Olympic Destroyer Malware Case Study:

The challenge of cyber-attack attribution

Josh Hakala

W200 Final

Hosting the Olympic Games is a coveted honor that allows each nation the opportunity to demonstrate their rich, cultural heritage, and gives their athletes a chance to proudly compete on their home turf in front of an international audience. Watching the opening ceremony on television, one could appreciate the historic Korean culture and the stunning visuals that represented its bright technological future in mobile computing, AI, and medical field. As these opening ceremonies have become increasingly more technologically extravagant they have also become competitive themselves, and thus it is a time to show the world what you can do. Every Olympics, it seems the host nation tries to outdo the previous host's spectacle of technology. So, if an opening ceremony incurred a glitch or disruption— such as a mechanical Olympic ring failing to fully open— then it may be perceived as an embarrassing international failure in a moment when the whole world is watching. While South Korea's opening ceremony was outstanding this year, it did not transpire without controversy and threatening activities that Korea did not fully prepare for: a well-coordinated and destructive cyber-attack.

The months leading up to the 2018 Winter Olympics in PyeongChang were challenging and worrisome. South Korea and the United States struggled to de-escalate the conflict growing with North Korea's nuclear missile program. Would a war break out that would kill millions of people in adjoining nations or would the Korean Peninsula stay calm until at least after the Olympics? After all, this is a time to demonstrate peace and prosperity with the world; allowing other nations to enter your borders for a massive, friendly festival of sport. Several months prior to the Olympics it seemed that we might not have a 2018 Winter Olympics because the United States and the host nation would be in a kinetic war with the North Koreans. Fortunately, North and South Korea, at least

for the short term, were able to put aside their differences. This time, they even agreed to compete under a single flag. However, a different kind of warfare was set to occur, using an alternative to the traditional kinetic destruction. Many cyber threat intelligence sources believe this cyber-attack was executed by a nation-state actor who was interested in disrupting the Olympic games in PyeongChang, South Korea. This attack is known as Olympic Destroyer.

The 2018 Winter games opening ceremony commenced the evening of February 9th, and we did not learn of the cyber-attack until the following morning. Yonhap, a local South Korean news agency, first reported the Olympics website was taken offline. Some users were unable to print their tickets to attend the event due to the site being down. Main press center IP television systems were shut off, and the Wi-Fi network at Olympic stadium also went offline. Soon following were rampant, speculative articles that these systems were downed by a direct attack on Olympic infrastructure. Additionally, we learn later there is evidence the malware was used against some PyeongChang hotels and an IT service Provider, AtoS.

Olympic Destroyer Malware Overview

Talos, Cisco's threat research group, was first to report a technical analysis of the cyber incident that occurred during the opening ceremonies in PyeongChang. It is believed they located the malware samples on VirusTotal—a community malware submission website—which were likely uploaded by operators of the Olympic website and at AtoS. After analyzing the malware, they named the incident Olympic Destroyer due to the destructive capabilities of the malware's computer wiper module and specific targeting of the Olympic games.

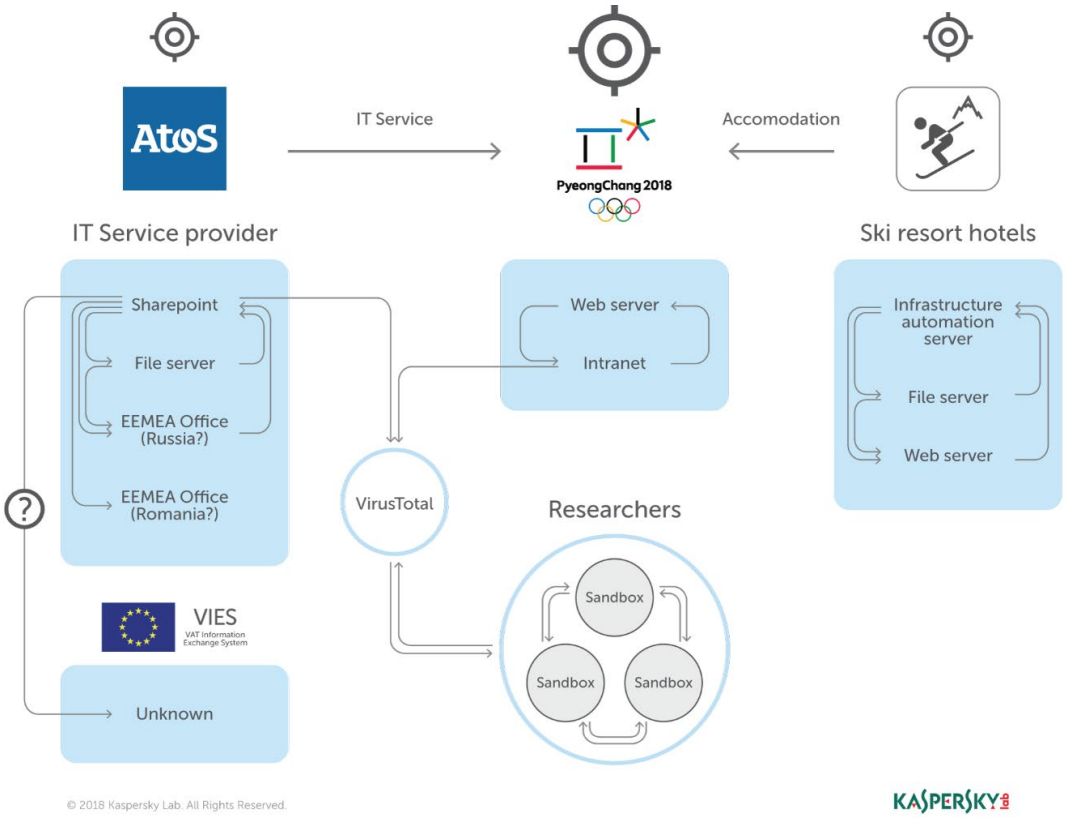

Figure 1: Kaspersky's interpretation of infrastructure affected by Olympic Destroyer

It is still not fully clear how the malware made its way into these systems, however, once Olympic Destroyer is executed on a system it sets in motion the steps to spread itself and delete files along the way. It performs a network discovery operation to locate potential Windows systems it will attempt to propagate itself to. Additionally, the initial payload drops multiple files locally: a Windows credential stealer, a web browser credential stealer, a copy of the initial Olympic Destroyer dropper, PsExec—a legitimate Microsoft SysInternals tool for executing commands on remote machines—and most importantly, a file wiper module. Once the malware had uncovered new credentials from browsers and Windows, it embeds them into the copied dropper. PsExec would then be used to execute the updated dropper on new systems identified during the network discovery. The wiper module, in an effort to render the system unusable, the wiper

deletes volume shadow copies (system restore), disables backups, disables OS startup repair options, deletes the system and security event logs, and disables all services running. The deletion functionality of the wiper module runs by enumerating network resources and deleting files on server network shares. After a 60-minute run time, the target system is then directed to shut down. After the shutdown, because of the of the wiper module, it is in a non-operational state when manually turned back on.

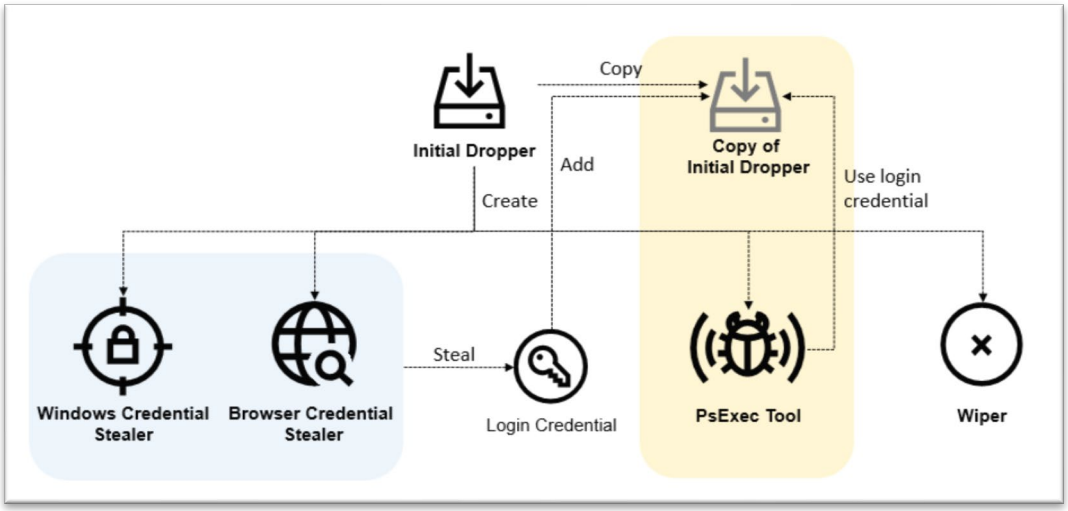

Figure 2: Kaspersky's Olympic Destroyer Functional Overview

Olympic Destroyer sought to delete files on servers. And interestingly the malware does not attempt to wipe the secondary dropped binaries, only the initial dropper. With the overall sophistication of the malware it would be a trivial function to embed into the code. The lack of a feature to fully mask its own tracks is a potential indication that the actor wanted the malware to be analyzed. In essence the malware was created for the purpose of disabling systems within the Olympic networks with the hopes it would be discovered and analyzed. It is hard to imagine a reason why an attacker would want their malware discovered, unless it was for misdirection or misattribution. This is one reason why some researchers believe this Olympic Destroyer

is a false-flag operation: a deceptive set of activities intended to look as though the malware originated from another actor. There exists more evidence within the code, that demonstrates the creator of Olympic Destroyer wanted to confuse researchers.

Threat Actors' Digital Fingerprints

The Cisco Talos' analysis notes there are similarities in Olympic Destroyer's wiper when compared to malware samples of Bad Rabbit and Nyetya (also called NotPetya and ExPetr). Bad Rabbit, released in fall 2017, was a true ransomware variant that shared many features and code with Nyetya, and is believed to be of Russian origin. The Nyetya malware attack occurred earlier in the same year; it was a wiper under the guise of being a ransomware variant. Nyetya is believed to be a Russian false-flag operation with the purpose of wiping machines of Ukrainian targets. Talos Researcher, Craig Williams, shared a graphic of the similarities of the three malware variants on Twitter; See Figure 3. Essentially, Olympic Destroyer is using very similar methods for worm propagation, credential harvesting and event log cleaning.

	OLYMPIC DESTROYER	NYETYA	BADRABBIT
INITIAL VECTOR	Unknown	Supply-chain attack (Medoc)	Drive-by download
PROPAGATIONS	WMI / SMB (via PsExec)	WMI SMB (via psexec) Exploits	WMI SMB (without psexec) Exploits SMB Brute forcing
EXPLOITS	None / Some EternalRomance Artifacts	EternalBlue EternalRomance	EternalRomance
DROPPED FILES	Mimikatz, Credential Stealers	Mimikatz-like password stealer legitimate psexec	Mimikatz-like password stealer DiskCryptor drivers DiskCryptor clients
HARDCODED CREDENTIALS	✓ patched	✗	✓
FILES ENCRYPTION	✗ remote share wipe	✓	✓
MBR MODIFICATION	✗	✓	✓
DISK ENCRYPTION	✗ remote share wipe	wipe	full encryption with DiskCryptor
EVENT LOGS CLEANING	✓	✓	✓
TOR PORTAL	✗	✗	✓

Figure 3: Olympic Destroyer, Nyetya, BadRabbit comparison

Another blog researched which performed an analysis of Olympic Destroyer was Intezer, an Israeli cybersecurity company, which performs “File DNA mapping.” This core feature involves investigating an uploaded sample for code reuse by comparing it to malware or legitimate applications. It will identify “genes,” or pieces of the code that are the same or similar. Intezer expresses the overall similarity to various samples as a percentage. Intezer’s analysis of the Olympic Destroyer malware identified connections with two separate Chinese APT groups: APT3, APT10.

Intezer notes Olympic Destroyer shared 18.5% of its Windows system credential stealer code with APT3’s credential stealer. Additionally, Talos and Intezer note that much of that code is directly from mimikatz. Mimikatz is an open source credential stealer available on the web, so code sharing here is not exactly that profound with respect to attribution. The code fragment similarities of APT10 can be found in a small portion Olympic Destroyer’s main binary where AES encryption keys are generated. Intezer notes that before analyzing Olympic Destroyer, it had only seen that specific code fragment in the single APT10 sample in their entire collection of malware samples.

The third major nation-state connection identified is Lazarus/BlueNoroff, widely believed to be an actor out of North Korea. Recorded Future, Talos, and Kaspersky researchers all note in their analysis that there are multiple similarities between Olympic Destroyer and Lazarus/BlueNoroff. Recorded Future identified parallels in the malware loader code between both malware samples. And Talos specifically points out the similarities of the Olympic Destroyer wiper to the BlueNoroff wiper which was used during a 2016 attack on SWIFT infrastructure at a Bangladesh bank. The wiper modules in BlueNoroff and Olympic Destroyer, while not identical, share very specific logic, such

as how much of a file to wipe: files bigger than 1MB, 4096 bytes are zeroed out—and files under 1MB are completely overwritten with zeroes.

Kaspersky's two blog reports on Olympic Destroyer were released on March 8th, much later than most which arrived on the web only a few days after the attack occurred on February 9th. But I believe the extra time performing analysis paid off as Kaspersky uncovered the most critical piece of evidence supporting the theory that a false-flag operation had occurred. Like in other reports, Kaspersky recognized the challenge in attributing this sample to a specific actor because of its mix of disparate code samples: legitimate software in PsExec, an open source credential harvesting tool in mimikatz, and links to multiple nation-state actors. Kaspersky doubled down on the North Korean Links identified by Recorded Future and Talos. They also noted that there are other high-level similarities, such as the method used "to decrypt payloads in memory using a secret password provided via a command line." They emphasize there are many similarities to the North Korean actor's malware that are really fascinating and which could carry a lot of weight toward potential attribution. But what Kaspersky discovered next became the most important artifact for the entire Olympic Destroyer cyber-attack.

In their analysis article titled, *The devil's in the Rich header*, Kaspersky uncovers a strange metadata link to BlueNoroff malware samples. When an application is built using Microsoft Visual Studio, it encodes into the binary a relatively obscure structure called the "Rich header." According to Kaspersky there is not really any actual documentation on this structure from Microsoft, but it is possible to reverse engineer it and decode its meaning. See Figure 4 for the decoding of the Olympic Destroyer Rich header. What they discovered was the Rich header for Olympic Destroyer was identical

to the rich header in the BlueNoroff samples. Simply stated, it appears the two malware samples were built using the same environment: Visual Studio 6. This alone is not a revelation, as many samples could be built with the same coding environment, and it is a relatively weak link for attribution because of this.

Raw data	Type	Count	Produced by
000C 1C7B 00000001	oldnames	1	12 build 7291
000A 1F6F 0000000B	cobj	11	VC 6 (build 8047)
000E 1C83 00000005	masm613	5	MASM 6 (build 7299)
0004 1F6F 00000004	stdlibdll	4	VC 6 (build 8047)
005D 0FC3 00000007	sdk/imp	7	VC 2003 (build 4035)
0001 0000 0000004D	imports	77	imports (build 0)
000B 2636 00000003	c++obj	3	VC 6 (build 9782)

Figure 4: Olympic Destroyer Rich header

Visual Studio 6 has historically been a commonly used build environment for Lazarus malware samples. It is sometimes used as a supporting attributable artifact to North Korea because it is such an old version that is very rarely seen in use today. Because of this peculiarity in rareness, Kaspersky dug a little deeper into the wiper component's code to test the validity of the alleged build environment. They discovered many discrepancies within the code that indicate it was not built with Visual Studio 6, Among the discrepancies was a reference to a library, 'mscoree.dll', which was non-existent in the time of Visual Studio 6. Additionally, after performing experimentation on different builds, Kaspersky noted a particular function call that is present in the Olympic Destroyer sample, *'___tmainCRTStartup.'* They determined this function is only created when generating binaries from a Visual Studio 2010 build environment. What Kaspersky

asserts is that these inconsistencies unequivocally prove the Rich header was modified after the binary was created, and that the Rich header was copied from a BlueNoroff sample into Olympic Destroyer. This evidence clearly points to a threat actor who is deliberately trying to frame North Korea by placing a common artifact that is relatively unique to their malware samples.

Kaspersky's analysis goes even further on the theory that the Olympic Destroyer Rich header was deceptively modified. They found another slightly different version of Olympic Destroyer malware on VirusTotal that had been modified with a few changes, among them the 60-minute shutdown delay being removed. And based off the compile timestamp, Kaspersky believes this file was hastily modified after the attack on the ski resort hotels began to ensure that when introducing the new variant elsewhere, removal the 60-minute shutdown delay would speed up the effectiveness and provide maximum impact to the opening ceremonies. But in the actor's hasty efforts to modify the worm, they forgot to swap out the Rich header for the fake one from a BlueNoroff sample. Kaspersky notes that the Rich header in this second variant appears to be legitimate. This further solidifies the first variant was indeed modified with a fake header and that someone was trying to frame North Korea.

Nation-state motives

Based off the evidence I have gathered from approximately 20 security research blog articles, there is digital evidence linking Olympic Destroyer to three countries for the creation of this malware: China, North Korea, and Russia. Because many similar pieces of these linked malware samples have been previously analyzed and can be found online, it is conceivable anyone could have created this malware. That is why it is

important to look “beyond the code,” and try to identify the threat actor through an alternative “lens” and broader context, such as ongoing relevant geopolitical issues. At least two of the purported nation-state actors have a significant reason to cause chaos at an event that is supposed to exemplify peaceful order.

While Intezer uncovered links to the Chinese threat actors APT3 and APT10, these links were relatively weak and did not represent a significant portion of the Olympic Destroyer malware code. Moreover, when looking at the historical incidents surrounding APT3 and APT10, neither actor’s motives really match the incident that took place at Olympic Games. Last year, Recorded future attributed APT3 activity, with high confidence, to the Chinese Ministry of State Security. They stated its targeting objectives are to “fulfill intelligence collection requirements on behalf of the MSS.” And APT10, according to FireEye, primarily targets US defense contractors for espionage in support of national security objectives. But the Olympic Destroyer attack was not an operation of obtaining intelligence or stealing intellectual property; it was a deliberate attack to disrupt the Olympics. A motive from either of these nation-state actors based in China does not match the type of attack that occurred, thus it was unlikely an operation originating from APT3 or APT10.

Evidence has been presented discounting the likelihood that the North Koreans were behind the attack because of the modified Rich header. However, it is entirely possible that North Korea could have purposefully placed that false-flag in the hopes it would be discovered by security researchers, who would then turn their attention elsewhere. While that seems unlikely, there is at least a concrete reason why North Korea would want to disrupt the Olympics more than China. Leading up to the

Olympics, North Korea and South Korea are still technically at war, and the North had been defiantly pursuing greater nuclear weapons capabilities to achieve influence and supremacy in the world. With the massive sanctions imposed on North Korea from the UN, coupled with their relations with South Korea, it would not be inconceivable that North Korea would lash out in a fit of malware rage.

A counter-point to this, however, is that North Korea wants to be on a level playing field with the top nations of the world, economically, politically, and especially militarily. They want to be prosperous like the South has become since the two nations' separation. They want the world to recognize them as a powerful nation, but conducting a cyber operation like Olympic Destroyer, if it became attributed to North Korea, would only diminish those goals. And they wanted to compete in the Olympic games. It seems the two nations did set aside their differences at least for that short time in February, offering some hope toward a peaceful resolution. This creates an unlikely scenario for North Korea being the source of the worm, despite the strong similarities in code.

Compared to the first two nations, where Olympic Destroyer malware's actions really match a nation-state objective can be seen in Russia. At the end of their Olympic Destroyer analysis, Kaspersky assesses Lazarus group was framed, and that the most likely group to do it was Sofacy (Also known as APT28 and Fancy Bear). A Russian antivirus company alleging the source of Olympic Destroyer malware is a Russian hacking group believed to be the GRU—the Main Intelligence Directorate—is fascinating and unprecedented (at least by U.S. antivirus vendors). Even Kaspersky's Russian language equivalent analysis blog page included the information about Russian attribution as well. The malware also fits previous operations associated with Russia,

such as the previously mentioned wiper, Nyetya, where it is believed they spread a fake ransomware variant that was designed to inflict damage to Ukraine. But beyond the Olympic Destroyer malware code itself is where the real connections become apparent.

On December 5th, 2017, the International Olympic Committee (IOC) officially banned Russia from participating as a nation in the upcoming 2018 Olympics in PyeongChang. They were banned due to the doping scandal which occurred during the 2014 Sochi Olympics in Russia. The IOC concluded that Russia conducted “systematic manipulation of the anti-doping rules and system in Russia,” and thus they suspended the Russian Olympic Committee; no Russian flags, no Russian anthem, and no Russian uniforms would be permitted in the upcoming Olympics. Being banned from a global event that your country takes a lot of pride in is a considerably humiliating situation and could quite possibly have been the motive for retaliation via Olympic Destroyer.

McAfee, Kaspersky, and other security companies and researchers reported investigating spear phishing emails from December into January, targeting Olympic games partners and the IOC. Kaspersky analyzed a PowerShell script embedded in a Word Doc from one of the spear phishing campaigns targeting South Korea and discovered many similarities to a PowerShell script found on an Olympic Destroyer victim machine, including using the same script obfuscation tool, URL structure, and RC4 cryptographic ciphers. The script in the spear phishing attachment created a backdoor to the threat actor and it could have been the vector used to gain initial access into the Olympic games infrastructure.

Another possible motive or contributing factor is in Russia’s view of the world’s view of Russia. According to Michael Connell and Sara Vogler in their cna.org article,

Russia's Approach to Cyber Warfare, specifically speaking on critical infrastructure, Russian cyber warfare "may also play a greater role in Russia's future strategic deterrence framework." If they have the ability to get into your systems before a conflict, they could disrupt control systems when they believe hostilities are at or near the breaking point for war.

So, while the Olympic games are not exactly deemed "critical infrastructure," it is reasonable to think Russia could have used this incident to test and demonstrate their cyber capabilities to the world. They were barred from participating in the Olympics and may have interpreted that as a pseudo attack on Russia. This "hostile" action of banning Russia could have caused them to practice, and demonstrate as a deterrent, their capabilities to remotely access and disrupt networks, critical or not. Additionally, Kaspersky points out that the malware creator for Olympic Destroyer could have conducted this operation in an effort to perfect the false-flag operation by collecting researcher findings, so additional measure could be put in place to hide traces of attribution in future operations.

The last piece of evidence pointing to Russia is related to the "Fancy Bears International Hack Team" (FBIHT), an alleged "hacktivist" that is pretending to be part of the Anonymous hacking group movement. The threat intelligence firm, ThreatConnect, labels this type of fake hacktivist activity as "faketivism," where "fictitious personas and groups claim credit for APT operations" to provide a medium to leak "data into the public domain. ThreatConnect identified multiple domains that appear to be spoofing the legitimate US and UK Anti-Doping domains' email login pages, which they have attributed to Sofacy due to the timing of a FBIHT blog post on Anti-doping within the

Olympics. FBIHT is actually a pro-Russian persona used to leak information obtained from the GRU's Sofacy group hacking operations." For clarification, the threat actor Sofacy is identified by CrowdStrike as Fancy Bear. CrowdStrike chose to the name group Fancy Bear because they use the word Bear for Russia-based adversaries, and the word Sofacy (which is the name of one of the actor's pieces of malware) reminded one of their analysts of the Iggy Azalea song "Fancy," where the part of the lyrics includes a line of "I'm so fancy." Sofacy, so fancy, Fancy Bear. It then appears the Russians created this aptly named moniker "Fancy Bears International Hack Team" to mock CrowdStrike.

FBIHT blog page claims they "stand for fair play and clean sport." They have previously leaked data from the World Anti-Doping Agency, US Anti-Doping Agency, and the International Association of Athletics Federations; and much of their efforts appear to demonstrate anti-American and anti-Western objectives. In January 2018, FBIHT posted on their blog an article stating they had "obtained the International Olympic Committee officials' correspondence," and that the emails and documents represent an ongoing struggle of "Anglo-Saxon" nations' goals which are less about protecting the integrity of clean Olympic sports but more so a "[fight] for power and cash in the sports world."

The interesting part about this post, and previously related doping scandal posts, is that they have been correlated to timelines of known Fancy Bear spear phishing and hacking activity. McAfee, CrowdStrike, and Kaspersky all identified spear phishing against the IOC shortly after Russia was banned from the Olympics, and then the following month FBIHT purports to have obtained these scandalous emails. This

coincidental timeline of events really only fits the motives of a Russian based APT. And this type of activity of using monikers to leak information, usually about the United States, is not new to Russia.

The recent U.S. Justice Department indictment of 12 Russian GRU intelligence operatives, issued by Special Counsel Robert Mueller, calls out two other fake personas identified as Russian fronts for their APT activities, that were used to leak information: “DC Leaks,” and “Guccifer 2.0.” In 2016, these two groups leaked information related to the Clinton Campaign, DCCC, and DNC. Comparing the indictment details of the GRU to the activities by FBIHT reveals striking similarities. And with the Olympic Destroyer incident, it appears to be a two-pronged campaign by the GRU. First, after the Russian ban from the Olympics, the GRU used the FBIHT to leak sensitive information likely obtained through phishing the IOC. The second phase, in an act of defiance and reprisal, the GRU disrupted the Olympic events by phishing and hacking the official Olympic partners, while trying to frame another potential nation-state actor who also shares a potential interest in sabotaging the Olympics. This type of activity is dangerous to the world and without reprimand will only get worse, as Russia will not have any incentive to stop.

Cyber warfare

Reviewing the United Nations Charter on cyber conflict, it becomes clear this attack at the Olympics, if actually conducted by Russia, does not likely constitute cyber warfare because it was not considered use of force. The damage caused is not like the kinetic damage associated with traditional warfare; some computers became inoperable, causing minor disturbances in operations. While these systems were

important for some functions of the opening ceremonies, they were not part of any critical infrastructure that affected territorial integrity of a sovereign nation. And overall, the disruption it caused was minimal and relatively short lived.

While Russia was upset with their exclusion from the Winter Olympics, this really provided them an opportunity to conduct a test and demonstrate to the World what Russia is capable of doing, without the operation classified as an actual cyber warfare event; it was a dry run. Now they are confident this methodology can be applied to something such as critical infrastructure. While this attack may have only been a minor nuisance compared to an attack actually damaging critical infrastructure, it should not go unpunished. Without any sort of reprimand, Russia now believes they are able to get away with this type of cyber activity and will likely continue to do so in preparation and sharpening their cyber spear for a major digital war.

References

International Olympic Committee Bans Russia

Yonhap News Report on Opening Ceremonies Disruption

International Olympic Committee confirms cyber-attack

Talos Olympic Destroyer Analysis

Intezer Olympic Destroyer Analysis

Endgame Olympic Destroyer Analysis

Recorded Future Olympic Destroyer Analysis

Lastline Olympic Destroyer Analysis 1

Lastline Olympic Destroyer Analysis 2

Kaspersky Olympic Destroyer Analysis 1

Kaspersky Olympic Destroyer Analysis 2

Kaspersky Olympic Destroyer Attribution RU

Kaspersky Olympic Destroyer Attribution US

Independent Security Researcher Olympic Destroyer Analysis

Talos Researcher Craig Williams Twitter Post

Recorded Future APT3 China MSS Connection

FireEye APT10

ThreatConnect faketivist vs. hacktivist groups

ThreatConnect Doping Domain spoofing

McAfee Identifies Olympic Phishing attacks

Fancy Bears International Hack Team website

Russia's Approach To Cyber Warfare - cna.org

Slate.com Mueller Indictment

Justice Department Mueller Indictment