given one of those fresh laptops and told to do his job. "It was very much just 'Find your corner, get to work, do whatever needs to be done,' " he says.

Early in the operation, the IT staffers rebuilding Maersk's network came to a sickening realization. They had located backups of almost all of Maersk's individual servers, dating from between three and seven days prior to NotPetya's onset. But no one could find a backup for one crucial layer of the company's network: its domain controllers, the servers that function as a detailed map of Maersk's network and set the basic rules that determine which users are allowed access to which systems.

Maersk's 150 or so domain controllers were programmed to sync their data with one another, so that, in theory, any of them could function as a backup for all the others. But that decentralized backup strategy hadn't accounted for one scenario: where every domain controller is wiped simultaneously. "If we can't recover our domain controllers," a Maersk IT staffer remembers thinking, "we can't recover anything."

> After a frantic global search, the admins finally found one lone surviving domain controller in a remote office—in Ghana.

After a frantic search that entailed calling hundreds of IT admins in data centers around the world, Maersk's desperate administrators finally found one lone surviving domain controller in a remote office—in Ghana. At some point before NotPetya struck, a blackout had knocked the Ghanaian machine offline, and the computer remained disconnected from the network.

It thus contained the singular known copy of the company's domain controller data left untouched by the malware—all thanks to a power outage. "There were a lot of joyous whoops in the office when we found it," a Maersk administrator says.

When the tense engineers in Maidenhead set up a connection to the Ghana office, however, they found its bandwidth was so thin that it would take days to transmit the several-hundred-gigabyte domain controller backup to the UK. Their next idea: put a Ghanaian staffer on the next plane to London. But none of the West African office's employees had a British visa.

So the Maidenhead operation arranged for a kind of relay race: One staffer from the Ghana office flew to Nigeria to meet another Maersk employee in the airport to hand off the very precious hard drive. That staffer then boarded the six-and-a-half-hour flight to Heathrow, carrying the keystone of Maersk's entire recovery process.

With that rescue operation completed, the Maidenhead office could begin bringing Maersk's core services back online. After the first days, Maersk's port operations had regained the ability to read the ships' inventory files, so operators were no longer blind to the contents of the hulking, 18,000-container vessels arriving in their harbors. But several days would pass after the initial outage before Maersk started taking orders through Maerskline.com for new shipments, and it would be more than a week before terminals around the world started functioning with any degree of normalcy.

In the meantime, Maersk staffers worked with whatever tools were still available to them. They taped paper documents to shipping containers at APM ports and took orders via personal Gmail accounts, WhatsApp, and Excel spreadsheets. "I can tell you it's a fairly bizarre experience to find yourself booking 500 shipping containers via WhatsApp, but that's what we did," one Maersk customer says.

About two weeks after the attack, Maersk's network had finally reached a point where the company could begin reissuing personal computers to the majority of staff. Back at the Copenhagen headquarters, a cafeteria in the basement of the building was turned into a reinstallation assembly line. Computers were lined up 20 at a time on dining tables as help desk staff walked down the rows, inserting USB drives they'd copied by the dozens, clicking through prompts for hours.

A few days after his return from Maidenhead, Henrik Jensen found his laptop in an alphabetized pile of hundreds, its hard drive wiped, a clean image of Windows installed. Everything that he and every other Maersk employee had stored locally on their machines, from notes to contacts to family photos, was gone.

Five months after Maersk had recovered from its NotPetya attack, Maersk chair Jim

Hagemann Snabe sat onstage at the World Economic Forum meeting in Davos, Switzerland, and lauded the "heroic effort" that went into the company's IT rescue operation. From June 27, when he was first awakened by a 4 am phone call in California, ahead of a planned appearance at a Stanford conference, he said, it took just 10 days for the company to rebuild its entire network of 4,000 servers and 45,000 PCs. (Full recovery had taken far longer: Some staffers at the Maidenhead operation continued to work day and night for close to two months to rebuild Maersk's software setup.) "We overcame the problem with human resilience," Snabe told the crowd.

Since then, Snabe went on, Maersk has worked not only to improve its cybersecurity but also to make it a "competitive advantage." Indeed, in the wake of NotPetya, IT staffers say that practically every security feature they've asked for has been almost immediately approved. Multifactor authentication has been rolled out across the company, along with a long-delayed upgrade to Windows 10.

Snabe, however, didn't say much about the company's security posture pre-NotPetya. Maersk security staffers tell WIRED that some of the corporation's servers were, up until the attack, still running Windows 2000—an operating system so old Microsoft no longer supported it. In 2016, one group of IT executives had pushed for a preemptive security redesign of Maersk's entire global network. They called attention to Maersk's less-than-perfect software patching, outdated operating systems, and above all insufficient network segmentation. That last vulnerability in particular, they warned, could allow malware with access to one part of the network to spread wildly beyond its initial foothold, exactly as NotPetya would the next year.

The security revamp was green-lit and budgeted. But its success was never made a so-called key performance indicator for Maersk's most senior IT overseers, so implementing it wouldn't contribute to their bonuses. They never carried the security makeover forward.

Few firms have paid more dearly for dragging their feet on security. In his Davos talk, Snabe claimed that the company suffered only a 20 percent reduction in total shipping volume during its NotPetya outage, thanks to its quick efforts and manual workarounds. But aside from the company's lost business and downtime, as well as the cost of rebuilding an entire network, Maersk also reimbursed many of its customers for the expense of rerouting or storing their marooned cargo. One Maersk customer described receiving a seven-figure check from the company to cover the cost of sending his cargo via last-minute chartered jet. "They paid me a cool million with no more than a two-minute discussion," he says.

> On top of the panic and disruption it caused, NotPetya may have wiped away evidence of espionage or even reconnaissance for future sabotage.

All told, Snabe estimated in his Davos comments, NotPetya cost Maersk between $250 million and $300 million. Most of the staffers WIRED spoke with privately suspected the company's accountants had low-balled the figure.

Regardless, those numbers only start to describe the magnitude of the damage. Logistics companies whose livelihoods depend on Maersk-owned terminals weren't all treated as well during the outage as Maersk's customers, for instance. Jeffrey Bader, president of a Port Newark–based trucking group, the Association of Bi-State Motor Carriers, estimates that the unreimbursed cost for trucking companies and truckers alone is in the tens of millions. "It was a nightmare," Bader says. "We lost a lot of money, and we're angry."

The wider cost of Maersk's disruption to the global supply chain as a whole—which depends on just-in-time delivery of products and manufacturing components—is far harder to measure. And, of course, Maersk was only one victim. Merck, whose ability to manufacture some drugs was temporarily shut down by NotPetya, told shareholders it lost a staggering $870 million due to the malware. FedEx, whose European subsidiary TNT Express was crippled in the attack and required months to recover some data, took a $400 million blow. French construction giant Saint-Gobain lost around the same amount. Reckitt Benckiser, the British manufacturer of Durex condoms, lost $129 million, and Mondelēz, the owner of chocolate-maker Cadbury, took a $188 million hit. Untold numbers of victims without public shareholders counted their losses in secret.

Only when you start to multiply Maersk's story—imagining the same paralysis, the same serial crises, the same grueling recovery—playing out across dozens of other NotPetya victims and countless other industries does the true scale of Russia's cyberwar crime begin to come into focus.

"This was a very significant wake-up call," Snabe said at his Davos panel. Then he added, with a Scandinavian touch of understatement, "You could say, a very expensive one."

One week after NotPetya's outbreak, Ukrainian police dressed in full SWAT camo gear and armed with assault rifles poured out of vans and into the modest headquarters of Linkos Group, running up the stairs like SEAL Team Six invading the bin Laden compound.

They pointed rifles at perplexed employees and lined them up in the hallway, according to the company's founder, Olesya Linnyk. On the second floor, next to her office, the armored cops even smashed open the door to one room with a metal baton, in spite of Linnyk's offer of a key to unlock it. "It was an absurd situation," Linnyk says after a deep breath of exasperation.

The militarized police squad finally found what it was looking for: the rack of servers that had played the role of patient zero in the NotPetya plague. They confiscated the offending

machines and put them in plastic bags.

Even now, more than a year after the attack's calamitous spread, cybersecurity experts still argue over the mysteries of NotPetya. What were the hackers' true intentions? The Kiev staff of security firm ISSP, including Oleh Derevianko and Oleksii Yasinsky, maintain that the attack was intended not merely for destruction but as a cleanup effort. After all, the hackers who launched it first had months of unfettered access to victims' networks. On top of the panic and disruption it caused, NotPetya may have also wiped away evidence of espionage or even reconnaissance for future sabotage. Just in May, the US Justice Department and Ukrainian security services announced that they'd disrupted a Russian operation that had infected half a million internet routers—mostly in Ukraine—with a new form of destructive malware.

While many in the security community still see NotPetya's international victims as collateral damage, Cisco's Craig Williams argues that Russia knew full well the extent of the pain the worm would inflict internationally. That fallout, he argues, was meant to explicitly punish anyone who would dare even to maintain an office inside the borders of Russia's enemy. "Anyone who thinks this was accidental is engaged in wishful thinking," Williams says. "This was a piece of malware designed to send a political message: If you do business in Ukraine, bad things are going to happen to you."

Almost everyone who has studied NotPetya, however, agrees on one point: that it could happen again or even reoccur on a larger scale. Global corporations are simply too interconnected, information security too complex, attack surfaces too broad to protect against state-trained hackers bent on releasing the next world-shaking worm. Russia, meanwhile, hardly seems to have been chastened by the US government's sanctions for NotPetya, which arrived a full eight months after the worm hit and whose punishments were muddled with other messages chastising Russia for everything from 2016 election disinformation to hacker probes of the US power grid. "The lack of a proper response has been almost an invitation to escalate more," says Thomas Rid, a political science professor at Johns Hopkins' School of Advanced International Studies.

But the most enduring object lesson of NotPetya may simply be the strange, extra-dimensional landscape of cyberwar's battlefield. This is the confounding geography of cyberwarfare: In ways that still defy human intuition, phantoms inside M.E.Doc's server room in a gritty corner of Kiev spread chaos into the gilded conference rooms of the capital's federal agencies, into ports dotting the globe, into the stately headquarters of Maersk on the Copenhagen harbor, and across the global economy. "Somehow the vulnerability of this Ukrainian accounting software affects the US national security supply of vaccines and global shipping?" asks Joshua Corman, a cybersecurity fellow at the Atlantic Council, as if still puzzling out the shape of the wormhole that made that cause-and-effect possible. "The physics of cyberspace are wholly different from every other war domain."

In those physics, NotPetya reminds us, distance is no defense. Every barbarian is already at every gate. And the network of entanglements in that ether, which have unified and elevated the world for the past 25 years, can, over a few hours on a summer day, bring it to a crashing halt.
