Threats Associated with Russia-Ukraine Conflict

Russia Invades Ukraine

As geo-political tensions continue to rise in the wake of the Russian invasion of Ukraine cyber offensive actions targeting Ukraine are also underway. it is anticipated that Russian state-sponsored cyber attacks could also be launched against organisations outside of Ukraine in conjunction with the invasion.

The US and the UK have issued warnings on cyber attacks, and Adarma believe these concerns are justified based on previous undisciplined Russian APT cyber attacks that initially targeted Ukraine only to spread wider. It is plausible that Russia would seek to conduct cyber attacks against NATO countries to distract efforts and attention away from the invasion of Ukraine and to retaliate against the ongoing sanctions that have been put in place.

Russia's Actors, Tactics and Capabilities

Throughout Russia's staging, prior to the invasion of Ukraine, a predictable pattern of cyber activity has been observed that aligns with their doctrine of deception known as "Maskirovka". This aims to add to the "fog of war" by conducting denial of service attacks on information systems that support the target country's critical national infrastructure and through the widespread dissemination of disinformation and propaganda.

Russian military intelligence used this phase of operations to gain footholds by breaching government and private sector organisations in advance of a physical invasion. In the current stage of the conflict, simultaneous cyber-

bombardment of telecommunications providers, news outlets, financial services, and energy and telecommunications providers is to be expected.

Although we are likely to see, mass defacement, consolidation of footholds and denial of service attacks, more destructive capabilities are likely to be reserved for systems that support military functionality only as any occupation will require to use the in-situ national infrastructure to consolidate any military gains made.

Russia operates multiple groups of cyber-capable resources across their military and intelligence services, and they are also thought to engage with private sector (crimeware) gangs to augment their capabilities. The major actors that participate in Russia's information warfare campaigns are:

1. GRU (Military Intelligence Agency) – this agency is broken down into several parts, with sections responsible for psychological operations / social engineering, disinformation as well as deploying more typical cyber strike weapons (denial of service attacks, credential stuffing and brute force attacks). Known widely as APT28, Fancy Bear and Sandworm, their main effort currently will likely be focused on Ukraine and supporting the advance of the invading forces.
2. SVR (Foreign Intelligence Service) – this is the Russian equivalent of the Secret Intelligence Service (MI6) in the UK or the CIA in the United States. Known as APT29, Cozy Bear and The Dukes, their main effort will probably remain on infiltrating and disrupting any international response to the conflict in Ukraine.
3. FSB (Federal Security Service) – the Russian equivalent of the Defence Security Service (MI5) in the UK. Known as Beserk Bear, Energetic Bear and a vast number of other designators, the FSB's main focus will likely remain on propaganda dissemination throughout their own populace and identifying / silencing domestic dissent online.
4. FSO (Federal Protective Service) – maintains responsibility for the defence of Russian domestic information systems, including their nuclear weapons control systems. This grouping whilst cyber capable does not appear to have an offensive strategy and thus has not been assigned a designator.
5. Internet Research Agency – a private organisation, funded by an oligarch connected to the Kremlin. Provides troll farm services which impersonate foreign domestic activists on social media channels to sow discord or further Russian influence abroad.

Organisations should consider each of these actors and analyse their deployed controls against the tools, techniques, and procedures that each group is known to employ. For prioritisation purposes, for organisations out with Ukraine, APT29 should be the first group to threat model.

DDoS and Ransomware Attacks Anticipated

It is likely that cyber offensive actions targeting Ukraine will primarily consist of DDoS attacks and defacement activity against Ukrainian government, media organisations, internet infrastructure, and e-services used by Ukrainian citizens such as digital banking. These cyber attacks would likely aim to cause confusion, hinder communications, weaken Ukrainian military response, and demoralise the Ukrainian population as part of a wider hybrid warfare operation.

Two cybersecurity firms with a strong business presence in Ukraine—ESET and Broadcom's Symantec—have reported that computer networks in the country have been hit with a new data-wiping attack. Our threat analysis indicates that the deployment of that first malware (named WhisperGate) was hidden under the guise of a fake ransomware outbreak and during a series of coordinated defacements of Ukrainian government websites.

Details about the attack are still being collected, and the attack is still ongoing. The scale and number of impacted systems is still unknown.

While attacks are currently targeting at Ukraine, from recent history we can expect that undisciplined DDoS attacks will likely have a much wider impact. An example of a cyber attack likely intended to target Ukraine specifically is the Sandworm Team's NotPetya attack in June 2017, which was estimated to have cost victims more than $10 billion in total. The attack first targeted Ukrainian companies on June 27 2017, but quickly spread to other countries, including the US, UK, France, Germany, Italy, Poland, and Australia. Even Russia was not immune from the attack. There was temporary disruption of public infrastructure and business, destruction of data, and significant economic damage across 65 countries.

What Adarma is doing

The Adarma SOC, in response, has stepped up its focus based on our intelligence. Increasing capacity and capability of the threat team. Threat Analysts and Modellers are constantly reviewing threat intelligence to ensure we are on top of an ever-changing situation.

Threat hunts have been initiated and this work will continue as we develop, test and implement detection content.

A dashboard has been deployed on your environment utilising current tactical indicators of compromise which will be updated as we obtain additional intelligence. This includes coverage for whispergate, hermetic wiperware, cyclops blink and other historical campaigns where attribution has been linked to Russian activity.

Adarma is mapping known TTP's to detective controls, and your engineer will be working to understand available telemetry and expedite control deployment. If you have any immediate concerns or need more urgent information, please contact Adarma service delivery, however full details will be provided during your scheduled service delivery calls.

Get prepared

Based on current intelligence, we do not believe that wiper attacks are automated. If a malicious actor cannot obtain elevated privileges, there is less chance that the malware can be deployed across a wide number of devices. However, we do believe that DDOS attacks and defacement work is significantly more likely. This threat is greatly increased if the company in question has an office in the impacted zone.

The threat is immediate and ongoing, and while longer term projects (such as segmentation) should continue, we are recommending that customers immediately address the following areas:

1. Identify unpatched systems and ensure they are re-patched as a matter of urgency
2. Verify that management interfaces of internet facing network devices are secure and monitored
3. Implement Multifactor Authentication
4. Verify if you or 3rd party network provider have any watchguard devices deployed
5. Ensure backups are in place for critical assets