CYBERSECURITY

Like a Spy Movie: How Russia Hacked Its Olympic Enemies

By Bruce Sussman

Read more about the author

SUN | DEC 26, 2021 | 7:15 AM PST

This is a top-read SecureWorld News story from our archives.

It's the kind of thing Hollywood would put on the big screen or Netflix with the label "based on a true story."

And they would certainly release it during the next Olympics because it has an Olympics theme.

The page-turning details come straight from a U.S. government indictment of seven Russian military officers. They are accused of hacking sports and anti-doping organizations on three continents.

Most Recent

Moscow viewed the targeted organizations as its

Olympic adversaries.

A post from the Microsoft Threat Intelligence Center offered few details, however, SecureWorld has uncovered a trail of deceit, lies, and social engineering which Russia used against its Olympic enemies around the time of a prior Olympics.

Russian agents even traveled the globe to track and then hack their targets. Here is the story.

The cyberattack setup: Russian Olympic athletes banned for doping

In July 2016, just before the Summer Olympic Games in Rio de Janeiro, Brazil, something called the McLaren Report came out. It detailed Russia's "Institutionalised Doping Conspiracy and Cover-Up," revealing how Russian athletes hide doping efforts and appear clean even if they are not.

[RELATED: See the final McLaren Report on athlete doping]

After arbitration, 111 Olympic athletes from Russia quickly found themselves banned from competing in the summer games in Rio.

Russia was embarrassed, denied the allegations, and apparently was out for revenge.

The Russian military's intelligence division, the GRU, began hunting the world for those who had made it look bad.

Russian cyber attacks aimed at anti-doping agencies and experts

Russia's GRU launched cyberattacks against anti-doping experts and agencies involved, including the World Anti-Doping Agency, the United States Anti-Doping Agency, and the Canadian Centre for Ethics in Sport, which is the Canadian anti-doping organization.

The nation-state hackers also targeted anti-doping officials at sporting federations like the IAAF and FIFA.

At first, the indictment says, seven Russian intelligence officers applied typical tools of the cyber spy and hacking trade:

- they used fictitious personas to hide their true identities
- used proxy servers to hide their true location
- researched victim details to prepare for social engineering
- sent spearphishing emails that tried to get people to click fake links or open documents that would install malware
- and, where this worked, they "compiled, used, and monitored malware command and control servers," which could help them track and steal information

This is efficient and somewhat effective, but not always.

Remote hacking fails, Russian hackers travel to their targets

There is a challenge with these traditional hacking methods. They typically require the target to take action, to fall for an impostor.

And as we've heard at our cybersecurity conferences across North America, *would-be victims* are getting smarter and many hackers are having to get more creative in their attacks.

In this case, the U.S. indictment says, Russian intelligence officers traveled the globe to track their targets, watched for them to connect to a Wi-Fi network, and then hacked them when they thought everything was secure.

Russian intelligence agents hack attendee at an anti-doping conference

What better place could there be to find your anti-doping enemies than at the World Anti-Doping Association (WADA) conference?

According to court documents, that is where two of the Russian Intelligence Officers traveled. And just like you see in a movie, they were lurking and waiting for their cyber target. They planned for the moment their target connected to the web.

Remember all the warnings about hotel Wi-Fi being insecure? Here is exhibit A. The Russian agents used it to track an employee of the CCES, which is Canada's anti-doping organization:

> "In mid-September 2016, WADA hosted an anti-doping conference in Lausanne, Switzerland. On September 18, 2016, defendants Morenets and Serebriakov traveled to Lausanne with equipment used in *close access* Wi-Fi compromises. On or about September 19, 2016, Morenets and Serebriakov compromised the Wi-Fi network of a hotel hosting the conference and leveraged that access to compromise the laptop and credentials of a senior CCES official staying at the hotel. Other conspirators thereafter used the stolen credentials to compromise CCES's networks in Canada...."

And just like that, Russia compromised the anti-doping agency, one of its Olympic enemies.

They launched similar attacks against anti-doping experts in other parts of the world, including Rio, where Russia was badly embarrassed by the doping scandal.

U.S. officials say once that phase of the attack was successful, access details were transferred to Russia for others to exploit.

What Russian hackers stole in these anti-doping cyber attacks

So what did Russia want besides usernames, passwords, and the ability to hack into the email accounts of anti-doping experts and the networks of their organizations?

The U.S. indictment says they wanted and stole information on medical records, athlete drug test results, and other data, including information regarding therapeutic use exemptions (TUEs), which allow athletes to use otherwise prohibited substances for approved reasons.

Russia launches a disinformation campaign with stolen data

Russian intelligence then took that data and launched a disinformation campaign.

Wait a minute, where have we heard about this strategy before? During the 2016 U.S. presidential election. Only in this case, it was not about who would become a U.S. president.

This now turned into an effort to exonerate Russian athletes and undermine the world's anti-doping efforts. And it is also where the connection between the hacks and Russia's Fancy Bear hacking group were plain as day:

> "From 2016 through 2018, the conspirators engaged in a proactive outreach campaign, using Twitter and e-mail to communicate with approximately 186 reporters about the stolen information. After articles were published, conspirators used the Fancy Bears' Hack Team social media accounts to draw attention to the articles in an attempt to amplify the exposure and effect of their message."

Mainstream news reporters were socially engineered to publish stolen information, which in turn allowed Russian-created social media accounts to share those reports as fact.

It all sounds like the plot of a movie, doesn't it? This one could be a documentary.

[RELATED: 20 Tricks the Russians Used in the DNC Hack]

Russian cyber attackers out of reach

Like all indictments against Russian hackers still in Russia, the charges mean nothing for the individuals involved as long as they stay in their homeland.

Russia has made headlines recently for ransomware attacks against Colonial Pipeline, JBS meat, and IT services company Kaseya. And President Biden recently gave Putin a no hack-list, along with a warning.

But long before these instances, Russia was hacking its Olympic enemies and using reporters and social media accounts against the west.

[RELATED: Cyber Attack Motivations: Russia vs. China]

Tags: Cybersecurity, Hackers, Olympics, Russia, Cybercrime / Threats

Comments

First Name*

Last Name

Email*

Comment*

protected by reCAPTCHA

Privacy - Terms

Submit Comment