Russian Organized Crime

By Damsith Marasinghe

1. Tools, Techniques & Procedures

- Primarily Russia employs for soft power IO, are hacker groups and internet trolls. Hacker groups provide Russia with a **covert, non-attributable** option for acquiring data and documents that can be used in disinformation campaigns and information operations. They conduct a range of cyber activities, from **Distributed Denial Service Attacks** (DDoS attacks) and **Cyber Espionage** to data/document exfiltration and digital sabotage

- Basic techniques used by hacktivists and other non-state actors—for instance, redirecting traffic—are no longer as useful as they were five or ten years ago. The crowd-sourced approach that has typified how the Kremlin has utilized hackers and criminal networks in the past is likely to be replaced by **more tailored approaches**, with the FSB (The Federal Security Service is a federal executive body) and other state agencies conducting network reconnaissance in advance and developing malware to attack specific system vulnerabilities.

- Techniques and tools they use, their impact, and how their effects can be **defended against or mitigated** are being studied but not how the adversary conducts cyber-attacks, what they intend to achieve, **how the adversary perceives risk and escalation in cyberspace**, and whether the attacks can be deterred are often overlooked.

- The simple **DDoS attacks and DNS hijackings that typified Russian cyber operations in Estonia and Georgia** have been overshadowed by more sophisticated tactics and malware tools, such as **BlackEnergy and Ouroboros**.

2. Common Targets

- Journalists, especially those reporting on ROC members in an unfavorable light, as legitimate targets were **Estonian government sites, including Parliament's webpage, websites of political parties, the country's largest banks, and the country's most prominent news and telecommunications outlets**. While Estonians insisted on a Russian hand, the activity appeared to be originating from botnets all over the world, including Egypt, Vietnam, and Peru. Indeed, instructions for conducting the ping attacks were posted online, as well as guidance for how to target specific Estonian websites.

- Microsoft has said the UK and six other countries outside of the US have been affected by a suspected Russian hacking attack that US authorities have warned poses a grave risk to government and private networks. Brad Smith, Microsoft 's chief legal counsel, said the company had uncovered 40 customers , including government agencies, Thinktanks, NG's and IT companies, who were targeted more precisely and compromised after the hackers had gained initial access earlier this year. Eight percent were in the US, including it is feared, agencies responsible for the US nuclear weapons stockpile. But the remainder was spread out across other countries. This included Canada and Mexico in North America, Belgium, Spain and UK in the Europe and Israel and the UAE in the Middle East.

- Russia maintains numerous units that are overseen by various security and intelligence agencies. Russia's security agencies compete with each other and often conduct similar operations on the same targets.

3. Monetary Model

Russian organized crime is adept at changing criminal activities and diversifying into new criminal markets. Financial markets and banks, for example, have become new targets of criminal opportunity.

- In a recent case in point (United States v. Alexander Lushtak), it was alleged that the defendant carried out a multimillion-dollar investment fraud scheme and the subsequent laundering of nearly $2 million of the proceeds of that scheme by depositing the moneys in an account at the Bank of New York.
- In United States v. Dominick Dionisio, et al., two persons alleged to be associated with La Cosa Nostra and an alleged member of the "Bor" Russian organized crime group were charged with operating a multimillion-dollar investment fraud and laundering the proceeds of the scheme.
- Legitimate businesses such as the movie business and textile industry have become targets of criminals from the former Soviet Union, and they are often used for money laundering. A major 1999 money laundering case is illustrative of this recent Russian organized crime activity. That case also involved the Bank of New York (BONY). In 1999, four individuals and two companies were indicted by the United States in connection with the laundering of more than $7 billion (some estimates range up to $10 billion).
- Finally, Russian organized crime clearly has the capacity to tap professional know-how in its financial schemes. As this case and the stock fraud cases demonstrate, some of those associated with Russian organized crime work primarily in the legitimate sectors of the economy.
- The regional department for combating organized crime in the Urals estimates that the theft and export of strategic and precious metals, especially aluminum and copper, is a major source of income for the region's criminal organizations. Those officials charged with managing the metals aid the thefts, and foreign delivery is made possible by the payment of bribes for the necessary export licenses. The stolen raw materials are sold abroad through well-organized networks, and the moneys received in payment are deposited into accounts held in foreign banks by "shell" companies that exist only on paper.
- The arsenals, military units, and defense facilities based in the region are the sources of weapons dealt in arms trafficking. Criminal organizations exploit the weakened military discipline, poor morale, and corruption of military command staff to obtain weapons through both theft and purchase. These arms are then sold abroad via the thriving black market in arms and defense equipment.

4. Motivation

- Detecting and following the behavioral pattern of adversaries in the cyber domain can often be challenging. Attribution issues, the technical nature of cyberwarfare, its recent and rapid evolution, its ephemeral effects, and the covert ways in which it is often used tend to obscure the motivations and strategies of the actors involved. The conceptual challenges associated with cyber mean that threats are often analyzed from a purely tactical and defensive perspective. Media reporting and forensic analysis usually focus on the origins and vectors of cyberattacks, the techniques and tools they use, their impact, and how their effects can be defended against or mitigated

- We make uninformed assumptions about their motivations, intentions, and risk calculations based on U.S. thinking about cyber. However, this can be misleading, and in some instances, dangerous. Adversaries, whether state or non-state actors, are likely to view interactions in cyberspace very differently than we do.
  How they integrate cyber into other warfare domains, how they calculate risk and perceive escalation in cyberspace, and the strategies they use to achieve their objectives in cyberspace are all likely to vary by considerable degrees. In more succinct terms, a one-size-fits-all approach to dealing with adversaries in cyberspace will not work.

5. Affiliations

- In Russia, for example, authorities there generally will not initiate a cybercrime investigation against one of their own unless a company or individual within the country's borders files an official complaint as a victim. Ensuring that no affiliates can produce victims in their own countries is the easiest way for these criminals to stay off the radar of domestic law enforcement agencies.
- Dark Side, as compared to many other malware strains, has a hard-coded do-not-install list of countries which are the principal members of the Commonwealth of Independent States (CIS) — former Soviet satellites that mostly have favorable affiliations with the Kremlin. The full exclusion list in Dark Side (published by **Cybereason,** XDR Company partnering with Defender) is below:

Russian - 419	Azerbaijani (Latin) - 42C	Uzbek (Latin) - 443	Uzbek (Cyrillic) - 843
Ukranian - 422	Georgian - 437	Tatar - 444	Arabic (Syria) - 2801
Belarusian - 423	Kazakh - 43F	Romanian (Moldova) - 818	
Tajik - 428	Kyrgyz (Cyrillic) - 440	Russian (Moldova) - 819	
Armenian - 42B	Turkmen - 442	Azerbaijani (Cyrillic) - 82C	

6.1 Famous hacks

- Murat Urtembayev — The first Soviet hacker
- Stepanov, Petrov, and Maskakov — The first hackers to be sentenced in Russia
- Vladimir Levin — A hacker who allegedly turned $100 into $10 million
- Evgeniy Bogachev — A hacker with a $3 million bounty on his head

A chronology developed by NBC News from U.S. intelligence sources shows Russia was involved in the following attacks:

- April – May 2007: Estonia, a tiny Baltic nation that was occupied by the Soviet Union until 1991, angered Moscow by planning to move a Russian World War II memorial and Russian soldiers' graves. Russia retaliating by temporarily disabling Estonia's internet, an especially harsh blow in the world's most internet dependent economy. The distributed denial of service (DDoS) attack focused on government offices and financial institutions, disrupting communications.
- June 2008: In a similar attack, Russia punished another former possession in the Baltic. When the Lithuanian government outlawed the display of Soviet symbols, Russian hackers defaced government web pages with hammer-and-sickles and five-pointed stars.
- August 2008: After Georgia's pro-Western government sent troops into a breakaway republic backed by Moscow, Russian land, sea and air units invaded the country – and Russian hackers attacked Georgia's internet, the first time Russia coordinated military and cyber action. Georgia's internal communications were effectively shut down.
- January 2009: As part of an effort to persuade the president of Kyrgyzstan to evict an American military base, Russian hackers shut down two of the country's four internet service providers with a DDOS attack. It worked. Kyrgyzstan removed the military base. Subsequently, Kyrgyzstan received $2 billion in aid and loans from the Kremlin.
- April 2009: After a media outlet in Kazakhstan published a statement by Kazakhstan's president that criticized Russia, a DDOS attack attributed to Russian elements shut down the outlet.
- August 2009: Russian hackers shut down Twitter and Facebook in Georgia to commemorate the first anniversary of the Russian invasion.
- May 2014: Three days before Ukraine's presidential election, a Russia-based hacking group, took down the country's election commission in an overnight attack. Even a back-up system was taken down, but Ukrainian computer experts were able to restore the system before election day. Ukrainian police say they arrested hackers who were trying to rig the results. The attack was aimed at creating chaos and hurting the nationalist candidate while helping the pro-Russian candidate. Russia's preferred candidate lost.

6.2 Famous hacks

- March 2014: For the second time, the Russian government allegedly coordinated military and cyber action. A DDOS attack 32 times larger than the largest known attack used during Russia's invasion of Georgia disrupted the internet in Ukraine while Russian-armed pro-Russian rebels were seizing control of the Crimea.
- May 2015: German investigators discovered hackers had penetrated the computer network of the German Bundestag, the most significant hack in German history. The BfV, German's domestic intelligence service, later said Russia was behind the attack and that they were seeking information not just on the workings of the Bundestag, but German leaders and NATO, among others. Security experts said hackers were trying to penetrate the computers of Chancellor Angela Merkel's Christian Democratic party.
- December 2015: Hackers believed to Russian took over the control center of a Ukrainian power station, locking controllers out of their own systems and eventually leaving 235,000 homes without power.
- June 2015 - November 2016: In the U.S., Russian hackers penetrated Democratic party computers, and gained access to the personal emails of Democratic officials, which in turn were distributed to the global media by WikiLeaks. Both the CIA and the FBI now believe the intrusions were intended to undermine the election, hurt Hillary Clinton and help Donald Trump win.
- October 2015: Security experts believe that the Russian government tried to hack into the Dutch government's computers to pull out a report about the shoot down of Flight MH17 over Ukraine. The Dutch Safety Board headed the investigation of the Malaysia Airlines downing, and concluded that the passenger plane was brought down by a Russian-made missile fired from an area held by pro-Russian rebels.
- January 2016: A security firm announces that it believes Russian hackers were behind attacks on Finland's Foreign Ministry several years before.
- December 2016: Earlier this month, BfV head Hans-Georg Maasen warned "There is growing evidence of attempts to influence the federal election next year," referring to German parliamentary elections likely to take place in September 2017. Maasen specifically cited Russia as the source of the attacks, adding, "We expect a further increase in cyber attacks in the run-up to the elections." Experts believe the Russians are trying to damage incumbent Chancellor Merkel, who supported sanctions against Putin's personal associates after Russia annexed Crimea.

Scott Borg, president of U.S. Consequences Unit, a cybersecurity firm that tracks Russian attacks, says that even as Russia's ambition grows it also acts on a much smaller scale. Said Borg, "They have tried to influence local elections in three or four eastern European countries as well as Germany."

References

https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf

https://idstch.com/geopolitics/russias-influence-operations-cyber-attacks-warfare-campaigns-and-motives/

https://krebsonsecurity.com/2021/05/try-this-one-weird-trick-russian-hackers-hate/

https://www.ojp.gov/pdffiles1/nij/187085.pdf

https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111