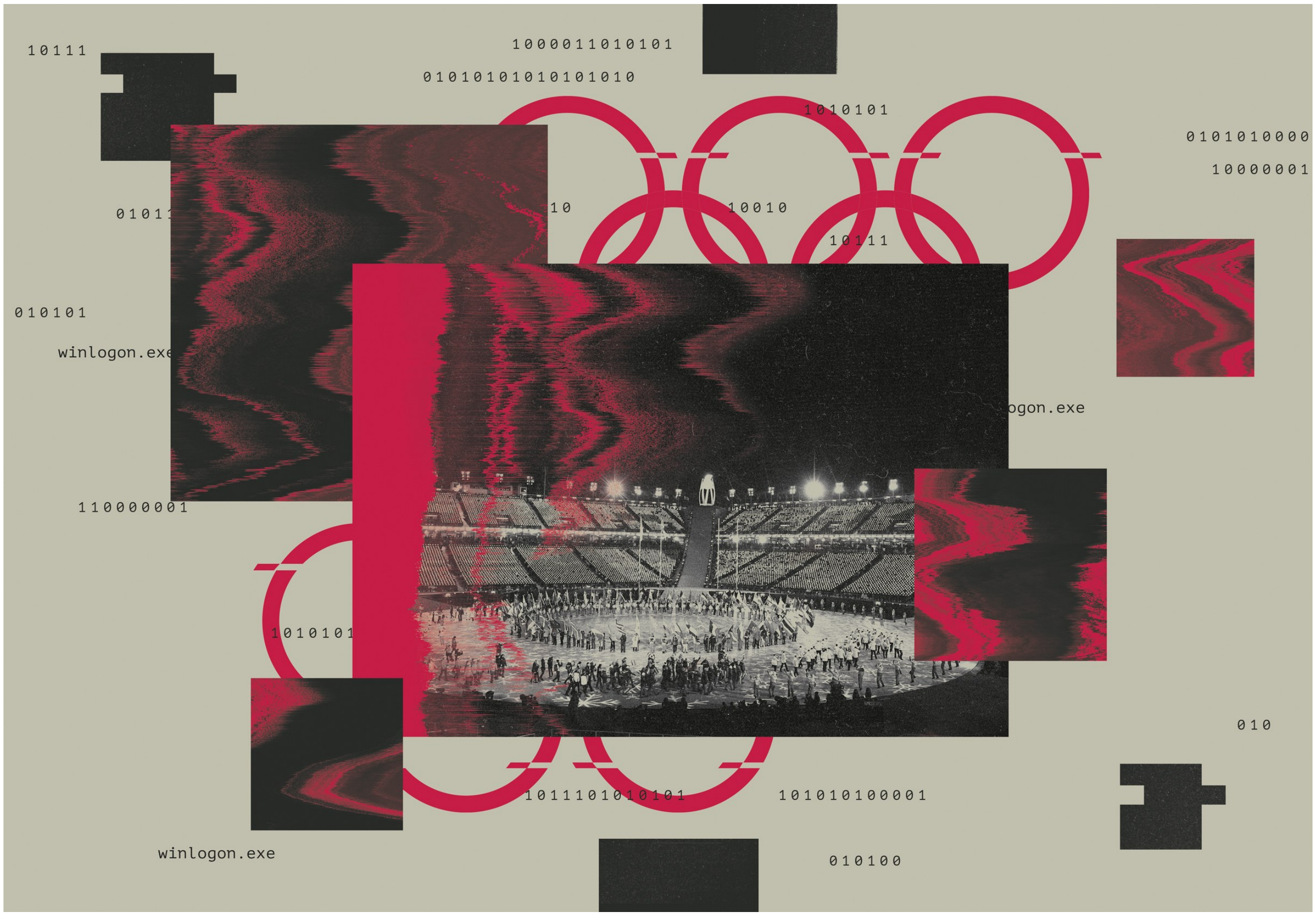
The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History

wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/



Just before 8 pm on February 9, 2018, high in the northeastern mountains of South Korea, Sang-jin Oh was sitting on a plastic chair a few dozen rows up from the floor of Pyeongchang's vast, pentagonal Olympic Stadium. He wore a gray and red official Olympics jacket that kept him warm despite the near-freezing weather, and his seat, behind the press section, had a clear view of the raised, circular stage a few hundred feet in front of him. The 2018 Winter Olympics opening ceremony was about to start.

As the lights darkened around the roofless structure, anticipation buzzed through the 35,000-person crowd, the glow of their phone screens floating like fireflies around the stadium. Few felt that anticipation more intensely than Oh. For more than three years, the 47-year-old civil servant had been director of technology for the Pyeongchang Olympics organizing committee. He'd overseen the setup of an IT infrastructure for the games comprising more than 10,000 PCs, more than 20,000 mobile devices, 6,300 Wi-Fi routers, and 300 servers in two Seoul data centers.

That immense collection of machines seemed to be functioning perfectly—almost. Half an hour earlier, he'd gotten word about a nagging technical issue. The source of that problem was a contractor, an IT firm from which the Olympics were renting another hundred servers. The contractor's glitches had been a long-term headache. Oh's response had been annoyance: Even now, with the entire world watching, the company was still working out its bugs?

> Andy Greenberg is a WIRED senior writer. This story is excerpted from his book *Sandworm*, to be published on November 5, 2019.

The data centers in Seoul, however, weren't reporting any such problems, and Oh's team believed the issues with the contractor were manageable. He didn't yet know that they were already preventing some attendees from printing tickets that would let them enter the stadium. So he'd settled into his seat, ready to watch a highlight of his career unfold.

Ten seconds before 8 pm, numbers began to form, one by one, in projected light around the stage, as a choir of children's voices counted down in Korean to the start of the event:

"*Sip! … Gu! … Pal! … Chil!*"

In the middle of the countdown, Oh's Samsung Galaxy Note8 phone abruptly lit up. He looked down to see a message from a subordinate on KakaoTalk, a popular Korean messaging app. The message shared perhaps the worst possible news Oh could have received at that exact moment: Something was shutting down every domain controller in the Seoul data centers, the servers that formed the backbone of the Olympics' IT infrastructure.

As the opening ceremony got underway, thousands of fireworks exploded around the stadium on cue, and dozens of massive puppets and Korean dancers entered the stage. Oh saw none of it. He was texting furiously with his staff as they watched their entire IT setup go dark. He quickly realized that what the partner company had reported wasn't a mere glitch. It had been the first sign of an unfolding attack. He needed to get to his technology operations center.

As Oh made his way out of the press section toward the exit, reporters around him had already begun complaining that the Wi-Fi seemed to have suddenly stopped working. Thousands of internet-linked TVs showing the ceremony around the stadium and in 12 other Olympic facilities had gone black. Every RFID-based security gate leading into every Olympic building was down. The Olympics' official app, including its digital ticketing function, was broken too; when it reached out for data from backend servers, they suddenly had none to offer.

The Pyeongchang organizing committee had prepared for this: Its cybersecurity advisory group had met 20 times since 2015. They'd conducted drills as early as the summer of the previous year, simulating disasters like cyberattacks, fires, and earthquakes. But now that one of those nightmare scenarios was playing out in reality, the feeling, for Oh, was both infuriating and surreal. “It's actually happened,” Oh thought, as if to shake himself out of the sense that it was all a bad dream.

Once Oh had made his way through the crowd, he ran to the stadium's exit, out into the cold night air, and across the parking lot, now joined by two other IT staffers. They jumped into a Hyundai SUV and began the 45-minute drive east, down through the mountains to the coastal city of Gangneung, where the Olympics' technology operations center was located.

From the car, Oh called staffers at the stadium and told them to start distributing Wi-Fi hot spots to reporters and to tell security to check badges manually, because all RFID systems were down. But that was the least of their worries. Oh knew that in just over two hours the opening ceremony would end, and tens of thousands of athletes, visiting dignitaries, and spectators would find that they had no Wi-Fi connections and no access to the Olympics app, full of schedules, hotel information, and maps. The result would be a humiliating confusion. If they couldn't recover the servers by the next morning, the entire IT backend of the organizing committee—responsible for everything from meals to hotel reservations to event ticketing—would remain offline as the actual games got underway. And a kind of technological fiasco that had never before struck the Olympics would unfold in one of the world's most wired countries.

Oh arrived at the technology operations center in Gangneung by 9 pm, halfway into the opening ceremony. The center consisted of a large open room with desks and computers for 150 staffers; one wall was covered with screens. When he walked in, many of those staffers were standing, clumped together, anxiously discussing how to respond to the attack—a problem compounded by the fact that they'd been locked out of many of their own basic services, like email and messaging.

All nine of the Olympic staff's domain controllers, the powerful machines that governed which employee could access which computers in the network, had somehow been paralyzed, crippling the entire system. The staff decided on a temporary workaround: They set all the surviving servers that powered some basic services, such as Wi-Fi and the internet-linked TVs, to bypass the dead gatekeeper machines. By doing so, they managed to bring those bare-minimum systems back online just minutes before the end of the ceremony.

Over the next two hours, as they attempted to rebuild the domain controllers to re-create a more long-term, secure network, the engineers would find again and again that the servers had been crippled. Some malicious presence in their systems remained, disrupting the machines faster than they could be rebuilt.

Oh and his staff worked frantically to rebuild the Olympics’ digital nervous system.

A few minutes before midnight, Oh and his administrators reluctantly decided on a desperate measure: They would cut off their entire network from the internet in an attempt to isolate it from the saboteurs who they figured must still have maintained a presence inside. That meant taking down every service—even the Olympics' public website—while they worked to root out whatever malware infection was tearing apart their machines from within.

For the rest of the night, Oh and his staff worked frantically to rebuild the Olympics' digital nervous system. By 5 am, a Korean security contractor, AhnLab, had managed to create an antivirus signature that could help Oh's staff vaccinate the network's thousands of PCs and servers against the mysterious malware that had infected them, a malicious file that Oh says was named simply winlogon.exe.

At 6:30 am, the Olympics' administrators reset staffers' passwords in hopes of locking out whatever means of access the hackers might have stolen. Just before 8 that morning, almost exactly 12 hours after the cyberattack on the Olympics had begun, Oh and his sleepless staffers finished reconstructing their servers from backups and began restarting every service.

Amazingly, it worked. The day's skating and ski jumping events went off with little more than a few Wi-Fi hiccups. R2-D2-style robots puttered around Olympic venues, vacuuming floors, delivering water bottles, and projecting weather reports. A *Boston Globe* reporter later called the games “impeccably organized.” One *USA Today* columnist wrote that “it's possible no Olympic Games have ever had so many moving pieces all run on time.” Thousands of athletes and millions of spectators remained blissfully unaware that the Olympics' staff had spent its first night fighting off an invisible enemy that threatened to throw the entire event into chaos.

Illustration: Joan Wong

Within hours of the attack, rumors began to trickle out into the cybersecurity community about the glitches that had marred the Olympics' website, Wi-Fi, and apps during the opening ceremony. Two days after the ceremony, the Pyeongchang organizing committee confirmed that it had indeed been the target of a cyberattack. But it refused to comment on who might have been behind it. Oh, who led the committee's response, has declined to discuss any possible source of the attack with WIRED.

The incident immediately became an international whodunit: Who would dare to hack the Olympics? The Pyeongchang cyberattack would turn out to be perhaps the most deceptive hacking operation in history, using the most sophisticated means ever seen to confound the forensic analysts searching for its culprit.

The difficulty of proving the source of an attack—the so-called attribution problem—has plagued cybersecurity since practically the dawn of the internet. Sophisticated hackers can route their connections through circuitous proxies and blind alleys, making it almost impossible to follow their tracks. Forensic analysts have nonetheless learned how to determine hackers' identities by other means, tying together clues in code, infrastructure connections, and political motivations.

In the past few years, however, state-sponsored cyberspies and saboteurs have increasingly experimented with another trick: planting false flags. Those evolving acts of deception, designed to throw off both security analysts and the public, have given rise to fraudulent narratives about hackers' identities that are difficult to dispel, even after governments announce the official findings of their intelligence agencies. It doesn't help that those official findings often arrive weeks or months later, with the most convincing evidence redacted to preserve secret investigative techniques and sources.

When North Korean hackers breached Sony Pictures in 2014 to prevent the release of the Kim Jong-un assassination comedy *The Interview*, for instance, they invented a hacktivist group called Guardians of Peace and tried to throw off investigators with a vague demand for “monetary compensation.” Even after the FBI officially named North Korea as the culprit and the White House imposed new sanctions against the Kim regime as punishment, several security firms continued to argue that the attack must have been an inside job, a story picked up by numerous news outlets—including WIRED.

When state-sponsored Russian hackers stole and leaked emails from the Democratic National Committee and Hillary Clinton's campaign in 2016, we now know that the Kremlin likewise created diversions and cover stories. It invented a lone Romanian hacker named Guccifer 2.0 to take credit for the hacks; it also spread the rumors that a murdered DNC staffer named Seth Rich had leaked the emails from inside the organization—and it distributed many of the stolen documents through a fake whistle-blowing site called DCLeaks. Those deceptions became conspiracy theories, fanned by right-wing commentators and then-presidential candidate Donald Trump.

The WIRED Guide to Cyberwar

The threat of cyberwar looms over the future: a new dimension of conflict capable of leapfrogging borders and teleporting the chaos of war to civilians thousands of miles beyond its front.

By
Andy Greenberg

The deceptions generated a self-perpetuating ouroboros of mistrust: Skeptics dismissed even glaring clues of the Kremlin's guilt, like Russian-language formatting errors in the leaked documents, seeing those giveaways as planted evidence. Even a joint statement from US intelligence agencies four months later naming Russia as the perpetrator couldn't shake the conviction of disbelievers. They persist even today: In an *Economist*/YouGov poll earlier this year, only about half of Americans said they believed Russia interfered in the election.

With the malware that hit the Pyeongchang Olympics, the state of the art in digital deception took several evolutionary leaps forward. Investigators would find in its code not merely a single false flag but layers of false clues pointing at multiple potential culprits. And some of those clues were hidden deeper than any cybersecurity analyst had ever seen before.

From the start, the geopolitical motivations behind the Olympics sabotage were far from clear. The usual suspect for any cyberattack in South Korea is, of course, North Korea. The hermit kingdom has tormented its capitalist neighbors with military provocations and low-grade cyberwar for years. In the run-up to the Olympics, analysts at the cybersecurity firm McAfee had warned that Korean-speaking hackers had targeted the Pyeongchang Olympic organizers with phishing emails and what appeared to be espionage malware. At the time, McAfee analysts hinted in a phone call with me that North Korea was likely behind the spying scheme.

But there were contradictory signals on the public stage. As the Olympics began, the North seemed to be experimenting with a friendlier approach to geopolitics. The North Korean dictator, Kim Jong-un, had sent his sister as a diplomatic emissary to the games and had invited South Korea's president, Moon Jae-in, to visit the North Korean capital of Pyongyang. The two countries had even taken the surprising step of combining their Olympic women's hockey teams in a show of friendship. Why would North Korea launch a disruptive cyberattack in the midst of that charm offensive?

Then there was Russia. The Kremlin had its own motive for an attack on Pyeongchang. Investigations into doping by Russian athletes had led to a humiliating result in advance of the 2018 Olympics: Russia was banned. Its athletes would be allowed to compete but not to wear Russian flags or accept medals on behalf of their country. For years in the lead-up to that verdict, a state-sponsored Russian hacker team known as Fancy Bear had been retaliating, stealing and leaking data from Olympics-related targets. Russia's exile from the games was exactly the sort of slight that might inspire the Kremlin to unleash a piece of disruptive malware against the opening ceremony. If the Russian government couldn't enjoy the Olympics, then no one would.

If Russia had been trying to send a message with an attack on the Olympics' servers, however, it was hardly a direct one. Days before the opening ceremony, it had preemptively denied any Olympics-targeted hacking. “We know that Western media are planning pseudo-investigations on the theme of ‘Russian fingerprints’ in hacking attacks on information resources related to the hosting of the Winter Olympic Games in the Republic of Korea,” Russia's Foreign Ministry had told Reuters. “Of course, no evidence will be presented to the world.”

In fact, there would be plenty of evidence vaguely hinting at Russia's responsibility. The problem, it would soon become clear, was that there seemed to be just as much evidence pointing in a tangle of other directions too.

Three days after the opening ceremony, Cisco's Talos security division revealed that it had obtained a copy of Olympics-targeted malware and dissected it. Someone from the Olympics organizing committee or perhaps the Korean security firm AhnLab had uploaded the code to VirusTotal, a common database of malware samples used by cybersecurity analysts, where Cisco's reverse-engineers found it. The company published its findings in a blog post that would give that malware a name: Olympic Destroyer.

In broad outline, Cisco's description of Olympic Destroyer's anatomy called to mind two previous Russian cyberattacks, NotPetya and Bad Rabbit. As with those earlier attacks, Olympic Destroyer used a password-stealing tool, then combined those stolen passwords with remote access features in Windows that allowed it to spread among computers on a network. Finally, it used a data-destroying component to delete the boot configuration from infected machines before disabling all Windows services and shutting the computer down so that it couldn't be rebooted. Analysts at the security firm CrowdStrike would find other apparent Russian calling cards, elements that resembled a piece of Russian ransomware known as XData.

Yet there seemed to be no clear code matches between Olympic Destroyer and the previous NotPetya or Bad Rabbit worms. Although it contained similar features, they had apparently been re-created from scratch or copied from elsewhere.

The deeper analysts dug, the stranger the clues became. The data-wiping portion of Olympic Destroyer shared characteristics with a sample of data-deleting code that had been used not by Russia but by the North Korean hacker group known as Lazarus. When Cisco researchers put the logical structures of the data-wiping components side by side, they seemed to roughly match. And both destroyed files with the same distinctive trick of deleting just their first 4,096 bytes. Was North Korea behind the attack after all?

There were still more signposts that led in completely different directions. The security firm Intezer noted that a chunk of the password-stealing code in Olympic Destroyer matched exactly with tools used by a hacker group known as APT3—a group that multiple cybersecurity firms have linked to the Chinese government. The company also traced a component that Olympic Destroyer used to generate encryption keys back to a third group, APT10, also reportedly linked to China. Intezer pointed out that the encryption component had never been used before by any other hacking teams, as far as the company's analysts could tell. Russia? North Korea? China? The more that forensic analysts reverse-engineered Olympic Destroyer's code, the further they seemed to get from arriving at a resolution.

In fact, all those contradictory clues seemed designed not to lead analysts toward any single false answer but to a collection of them, undermining any particular conclusion. The mystery became an epistemological crisis that left researchers doubting themselves. “It was psychological warfare on reverse-engineers,” says Silas Cutler, a security researcher who worked for CrowdStrike at the time. “It hooked into all those things you do as a backup check, that make you think ‘I know what this is.’ And it poisoned them.”

That self-doubt, just as much as the sabotage effects on the Olympics, seemed to have been the malware's true aim, says Craig Williams, a researcher at Cisco. “Even as it accomplished its mission, it also sent a message to the security community,” Williams says. “*You can be misled*.”

The Olympics organizing committee, it turned out, wasn't Olympic Destroyer's only victim. According to the Russian security firm Kaspersky, the cyberattack also hit other targets with connections to the Olympics, including Atos, an IT services provider in France that had supported the event, and two ski resorts in Pyeongchang. One of those resorts had been infected seriously enough that its automated ski gates and ski lifts were temporarily paralyzed.

In the days after the opening ceremony attack, Kaspersky's Global Research and Analysis Team obtained a copy of the Olympic Destroyer malware from one of the ski resorts and began dusting it for fingerprints. But rather than focusing on the malware's code, as Cisco and Intezer had done, they looked at its “header,” a part of the file's metadata that includes clues about what sorts of programming tools were used to write it. Comparing that header with others in Kaspersky's vast database of malware samples, they found it perfectly matched the header of the North Korean Lazarus hackers' data-wiping malware—the same one Cisco had already pointed to as sharing traits with Olympic Destroyer. The North Korean theory seemed to be confirmed.

But one senior Kaspersky researcher named Igor Soumenkov decided to go a step further. Soumenkov, a hacker prodigy who'd been recruited to Kaspersky's research team as a teenager years earlier, had a uniquely deep knowledge of file headers, and he decided to double-check his colleagues' findings.

A tall, soft-spoken engineer, Soumenkov had a habit of arriving at work late in the morning and staying at Kaspersky's headquarters well after dark—a partially nocturnal schedule that he kept to avoid Moscow traffic.

One night, as his coworkers headed home, he pored over the code at a cubicle overlooking the city's jammed Leningradskoye Highway. By the end of that night, the traffic had thinned, he was virtually alone in the office, and he had determined that the header metadata didn't actually match other clues in the Olympic Destroyer code itself; the malware hadn't been written with the programming tools that the header implied. The metadata had been forged.

This was something different from all the other signs of misdirection that researchers had fixated on. The other red herrings in Olympic Destroyer had been so vexing in part because there was no way to tell which clues were real and which were deceptions. But now, deep in the folds of false flags wrapped around the Olympic malware, Soumenkov had found one flag that was *provably* false. It was now clear that someone had tried to make the malware look North Korean and failed due to a slipup. It was only through Kaspersky's fastidious triple-checking that it came to light.

“It was psychological warfare on reverse-engineers.”

A few months later, I sat down with Soumenkov in a Kaspersky conference room in Moscow. Over an hour-long briefing, he explained in perfect English and with the clarity of a computer science professor how he'd defeated the attempted deception deep in Olympic Destroyer's metadata. I summarized what he seemed to have laid out for me: The Olympics attack clearly wasn't the work of North Korea. “It didn't look like them at all,” Soumenkov agreed.

And it certainly wasn't Chinese, I suggested, despite the more transparent false code hidden in Olympic Destroyer that fooled some researchers early on. “Chinese code is very recognizable, and this looks different,” Soumenkov agreed again.

Finally, I asked the glaring question: If not China, and not North Korea, then who? It seemed that the conclusion of that process of elimination was practically sitting there in the conference room with us and yet couldn't be spoken aloud.

“Ah, for that question, I brought a nice game,” Soumenkov said, affecting a kind of chipper tone. He pulled out a small black cloth bag and took out of it a set of dice. On each side of the small black cubes were written words like *Anonymous*, *Cybercriminals*, *Hacktivists*, *USA*, *China*, *Russia*, *Ukraine*, *Cyberterrorists*, *Iran*.

Kaspersky, like many other security firms, has a strict policy of only pinning attacks on hackers using the firm's own system of nicknames, never naming the country or government behind a hacking incident or hacker group—the safest way to avoid the murky and often political pitfalls of attribution. But the so-called attribution dice that Soumenkov held in his hand, which I'd seen before at hacker conferences, represented the most cynical exaggeration of the attribution problem: That no cyberattack can ever truly be traced to its source, and anyone who tries is simply guessing.

Soumenkov tossed the dice on the table. “Attribution is a tricky game,” he said. “Who is behind this? It's not our story, and it will never be.”

Michael Matonis was working from his home, a 400-square-foot basement apartment in the Washington, DC, neighborhood of Capitol Hill, when he first began to pull at the threads that would unravel Olympic Destroyer's mystery. The 28-year-old, a former anarchist punk turned security researcher with a controlled mass of curly black hair, had only recently moved to the city from upstate New York, and he still didn't have a desk at the Reston, Virginia, office of FireEye, the security and private intelligence firm that employed him. So on the day in February when he started to examine the malware that had struck Pyeongchang, Matonis was sitting at his makeshift workspace: a folding metal chair with his laptop propped up on a plastic table.

On a whim, Matonis decided to try a different approach from much of the rest of the perplexed security industry. He didn't search for clues in the malware's code. Instead, in the days after the attack, Matonis looked at a far more mundane element of the operation: a fake, malware-laced Word document that had served as the first step in the nearly disastrous opening ceremony sabotage campaign.

The document, which appeared to contain a list of VIP delegates to the games, had likely been emailed to Olympics staff as an attachment. If anyone opened that attachment, it would run a malicious macro script that planted a backdoor on their PC, offering the Olympics hackers their first foothold on the target network. When Matonis pulled the infected document from VirusTotal, the malware repository where it had been uploaded by incident responders, he saw that the bait had likely been sent to Olympics staff in late November 2017, more than two months before the games began. The hackers had laid in wait for months before triggering their logic bomb.

Matonis began combing VirusTotal and FireEye's historical collection of malware, looking for matches to that code sample. On a first scan, he found none. But Matonis did notice that a few dozen malware-infected documents from the archives corresponded to his file's rough characteristics: They similarly carried embedded Word macros and, like the Olympics-targeted file, had been built to launch a certain common set of hacking tools called PowerShell Empire. The malicious Word macro traps, however, looked very different from one another, with their own unique layers of obfuscation.

Over the next two days, Matonis searched for patterns in that obfuscation that might serve as a clue. When he wasn't at his laptop, he'd turn the puzzle over in his mind, in the shower or lying on the floor of his apartment, staring up at the ceiling. Finally, he found a telling pattern in the malware specimens' encoding. Matonis declined to share with me the details of this discovery for fear of tipping off the hackers to their tell. But he could see that, like teenage punks who all pin just the right obscure band's buttons to their jackets and style their hair in the same shapes, the attempt to make the encoded files look unique had instead made one set of them a distinctly recognizable group. He soon deduced that the source of that signal in the noise was a common tool used to create each one of the booby-trapped documents. It was an open source program, easily found online, called Malicious Macro Generator.

Matonis speculated that the hackers had chosen the program in order to blend in with a crowd of other malware authors, but it had ultimately had the opposite effect, setting them apart as a distinct set. Beyond their shared tools, the malware group was also tied together by the author names Matonis pulled from the files' metadata: Almost all had been written by someone named either “AV,” “BD,” or “john.” When he looked at the command and control servers that the malware connected back to—the strings that would control the puppetry of any successful infections—all but a few of the IP addresses of those machines overlapped too. The fingerprints were hardly exact. But over the next days, he assembled a loose mesh of clues that added up to a solid net, tying the fake Word documents together.

Only after he had established those hidden connections did Matonis go back to the Word documents that had served as the vehicles for each malware sample and begin to Google-translate their contents, some written in Cyrillic. Among the files he'd tied to the Olympic Destroyer bait, Matonis found two other bait documents from the collection that dated back to 2017 and seemed to target Ukrainian LGBT activist groups, using infected files that pretended to be a gay rights organization's strategy document and a map of a Kiev Pride parade. Others targeted Ukrainian companies and government agencies with a tainted copy of draft legislation.

This, for Matonis, was ominously familiar territory: For more than two years, he and the rest of the security industry had watched Russia launch a series of destructive hacking operations against Ukraine, a relentless cyberwar that accompanied Russia's invasion of the country after its pro-Western 2014 revolution.

Even as that physical war had killed 13,000 people in Ukraine and displaced millions more, a Russian hacker group known as Sandworm had waged a full-blown cyberwar against Ukraine as well: It had barraged Ukrainian companies, government agencies, railways, and airports with wave after wave of data-destroying intrusions, including two unprecedented breaches of Ukrainian power utilities in 2015 and 2016 that had caused blackouts for hundreds of thousands of people. Those attacks culminated in NotPetya, a worm that had spread rapidly beyond Ukraine's borders and ultimately inflicted $10 billion in damage on global networks, the most costly cyberattack in history.

In Matonis' mind, all other suspects for the Olympics attack fell away. Matonis couldn't yet connect the attack to any particular hacker group, but only one country would have been targeting Ukraine, nearly a year before the Pyeongchang attack, using the same infrastructure it would later use to hack the Olympics organizing committee—and it wasn't China or North Korea.

Strangely, other infected documents in the collection Matonis had unearthed seemed to target victims in the Russian business and real estate world. Had a team of Russian hackers been tasked with spying on some Russian oligarch on behalf of their intelligence taskmasters? Were they engaged in profit-focused cybercrime as a side gig?

Regardless, Matonis felt that he was on his way to finally, definitively cutting through the Olympics cyberattack's false flags to reveal its true origin: the Kremlin.

Illustration: Joan Wong

After Matonis had made those first, thrilling connections between Olympic Destroyer and a very familiar set of Russian hacking victims, he sensed he had explored beyond the part of Olympic Destroyer that its creators had intended for researchers to see—that he was now peering behind its curtain of false flags. He wanted to find out how much further he could go toward uncovering those hackers' full identities. So he told his boss that he wouldn't be coming into the FireEye office for the foreseeable future. For the next three weeks, he barely left his bunker apartment. He worked on his laptop from the same folding chair, with his back to the only window in his home that allowed in sunlight, poring over every data point that might reveal the next cluster of the hackers' targets.

A pre-internet-era detective might start a rudimentary search for a person by consulting phone books. Matonis started digging into the online equivalent, the directory of the web's global network known as the Domain Name System. DNS servers translate human-readable domains like facebook.com into the machine-readable IP addresses that describe the location of a networked computer that runs that site or service, like 69.63.176.13.

Matonis began painstakingly checking every IP address his hackers had used as a command and control server in their campaign of malicious Word document phishing; he wanted to see what domains those IP addresses had hosted. Since those domain names can move from machine to machine, he also used a reverse-lookup tool to flip the search—checking every name to see what other IP addresses had hosted it. He created a set of treelike maps connecting dozens of IP addresses and domain names linked to the Olympics attack. And far down the branch of one tree, a string of characters lit up like neon in Matonis' mind: account-loginserv.com.

A photographic memory can come in handy for an intelligence analyst. As soon as Matonis saw the account-loginserv.com domain, he instantly knew he had seen it nearly a year earlier in an FBI “flash”—a short alert sent out to US cybersecurity practitioners and potential victims. This one had offered a new detail about the hackers who, in 2016, had reportedly breached the Arizona and Illinois state boards of elections. These had been some of the most aggressive elements of Russia's meddling in US elections: Election officials had warned in 2016 that, beyond stealing and leaking emails from Democratic Party targets, Russian hackers had broken into the two states' voter rolls, accessing computers that held thousands of Americans' personal data with unknown intentions. According to the FBI flash alert Matonis had seen, the same intruders had also spoofed emails from a voting technology company, later reported to be the Tallahassee, Florida-based firm VR Systems, in an attempt to trick more election-related victims into giving up their passwords.

Matonis had found a fingerprint that linked the Olympics attackers back to a hacking operation that directly targeted the 2016 US election.

Matonis drew up a jumbled map of the connections on a piece of paper that he slapped onto his refrigerator with an Elvis magnet, and marveled at what he'd found. Based on the FBI alert—and Matonis told me he confirmed the connection with another human source he declined to reveal—the fake VR Systems emails were part of a phishing campaign that seemed to have also used a spoofed login page at the account-loginserv.com domain he'd found in his Olympic Destroyer map. At the end of his long chain of internet-address connections, Matonis had found a fingerprint that linked the Olympics attackers back to a hacking operation that directly targeted the 2016 US election. Not only had he solved the whodunit of Olympic Destroyer's origin, he'd gone further, showing that the culprit had been implicated in the most notorious hacking campaign ever to hit the American political system.

Matonis had, since he was a teenager, been a motorcycle fan. When he was just barely old enough to ride one legally, he had scraped together enough money to buy a 1975 Honda CB750. Then one day a friend let him try riding his 2001 Harley-Davidson with an 1100 EVO engine. In three seconds, he was flying along a country road in upstate New York at 65 miles an hour, simultaneously fearing for his life and laughing uncontrollably.

When Matonis had finally outsmarted the most deceptive malware in history, he says he felt that same feeling, a rush that he could only compare to taking off on that Harley-Davidson in first gear. He sat alone in his DC apartment, staring at his screen and laughing.

By the time Matonis had drawn those connections, the US government had already drawn its own. The NSA and CIA, after all, have access to human spies and hacking abilities that no private-sector cybersecurity firm can rival. In late February, while Matonis was still holed up in his basement apartment, two unnamed intelligence officials told *The Washington Post* that the Olympics cyberattack had been carried out by Russia and that it had sought to frame North Korea. The anonymous officials went further, blaming the attack specifically on Russia's military intelligence agency, the GRU—the same agency that had masterminded the interference in the 2016 US election and the blackout attacks in Ukraine, and had unleashed NotPetya's devastation.

But as with most public pronouncements from inside the black box of the US intelligence apparatus, there was no way to check the government's work. Neither Matonis nor anyone else in media or cybersecurity research was privy to the trail the agencies had followed.

A set of US government findings that were far more useful and interesting to Matonis came months after his basement detective work. On July 13, 2018, special counsel Robert Mueller unsealed an indictment against 12 GRU hackers for engaging in election interference, laying out the evidence that they'd hacked the DNC and the Clinton campaign; the indictment even included details like the servers they'd used and the terms they'd typed into a search engine.

Deep in the 29-page indictment, Matonis read a description of the alleged activities of one GRU hacker named Anatoliy Sergeyevich Kovalev. Along with two other agents, Kovalev was named as a member of GRU Unit 74455, based in the northern Moscow suburb of Khimki in a 20-story building known as “the Tower.”

The indictment stated that Unit 74455 had provided backend servers for the GRU's intrusions into the DNC and the Clinton campaign. But more surprisingly, the indictment added that the group had “assisted in” the operation to leak the emails stolen in those operations. Unit 74455, the charges stated, had helped to set up DCLeaks.com and even Guccifer 2.0, the fake Romanian hacker persona that had claimed credit for the intrusions and given the Democrats' stolen emails to WikiLeaks.

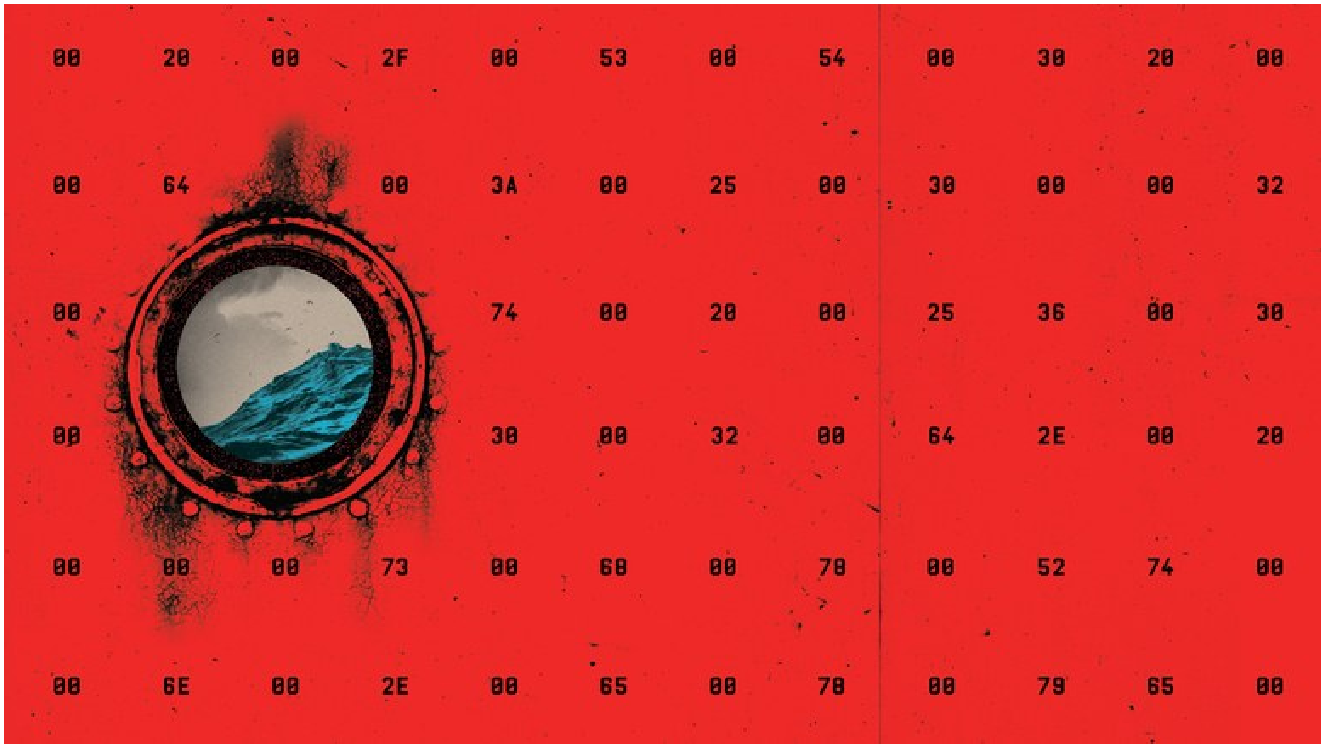
Kovalev, listed as 26 years old, was also accused of breaching one state's board of elections and stealing the personal information of some 500,000 voters. Later, he allegedly breached a voting systems company and then impersonated its emails in an attempt to hack voting officials in Florida with spoofed messages laced with malware. An FBI wanted poster for Kovalev showed a picture of a blue-eyed man with a slight smile and close-cropped, blond hair.

Though the indictment didn't say it explicitly, Kovalev's charges described exactly the activities outlined in the FBI flash alert that Matonis had linked to the Olympic Destroyer attack. Despite all of the malware's unprecedented deceptions and misdirections, Matonis could now tie Olympic Destroyer to a specific GRU unit, working at 22 Kirova Street in Khimki, Moscow, a tower of steel and mirrored glass on the western bank of the Moscow Canal.

A few months after Matonis shared those connections with me, in late November of 2018, I stood on a snow-covered path that wound along that frozen waterway on the outskirts of Moscow, staring up at the Tower.

I had, by then, been following the hackers known as Sandworm for two full years, and I was in the final stages of writing a book that investigated the remarkable arc of their attacks. I had traveled to Ukraine to interview the utility engineers who'd twice watched their power grids' circuit breakers be flipped open by unseen hands. I'd flown to Copenhagen to speak with sources at the shipping firm Maersk who whispered to me about the chaos that had unfolded when NotPetya paralyzed 17 of their terminals at ports around the globe, instantly shutting down the world's largest shipping conglomerate. And I'd sat with analysts from the Slovakian cybersecurity firm ESET in their office in Bratislava as they broke down their evidence that tied all of those attacks to a single group of hackers.

Beyond the connections in Matonis' branching chart and in the Mueller report that pinned the Olympics attack on the GRU, Matonis had shared with me other details that loosely tied those hackers directly to Sandworm's earlier attacks. In some cases, they had placed command and control servers in data centers run by two of the same companies, Fortunix Networks and Global Layer, that had hosted servers used to trigger Ukraine's 2015 blackout and later the 2017 NotPetya worm. Matonis argued that those thin clues, on top of the vastly stronger case that all of those attacks were carried out by the GRU, suggested that Sandworm was, in fact, GRU Unit 74455. Which would put them in the building looming over me that snowy day in Moscow.


00 20 00 2F 00 53 00 54 00 30 20 00
00 64 00 3A 00 25 00 30 00 00 32
00 74 00 20 00 25 36 00 30
00 30 00 32 00 64 2E 00 20
00 00 00 73 00 68 00 78 00 52 74 00
00 6E 00 2E 00 65 00 78 00 79 65 00

The Untold Story of NotPetya, the Code that Crashed the World

Crippled ports. Paralyzed corporations. Frozen government agencies. Inside the most devastating cyberattack in history.

By
Andy Greenberg

Standing there in the shadow of that opaque, reflective tower, I didn't know exactly what I hoped to accomplish. There was no guarantee that Sandworm's hackers were inside—they may have just as easily been split between that Khimki building and another GRU address named in the Mueller indictment, at 20 Komsomolskiy Prospekt, a building in central Moscow that I'd walked by that morning on my way to the train.

The Tower, of course, wasn't marked as a GRU facility. It was surrounded by an iron fence and surveillance cameras, with a sign at its gate that read GLAVNOYE UPRAVLENIYE OBUSTROYSTVA VOYSK—roughly, “General Directorate for the Arrangement of Troops.” I guessed that if I dared ask the guard at that gate if I could speak with someone from GRU Unit 74455, I was likely to end up detained in a room where I would be asked hard questions by Russian government officials, rather than the other way around.

This, I realized, might be the closest I had ever stood to Sandworm's hackers, and yet I could get no closer. A security guard appeared on the edge of the parking lot above me, looking out from within the Tower's fence—whether watching me or taking a smoke break, I couldn't tell. It was time for me to leave.

I walked north along the Moscow Canal, away from the Tower, and through the hush of the neighborhood's snow-padded parks and pathways to the nearby train station. On the train back to the city center, I glimpsed the glass building one last time, from the other side of the frozen water, before it was swallowed up in the Moscow skyline.

In early April of this year, I received an email via my Korean translator from Sang-jin Oh, the Korean official who led the response to Olympic Destroyer on the ground in Pyeongchang. He repeated what he'd said all along—that he would never discuss who might be responsible for the Olympics attack. He also noted that he and I wouldn't speak again: He'd moved on to a position in South Korea's Blue House, the office of the president, and wasn't authorized to take interviews. But in our final phone conversation months earlier, Oh's voice had still smoldered with anger when he recalled the opening ceremony and the 12 hours he'd spent desperately working to avert disaster.

“It still makes me furious that, without any clear purpose, someone hacked this event,” he'd said. “It would have been a huge black mark on these games of peace. I can only hope that the international community can figure out a way that this will never happen again.”

Even now, Russia's attack on the Olympics still haunts cyberwar wonks. (Russia's foreign ministry didn't respond to multiple requests for comment from WIRED.) Yes, the US government and the cybersecurity industry eventually solved the puzzle, after some initial false starts and confusion. But the attack set a new bar for deception, one that might still prove to have disastrous consequences when its tricks are repeated or evolve further, says Jason Healey, a cyberconflict-focused researcher at the Columbia School for International and Public Affairs

“Olympic Destroyer was the first time someone used false flags of that kind of sophistication in a significant, national-security-relevant attack,” Healey says. “It's a harbinger of what the conflicts of the future might look like.”

“If you can't imagine this with US and Russia, imagine it with India and Pakistan, or China and Taiwan, where a false flag provokes a much stronger response than intended.”

Healey, who worked in the George W. Bush White House as director for cyber infrastructure protection, says he has no doubt that US intelligence agencies can see through deceptive clues that muddy attribution. He's more worried about other countries where a misattributed cyberattack could have lasting consequences. “For the folks that can't afford CrowdStrike and FireEye, for the vast bulk of nations, attribution is still an issue,” Healey says. “If you can't imagine this with US and Russia, imagine it with India and Pakistan, or China and Taiwan, where a false flag provokes a much stronger response than even its authors intended, in a way that leaves the world looking very different afterwards.”

But false flags work here in the US, too, argues John Hultquist, the director of intelligence analysis at FireEye and Matonis' former boss before Matonis left the firm in July. Look no further, Hultquist says, than the half of Americans—or 73 percent of registered Republicans—who refuse to accept that Russia hacked the DNC or the Clinton campaign.

As the 2020 election approaches, Olympic Destroyer shows that Russia has only advanced its deception techniques—graduating from flimsy cover stories to the most sophisticated planted digital fingerprints ever seen. And if they can fool even a few researchers or reporters, they can sow even more of the public confusion that misled the American electorate in 2016. “The question is one of audience,” Hultquist says. “The problem is that the US government may never say a thing, and within 24 hours, the damage is done. The public was the audience in the first place.”

The GRU hackers known as Sandworm, meanwhile, are still out there. And Olympic Destroyer suggests they've been escalating not only their wanton acts of disruption but also their deception techniques. After years of crossing one red line after another, their next move is impossible to predict. But when those hackers do strike again, they may appear in a form we don't even recognize.

Source photos: Getty Images; Maxim Shemetov/Reuters (building)

From the book ***SANDWORM****, by Andy Greenberg, to be published on November 5, 2019, by Doubleday, an imprint of the Knopf Doubleday Group, a division of Penguin Random House LLC. Copyright © 2019 by Andy Greenberg. Greenberg is a senior writer for* WIRED.
