Cyberthreats during Russian-Ukrainian tensions: what can we learn from history to be prepared?

news.sophos.com/en-us/2022/02/22/cyberthreats-during-russian-ukrainian-tensions-what-can-we-learn-from-history-to-be-prepared/

Chester Wisniewski

February 23, 2022

With Russian troops targeting Ukraine and distributed denial of service (DDoS) attacks sporadically disrupting Ukrainian government websites and financial service providers, there is much talk about being prepared for cyber conflict.

While all organizations should always be prepared for an attack from any direction, it can be helpful to know what to look for when the risk of attack increases. I decided to review the history of known or suspected Russian state activities in the cyber realm to assess what types of activities to expect and how organizations can be prepared.

Destabilizing denial of service attacks

The earliest known activity dates to April 26, 2007, when the Estonian government moved a statue commemorating the Soviet Union's liberation of Estonia from the Nazis to a less prominent location. This action infuriated Estonia's Russian speaking population and destabilized relations with Moscow. Soon after there were riots in the streets, protests outside of the Estonian embassy in Moscow and a wave of debilitating DDoS attacks on Estonian government and financial services websites.

Fully prepared tools and instructions on how to participate in DDoS attacks appeared on Russian forums almost immediately after the moving of the statue. These attacks targeted websites belonging to the President, Parliament, police, political parties, and major media outlets.

While calling on fellow “Russian patriots” to help punish Estonia, this was unlikely to have been a grassroots movement that sprung from zero with tools and a list of targets at the ready. The same tactics were later deployed by Anonymous in defense of Wikileaks, using a tool called the low orbit ion canon (LOIC).

On May 4, 2007, the attacks intensified and additionally began targeting banks. Exactly seven days later the attacks ceased at midnight, as abruptly as they had begun.

Everyone immediately implicated Russia, but attributing distributed denial of service attacks is near impossible, by design. It is now widely believed these DDoS attacks were the work of the Russian Business Network (RBN), a notorious organized crime group in Russia with ties to spamming, botnets and pharmaceutical affiliate schemes. Their services appear to have been “procured” for precisely a week to conduct these attacks.

On July 19, 2008, a new wave of DDoS attacks began targeting news and government websites in Georgia. These attacks mysteriously intensified dramatically on August 8, 2008, as Russian troops invaded the separatist province of South Ossetia. Initially they targeted Georgian news and government sites before moving on to include financial institutions, businesses, education, Western media, and a Georgian hacker website.

Like the earlier attacks on Estonia, a website appeared featuring a list of targets as well as a set of tools with instructions for using them. This ruse also attempted to attribute the attacks to “patriots” defending against Georgian aggression, yet most of the actual attack traffic originated from a known large botnet believed to be controlled by RBN.

Digital defacement and spam

The attacks on Georgia also included website defacements and massive spam campaigns designed to clog Georgian’s inboxes. All of this appeared to be designed to inspire a lack of confidence in the ability of Georgia to defend and govern itself and to prevent the government from effectively communicating with its citizens and the outside world.

Less than a year later, a further series of DDoS attacks began in Kyrgyzstan in January 2009. This happened to coincide with a decision-making process the Kyrgyzstani government was entering into to decide whether to renew a lease on a US air base in their territory. Coincidence? It appeared to be conducted by the RBN once again, but this time no ruse of “patriots” expressing their digital opinions.

This brings us to the most recent kinetic conflict, the invasion of Crimea in 2014.

Disinformation and isolation

Low-level information warfare has been ongoing against Ukraine since 2009, with many attacks coinciding with events that could be interpreted as threatening to Russian interests such as a NATO summit and negotiations between Ukraine and the EU for an Association Agreement.

In March 2014, the New York Times reported that “Snake” malware had infiltrated the Ukraine Prime Minister’s Office and several remote embassies at the same time as anti-government protests began in Ukraine. Near the end of 2013 and into 2014, ESET also published research documenting attacks against military targets and media outlets dubbed “Operation Potao Express.”

As before a homegrown cyber group known as “Cyber Berkut” executed DDoS attacks and web defacements, without causing much actual harm. It did, however, create a lot of confusion and that alone has an impact during times of conflict.

Early in the conflict soldiers without insignias seized control of Crimea’s telecommunications networks and the only internet exchange in the region, causing an information blackout. The attackers abused their access to the mobile phone network to identify anti-Russian protesters and send them SMS messages saying, “Dear subscriber, you are registered as a participant in a mass disturbance.”

After isolating Crimea’s ability to communicate, the attackers also tampered with the mobile phones of members of the Ukrainian Parliament, preventing them from effectively reacting to the invasion. As noted in Military Cyber Affairs, disinformation campaigns kicked into full swing:

“In one case, Russia paid a single person to hold multiple different web identities. One actor in St. Petersburg conveyed that she was acting as three different bloggers with ten blogs, while also commenting on other sites. Another individual was employed to simply comment on news and social media 126 times every twelve hours.”

Paralyzing power supplies

On December 23, 2015, the power was abruptly turned off for about half of the residents of Ivano-Frankivsk, Ukraine. This is widely believed to have been the work of state-sponsored Russian hackers. The initial attacks began more than 6 months before the power blinked out when employees at three power distribution centers opened a malicious Microsoft Office document with a macro designed to install malware called BlackEnergy.

The attackers were able to acquire remote access credentials to the Supervisory Control and Data Acquisition (SCADA) network and take control of the substation controls to begin opening circuit breakers. The attackers then proceeded to brick those remote controls to prevent the breakers from being closed remotely to restore power. Additionally, the attackers deployed a “wiper” to brick the computers used to control the grid and simultaneously conducted a telephone denial of service (TDoS) attack by clogging the customer service numbers, frustrating customers trying to report the outages.

Nearly one year later, on December 17, 2016, the lights blinked out once again in Kyiv. Coincidence? Likely not.

This time the malware responsible was called Industroyer/CrashOverride and it was immensely more sophisticated. The malware was designed with modular components that could scan the network to find SCADA controllers and it also spoke their language. It also had a wiper component to erase the system. The attack didn’t appear related to BlackEnergy or the known wiper tool, KillDisk, but there was no doubt who was behind it.

Email exposure

In June 2016, during a close Presidential election campaign between Hillary Clinton and Donald Trump, a new character named Guccifer 2.0 appeared on the scene claiming to have hacked the Democratic National Committee and proceeded to hand over their emails to Wikileaks. While not officially attributed to Russia, this appeared alongside other disinformation campaigns during the 2016 election and is widely believed to be the work of the Kremlin.

Supply chain attacks: NotPetya

Russia’s persistent attacks against Ukraine weren’t over and they turned up the heat on June 27, 2017, when they unleashed a new piece of malware now dubbed NotPetya.

NotPetya was disguised as a new strain of ransomware and deployed through a hacked supply chain of a Ukrainian accounting software provider. In fact, it was not really ransomware at all. Although it would encrypt a computer, it was impossible to decrypt, effectively wiping the device and making it useless.

The victims weren’t limited to Ukrainian companies. The malware spread around the world within hours, mostly impacting organizations that had operations in Ukraine where the booby-trapped accounting software was used.

NotPetya is estimated to have caused at least $10 billion USD in damage worldwide.

False Flags

As the Winter Olympic games opened in PyeongChang on February 9, 2018, another attack was about to be unleashed on the world. The malware attack disabled every domain controller across the entire Olympic network, preventing everything from Wi-Fi to ticket gates from working properly. Miraculously, the IT team was able to isolate the network, rebuild and remove the malware from the systems and have everything up and running for the next morning, barely skipping a beat.

Then it was time to conduct the malware analysis to attempt to determine who would want to attack and disable the entire Olympic network? Malware attribution is hard, but there were some clues left behind that might help, or they could be false flags trying to point the finger at an uninvolved third party.

The “evidence” appeared to point at North Korea and China, yet it was almost too obvious to attempt to blame North Korea. In the end, some brilliant detective work by Igor Soumenkov of Kaspersky Lab found a smoking gun that pointed directly at Moscow.

A few years later, just before the festive holidays in late 2020, word spread of a supply chain attack targeting the SolarWinds Orion software used to manage networking infrastructure for large and mid-size organizations around the globe, including many US Federal Government agencies. The software update mechanisms had been hijacked and used to deploy a backdoor.

The high-profile nature of the victims, combined with the access afforded through the stealthily deployed backdoor may make this attack one of the largest and most damaging cyberespionage attacks in modern history.

The U.S. Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of Director of National Intelligence (ODNI), and the National Security Agency (NSA) released a joint statement saying their investigation indicated that:

“…an Advanced Persistent Threat actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks. At this time, we believe this was, and continues to be, an intelligence gathering effort.”

Russian cyberconflict in 2022

In 2022, as political tensions escalated in advance of the war, numerous Ukrainian government websites were defaced, and systems were infected with malware disguised as a ransomware attack.

Multiple components of these attacks echoed the past. The malware was not actually ransomware, it was simply a sophisticated wiper, as was seen in the NotPetya attacks. Additionally, there were many false flags left behind implying it might be the work of Ukrainian dissidents or Polish partisans.

As the conflict moved into February, it became clear that the standard Russian conflict playbook was in action: distract, confuse, deny, and attempt to divide.

On Tuesday February 15, 2022, a series of debilitating DDoS attacks were unleashed against Ukrainian government and military websites, as well as against three of Ukraine's largest banks. In an unprecedented move the White House has already declassified some intelligence and pinned the attacks on the Russian GRU.

The war began on February 24, 2022. Sophos is maintaining a rolling summary of cyberattack developments as they unfold.

The Russian playbook for cyberwarfare

What now? Regardless of whether things continue to escalate, cyberoperations are sure to continue. Ukraine has been under a constant barrage of attacks with varying degrees of peaks and troughs since Viktor Yanukovych was deposed in 2014.

Russia's official "The Military Doctrine of the Russian Federation" from 2010 states:

"the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force."

This suggests a continuance of previous behaviors before a conflict, and makes DDoS attacks a potential sign of an imminent kinetic response.

Information warfare is how the Kremlin can try to control the rest of the world's response to actions in Ukraine or any other target of attack.

False flags, misattribution, disrupted communications, and social media manipulation are all key components of Russia's information warfare playbook. They don't need to create a permanent cover for activities on the ground and elsewhere, they simply need to cause enough delay, confusion and contradiction to enable other simultaneous operations to accomplish their objectives.

Prepare and protect

Interestingly, the United States and United Kingdom are trying to preempt some of the misinformation campaigns, and this could limit their effectiveness. However, we shouldn't assume the attackers will stop trying, so we need to remain prepared and vigilant.

For example, organizations in countries surrounding Ukraine should be prepared to be drawn into any online mischief, even if they are not operating directly inside Ukraine. Previous attacks and misinformation have leaked over into Estonia, Poland, and other bordering states, even if only as collateral damage.

From a global perspective, we should expect a range of "patriotic" freelancers in Russia, by which I mean ransomware criminals, phish writers and botnet operators, to lash out with even more fervor than normal at targets perceived to be against the Motherland.

It is unlikely Russia would directly attack NATO members and risk invocation of Article V. However, its recent gestures toward reining in criminals operating from the Russian Federation and their Commonwealth of Independent States (CIS) partners will probably come to an end, and instead we will see the threats multiply.

While defense-in-depth security should be the normal thing to strive for at the best of times, it is especially important if we can expect an increase in the frequency and severity of attacks. The misinformation and propaganda will soon reach a fever pitch, but we must keep our nose to the ground, batten down the hatches and monitor for anything unusual on our networks as the conflict cycles ebb and flow and even when/if they end soon. Because as we all know, it could take months for evidence of digital intrusions due to this Russian-Ukrainian conflict to surface.