[redacted]

[redacted] Issues Arising from Russian Cyber Intrusion and Destructive Attack Campaigns Targeting Ukraine

Ongoing cyber espionage and attack campaigns mounted against Ukraine by the government of Russia through its intelligence services, associated contractors and other proxies, have resulted in significant disruption and destruction of critical infrastructure, elections processes, and government / intelligence / military communications.

Irresponsible deployment of malware during these incidents has resulted in substantial collateral damage to US, allied and partner systems and networks world-wide.

Capabilities, talent, and infrastructure used in these campaigns has also been leveraged by intrusion set operators to target other global victims, including US and Western critical infrastructure and other key resources.

US response options to date have included public attribution, indictment, law enforcement led takedown operations targeting malware infrastructure, and sanctions. These actions have imposed some costs, but it is unclear whether such actions have changed adversary decision calculus, as associated threat activity continues and remains a matter of ongoing concern.

Overview

Sustained campaigns intended for espionage, sabotage, and prompt destructive effects have been mounted against government, military, and critical infrastructure networks by multiple intrusion sets attributed by industry to the Russian intelligence services and armed forces. These campaigns, ongoing since at least 2012, if not earlier, have resulted in both periodic incidents of major significance including disruption of electrical and transportation critical infrastructure, attempts to interfere with elections and other political system processes, as well as persistent cumulative effects due to loss of confidentiality of national security communications and reported battlefield impacts. The effects of these campaigns have reached beyond the country to include substantial collateral damage from uncontrolled destructive incidents. Russian offensive cyber operations in Ukraine are also believed to serve as a live-fire "battlelab" in which the armed forces and intelligence services may experiment with new capabilities, novel tactics, techniques, and procedures (TTP), and the improved integration of cyber planning and execution with traditional combined arms and active measures instruments. Offensive infrastructure, developer and operator talent, and tooling used in these campaigns have also been linked to other ongoing global cyber threat activities including espionage against US, NATO, as well as other allied and partner countries, and the suspected reconnaissance and operational preparation of the environment (OPE) for potential future destructive action against critical infrastructure systems and networks.

Context

Russian leadership has expressed various strategic interests in controlling Ukraine and other countries within the "near abroad" of former Soviet states. This includes access to port facilities, control of key pipeline and other transportation connectivity with Europe, access to legacy defense industrial base resources that remain critical to production and sustainment of multiple Russian military platforms, and a perceived utility in ensuring the country continues to serve as a buffer for strategic depth between core Russian state borders and NATO members states. The degree to which the Kremlin weighs these interests in action remains unclear, but Russia has sought to exert

[redacted]

[redacted]

[redacted]

influence through covert action and hybrid operations in Ukraine as in many states in the near abroad.

These activities accelerated following a "color revolution" or "Arab Spring" like shift in existing political equilibrium in late 2013 and early 2014 commonly known as Euromaidan, where popular pressure in the form of protests and mass demonstrations seeking to increase Kiev's alignment with the European Union led to the removal ofthen President Viktor Yanukovych and a change in Ukraine's government. As a result of these events, which were seen as an immediate threat to sustained Russian influence, the Kremlin accelerated covert intervention against the country using both kinetic and cyber operations.

Significant events

In the wake of the Maidan events, the people of Ukraine faced a difficult conversation with themselves regarding the nature of the government that should be formed, and the kind of policies that should emerge in order to address the divergent equities of differing political viewpoints. Political parties generally aligned against Russian interests had previously suffered ongoing cyber attack in multiple unattributed incidents since at least 2011, including distributed denial of service attacks which had over time impacted the ability to organize and communicate with supporters. While conclusive attribution in these cases was not reached, these incidents are consistent with other cases of Russian covert action by intelligence services reportedly leveraging contract hacker for hire services as proxies against multiple targets in other crises. These events continued and escalated after the "Revolution of Dignity" as the country prepared for new elections.

Intrusion operations targeted the Central Election Commission during the elections of May 2014. Adversary operators delivered destructive effects through deployment of wiper malware against the Commission's networks, and after the government of Ukraine rallied a unique public-private partnership to recover systems in order to conclude ballot counting and finalize results, attempred to further interfere by altering the integrity of publicly announced results. While these actions were claimed by CyberBerkut, a purported ideologically motivated hacktivist group, industry cyber threat researchers attributed the incidents to the intrusion set ISOTOPE / BERSERK BEAR / ALLANITE commonly linked to the Russian intelligence services.

The continued contested political environment in Kiev resulted in Russian military intervention in mid 2014 - initially conducted through irregular forces supported by covert special forces advisors and direct action elements (so-called "little green men"), but escalating to include multiple unacknowledged deployments involving units of the Russian armed forces. Military operations resulted in seizure of the Crimea and additional territories in the eastern regions of Ukraine, including the Donetsk and Luhansk areas of the Donbas province. Tactical gains by Russian forces were supported by extensive electronic warfare activities, as well as offensive cyber operations directed against Ukrainian military tactical communications networks, targeting technologies, and headquarters information environments. The government of Ukraine has disputed the impacts of these intrusions, issuing denials in part due to political sensitivities but also likely due to a lack of organic capacity to evaluate technical and operational observables. Independent commercial cyber intelligence has however provided extensive reporting detail regarding multiple aspects of these actions. The fighting also drove intensified hostile propaganda operations intended to degrade the morale of Ukrainian armed forces and its supporting populations, including messaging carried out

[redacted]

through coordinated inauthentic activity via social media as well as direct threats delivered to specific mobile devices based on geographic or relationship targeting.

As events at the front began to stalemate, Russian intrusion sets began to seek strategic effects through operations targeting the country's critical infrastructure networks. These actions were likely intended to damage civilian economic interests, exacerbate perceptions of chaos and other conflict impact, and to reinforce messaging that the Kiev government was too weak to control the country. The actions also allowed adversary planners and offensive cyber operators to gain experience, develop and test new operational capabilities, and evaluate the effects and recovery after destructive action. Destructive intrusion events initially leveraged existing intrusion infrastructure and tooling as operators turned from espionage objectives to sabotage and direct attack. In October 2015, access provided through initial foothold using a customized variant of the commodity criminal malware commonly known as BlackEnergy, leveraged as part of the sustained SANDWORM / VOODOO BEAR / IRON VIKING / ELECTRUM intrusion set, was used to deliver destructive wiper malware against aviation and light rail transportation, as well as media targets, in Kiev. Further attempts against other rail transport targets continued in early December 2015, and operators expanded destructive action to include electrical utility targets, delivering effects through manually interactive operator commands intended to disrupt elements within the country's electrical distribution grid. Impact was limited and temporary in nature due to the victim utility's ability to fallback on analogue and mechanical processes to quickly restore power. Transportation sector targets would continue to be targeted in January 2016, with additional espionage against aviation and railway networks with suspected intent as operational preparation of the environment.

Attackers struck again in destructive actions leveraging intrusion access across the financial sector, including the national Treasury, in December 2016. These events leveraged access through a new malware variant known as Telebots / STRAYKEY, repurposed from commodity open source tooling, and delivered destructive effects through a wiper malware variant tracked as WHITEROSE. Industry continued attribution of this intrusion to Russian intelligence services as part of the SANDWORM / VOODOO BEAR / IRON VIKING / ELECTRUM activity group. Destructive action would again target electrical sector victims in December 2016, with deployment of a new custom developed malware variant known as CRASHOVERRIDE / Industroyer, intended to deliver deliberate weaponized effects against victim critical infrastructure through malicious instructions to manipulate electrical circuit flow. This attack also had limited effect, as adversary operators apparently did not anticipate response actions by the targeted utility and failed to deliver more significant follow on effects that could have resulted in further destruction under other scenarios. Destructive intrusions against other targets, deploying Moonraker Petya modified ransomware variant intended for nonreversible effects, would also be observed in December 2016.

The use of criminal ransomware as a destructive payload would continue in June 2017, where adversary operators would deploy a second modified Petya variant through a compromised software update infrastructure of an accounting application package mandated by law for use by all businesses operating in the country. The NotPetya / Nyetya malware would propagate through exploitation of a wormable vulnerability first disclosed in April 2017, when an unattributed group calling itself the Shadowbrokers released exploit code purported to have been stolen from classified US government offensive cyber operations activity. Adversary operators failed to take adequate measures to understand the target environments in which NotPetya / Nyetya implant was deployed, resulting in extensive global collateral damage as the malware infected the unsegmented corporate networks of US, European and other firms doing business in Ukraine. Despite the high profile nature of this

[redacted]

failure, the same operators would attempt restrike in October 2017 through yet another modified ransomware variant tracked by industry as BadRabbit. Effects against aviation, rail, and media networks were reported. This attack may have been intended as earlier follow-on to the prior incidents, but warning issued by the Ukrainian Security Service (SBU) may have altered adversary timelines. The NotPetya / Nyetya and BadRabbit campaigns would again be attributed by cybersecurity industry reporting to Russian intelligence service SANDWORM / VOODOO BEAR / IRON VIKING / ELECTRUM activity.

Further attempted critical infrastructure targeting was noted through 2018 involving a new malware variant known commonly as VPNFilter, attributed in Department of Justice public indictment to APT28 / FANCY BEAR / IRON TWILIGHT / STRONTIUM activity, which included a purported attempt to target water sector utilities and associated chlorine toxic industrial chemical storage. Elections held in spring 2019 would again result in espionage operations targeting the political process and its associated infrastructure, along with media organizations providing access to potential victims, in incidents tracked by industry in connection with ISOTOPE / BERSERK BEAR / ALLANITE activity groups. Associated influence campaigns through misattribution front leak websites were also noted. Additional continuing espionage against Ukraine government, intelligence service, and military networks tracked in connection with other Russian attributed intrusion sets, including TeamSpy / IRON LYRIC; Armageddon / SPICEY HONEY, and Vermin, has also been subsequently reported. These accesses may provide both espionage value and pre-positioned access for future delivery of disruptive or destructive effects.

[redacted]

[redacted]

[redacted]