Threat Intelligence Alert: Russia/Ukraine Conflict

Threat Intelligence Alert

COPYRIGHT AND CONFIDENTIALITY STATEMENTS

CONTROL INFORMATION

Document Title	Threat Intelligence Alert: Russia/Ukraine Conflict
Version	1.3
Publication Date	24/02/2022
Classification	PUBLIC

Version	Date	Author	Change Summary
1.0	24/02/2022	Strategic Threat Intelligence Practice	Report Created
1.1	25/02/2022	Strategic Threat Intelligence Practice	TTPs Updated
1.2	28/02/2022	Strategic Threat Intelligence Practice	Context Updated
1.3	05/04/2022	Strategic Threat Intelligence Practice	FAQ and Additional Tools Added

Table of Contents

FAQ: Updated 05/04/2022

While NCC Group is part of several intelligences sharing collectives we do not have the level of access that is enjoyed by military or intelligence agencies. The following comments are predictions based upon our understanding of geopolitics and how this influences the cyber threat landscape, using open-source reporting and telemetry from our global network of incident responders and managed detection and response services.

Where is the cyber offensive from Russia?

On January 17th NCSC UK published a general advisory detailing how organisations can enhance their security posture in the event of a heightened cyber threat. The message came in preparation for a possible escalation of the brewing Russia-Ukraine conflict, yet to develop into a war, and was echoed by the additional five eyes nations (Australia, Canada, New Zealand, United Kingdom and United States). Since then, we have observed repeated warnings from the cyber security wings of the five eyes nations, in particular, highlighting the risk to critical national infrastructure.

In a joint advisory CISA (the US Cyber Security and Infrastructure Security Agency), the FBI (US Federal Bureau of Investigation) and the DoE (US Department of Energy), highlighted TTPs demonstrated by Russian threat actors attributed to the Russian Federal Security Service (FSB) during a global energy sector intrusion campaign, between 2011 and 2018. During this period, the Ukrainian power grid was crippled by CRASHOVERRIDE malware which is also attributed to Russian Military Intelligence (GRU). There are of course many other examples of Russian APT activity such as the 2015 compromise of the German Parliament[1], the 2016 breach of the Democratic National Committee network, the 2018 Olympic Destroyer cyber-attacks on the Winter Olympics hosted by South Korea, the 2021 compromise of French Software company Centreon[2], and the SolarWinds Supply chain attack, the list goes on.

With all of these examples, the capability of Russian APT groups is clear and the warnings are a prudent step. However, outside of the collection of destructive wipers, defacement and DDoS attacks aimed at Ukrainian services, the offensive capabilities of the Russian state have yet to be evidenced in this conflict. So where is Russia's fearsome cyber capability?

Theory 1 - Military Support

Russian state cyber capability has focused on supporting the military effort within Ukraine, which has faltered in recent weeks, including efforts to hamper communications within Ukraine, prevent resupply and logistical support flowing in from international aid. The most recent example, a cyber-attack on Ukrtelecom (Ukrainian telecoms provider) reducing their connectivity to just 13%[3].

Theory 2 - Defensive Operations

Russian state cyber capability is focused on bolstering defensive operations within Russia. Undoubtably, western nation states are targeting Russian infrastructure seeking intelligence and potentially footholds in case of further escalation, in addition to an influx of targeting by hacktivist groups such as Anonymous. We have seen a number of significant leaks including

[1] EUR-Lex - 32020R1536 - EN - EUR-Lex (europa.eu)

[2] GB Sandworm intrusion set campaign targeting Centreon systems – CERT-FR (ssi.gouv.fr)

[3] Ukraine war: Major internet provider suffers cyber-attack - BBC News

the names, addresses, phone numbers, license plates etc of 620 FSB employees[4], and several prominent Russian organisations including the Central Bank of Russia, have had significant volumes of data leaked. The Russian Foreign Ministry highlighted that Russia was suffering from sustained and coordinated cyber-attacks by "Ukrainian special ICT operations centres, trained by the US and other NATO experts". Additionally, this is "being reinforced with anonymous hackers and trolls", whilst the relevant Russian agencies are engaged in repelling these attacks and prioritising the bolstering defences[5].

Will we see any offensive cyber activity from Russian APT groups?

The statement from the Russian Foreign Ministry includes a clear indication that there will be repercussions for the cyber-attacks they have suffered:

"Nobody must have any doubt that the cyber aggression being waged against Russia will have dramatic consequences for its inspirers and operators. The sources of these attacks will be identified, and the culprits will inevitably be called to account for their activities in accordance with the law."

While the statement does indicate that these repercussions would be in accordance with the law, the Russian military has suffered a great deal of embarrassment due to the lack of progress in Ukraine and has weakened their position on the world stage. It is therefore possible that we will see a significant cyber-attack at some stage soon, in an attempt to regain some of the fear factor.

The most likely scenario emanating from Russia is increased activity from the various organised crime groups operating within Russia. These financially motivated groups are extremely capable and highly active. They will now be further incentivised by the ideological drive to defend their nation and in response to the sanctions, target western organisations.

Are there areas of increased threat that organisations should focus on?

Throughout the Russian invasion of Ukraine, there has been a strong focus on nation-state driven threats and the impact that these might have on critical infrastructure. As the operation enters its second month, we are reassessing the threats related to this conflict.

Supply Chain

Both Russia and Ukraine are responsible for either producing or providing means to transfer high volumes of gas and agricultural commodities. For example, both countries are the top exporters of sunflower seeds or crude sunflower oil in the world[1]. Undoubtedly, Europe is heavily reliant upon those products. The disruption of production and logistics to these goods would cause shortages beyond the immediate areas of conflict. Hence, attacks on the supply chain of commodities such as wheat, sunflower oil and metal, become attractive due to the high impact that this might cause. These attacks could vary from directly disrupting the production units to the various stakeholders in the supply chain such as freight, storage, or even software and systems providers.

[4] Ukraine spy agency posts names and addresses of more than 600 'Russian agents working for the FSB' | The Independent

[5] Foreign Ministry statement on continued cyberattack by the "collective West" - The Ministry of Foreign Affairs of the Russian Federation (mid.ru)

Insider Threat

The insider threat category is ever present in organisations both in terms of malicious and accidental insiders, the international response to this conflict and in particular the hacktivism we have observed may also play a part in increasing the malicious insider threat through ideological motivations. We have seen multiple organisations announce that they are ceasing operations in Russia and the dark web is awash with lists of organisations that are still active within Russia. This is fuelling the increase in hacktivism but it could also inspire ideologically driven employees to carry out malicious acts against their own company, if they are perceived as maintaining an impartial or supportive stance against Russia. Threat groups can take advantage of this, in the past we have seen active attempts to recruit insiders. In a politically polarised world, it is increasingly likely to observe such ideological drivers result in malicious insider activity.

As the conflict continues to last longer than initially expected, threat actors have had sufficient time to assess their options and make the right contacts within potential targets to facilitate possible attacks. The use of affiliates acting on behalf of threat actors is a popular business model amongst financially driven threat actors, as such, it would not come as a surprise if we were to observe this method during the conflict.

Hacktivists

With similar motivations to the ideologically driven malicious insider, hacktivist groups have been actively involved in targeting Russian State apparatus and organisations which continue to operate within Russia. As we have witnessed more recently, the hacker collective Anonymous have been steering their attacks towards Russian websites. Specifically, they were responsible for leaking the personal data of Russian FSB operatives and taking control of Russian TV channels to broadcast footage of the invasion in Ukraine. In addition, numerous hacktivists are acting autonomously as well as in small groups, offering up their skillset to upset the natural flow of information on the internet.

Furthermore, Ukrainian officials publicly sought the contributions of an “IT army” to assist in their defence against the Russian invasion, and the response thus far has been overwhelming. These cyber volunteers have focused mainly upon launching DDoS attacks against important Russian websites, or conducting breach and leak campaigns on highly valuable databases such as the Russian Space Research Institute website[1]. We should however bear in mind that hacktivism functions in both directions, and as such, hacktivists could run operations in favour of Russia. Consequently, the likelihood of malicious activity aimed towards Western organisations who have overtly shown their support for Ukraine should not be overlooked.

Opportunists

Another area of increased activity is from opportunist hackers using the invasion of Ukraine as a theme in their phishing campaigns. These groups act independently and their primary motivation is financial gain. The Russia/Ukraine conflict has provoked a great deal of global interest, consequently, all information related to this topic is highly likely to attract the attention of the recipient of the phishing email. Opportunistic hackers try to capitalise on this by using documents influenced by the Russian invasion in their phishing campaigns to lure their perspective victims. These documents aim to gain initial access by executing malicious macros or triggering template injections[2]. It is a long-standing trend by threat actors to adapt their phishing campaigns to geopolitical conflicts or other major events.

Organised Crime Groups

Organised crime groups (OCGs) have overwhelmingly embraced Ransomware either in isolation or where offering Ransomware as a Service. While we have theorised that we would see an increase in activity from financially motivated threat actors like OCGs in Russia due to the economic sanctions, we have yet to observe such a trend.

Using ransomware as a measure of OCG activity we have observed a pattern between Q4 2021 and Q1 2022 for the hack & leak ransomware targeting of European organisations; there has been a gradual increase however this is not indicative of a conscious change in targeting preference.

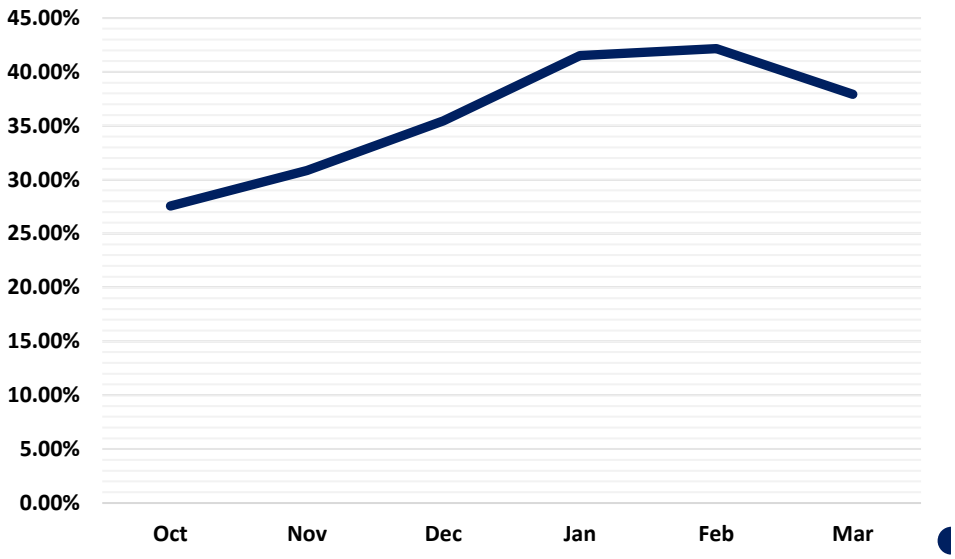

Figure 1: Percentage of European Ransomware Hack and Leak Victims (of the monthly global total)

As can be seen in the graph above, there has been a gradual but visible increase in European victims from October to February, with a moderate decline in March 2022. Throughout the entirety of Q1 2022, Europe accounted for 40% of all ransomware hack & leak victims, which is one of the largest weightings that we have seen on a quarterly basis.

The US authorities have released a warning[6] on the 21st of March following increased scanning activity originating from Russia against US organisations[7]. This follows a theme of consistent messaging from Western nations of increased threat from Russian-based threat actors. NCC Group will continue to monitor the regional targeting as we progress through 2022 to see if a true pattern begins to materialise.

Nation States

As is to be expected with highly impactful geopolitical events, various nations have their own agendas and often take advantage of the resulting confusion and panic. During Russia's invasion of Ukraine, malicious cyber activity by seemingly uninvolved nation states using the war in phishing lures to carry out their own unrelated cyber espionage operations has been documented. According to Checkpoint researchers, three APT groups were observed

[6] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/

[7] https://news.sophos.com/en-us/2022/03/22/as-russias-ground-advance-stalls-biden-warns-of-an-increase-in-cyberattacks/

carrying out this activity, El Machete (Spanish-speaking Country Group), Lyceum (Iranian Group), and SideWinder (thought to be Indian)[8].

Of these APT groups, a plethora of lures have been used such as official-looking documents, news articles and even job postings contained within spear-phishing emails. For example, Lyceum sent an email to an Israeli energy company regarding "Russia War Crimes in Ukraine" with malicious Office documents containing macros to begin the infection chain. This activity shows that nation-states with motives far-removed from current geopolitical events use, and will likely continue to use, the current geopolitical context to facilitate cyber-attacks to their own ends. NCC Group will continue to monitor APT activity taking advantage of the Russia-Ukraine war for initial access as the situation in Eastern Europe continues to develop.

What steps should organisations be taking given the current situation?

To secure their critical assets during this period, organisations shouldn't deviate much from the basic principles of cyber security. As already indicated, organisations are heavily targeted due to the current climate in Ukraine, hence sophisticated phishing campaigns should be expected. Moreover, the threat from malicious insiders is an area of concern especially if the organisation has strong affiliations with the area of conflict. Additionally, extra focus is required to evaluate the security posture due to the latent longevity of the conflict. During the first two weeks of the offensive there was a natural reaction towards securing the "low hanging fruits". As the conflict continues, organisations should focus on the longer game and identify strategies to minimise the impact on a wider scale. Changes to the security policy of the company might be required to accommodate long term changes, and business continuity should remain at the heart of decision making.

It is crucial to identify the exposure of each organisation to the potential threats that may manifest as a result of this conflict. As mentioned, the threats evolve as the conflict changes shape and direction. Whether an organisation is dependent upon other markets and industries might be more relevant now compared to 4 weeks ago. Organisations should therefore try to identify any vendors or clients that might be newly impacted and how this may pose a threat to them.

Additionally, we must consider the impact of this conflict should it continue for a substantial amount of time. Again, as both Ukraine and Russia are responsible for supplying the rest of the world with certain commodities, the impact of any disruption would be multisectoral. Consequently, it is pivotal to identify the extent to which we rely upon certain products, and whether there are affiliations with any partners that may be impacted from their shortage. If so, alternative supplies might be considered, and a reassessment of the existing relationship should be taken into consideration.

NCSC (UK) has called on organisations in the UK to bolster their online defences, with similar advice being issued by their US and Australian counterparts, their advice can be found via the following links.

- Actions to take when the cyber threat is heightened - NCSC.GOV.UK
- Shields Up | CISA
- 2022-02: Australian organisations should urgently adopt an enhanced cyber security posture | Cyber.gov.au

[8] https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

Context: Russia/Ukraine Conflict

Russia Recognises Donetsk and Luhansk: 21/02/2022

On the evening of the 21st of February, Russian President Vladimir Putin officially recognised Donetsk and Luhansk as independent states. From an international perspective, these regions are considered part of Ukraine despite both declaring independence in 2014. Under the Minsk Agreement signed in February 2015, Ukraine retains full control of the state border throughout the conflict area but adopts permanent legislation on the special status of certain areas within Donetsk and Luhansk, allowing for local self-governance.[9]

Recognition by the Russian federation, which was a signatory of the Minsk Agreement in 2015, was arguably a breach of section 9 which relates to full control of state borders. The concern was that this would in turn result in a breach to section 10, which calls for the "withdrawal of all foreign armed formations, military equipment, as well as mercenaries from the territory of Ukraine". [10]

Following the Russian Parliament's decision to approve the use of Russian military forces outside of the country, there was an expectation amongst the western allies that this approval paved the way for weapons and troops to flood into Ukraine under the guise of "Peace Keeping".

US and UK Intelligence Agencies Disclose New Russian Malware: 23/02/2022

In a joint advisory, the UK National Cyber Security Centre (NCSC), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) disclosed details of a large-scale modular malware framework which is affecting network devices, "Cyclops Blink".

This malware is believed to be a replacement for the VPNFilter malware which was exposed and then disrupted by US authorities in 2018. It is reported that "Cyclops Blink " has been active since June 2019. The malware has been attributed to a Russian APT known as Sandworm, a group already linked to a number of cyber operations in the Ukraine, including the disruption of Ukrainian electricity in 2015 and the NotPetya ransomware variant in 2017.

Cyber-attacks impact Ukrainian Organisations: 23/02/2022

Two cybersecurity firms ESET and Broadcom's Symantec reported Wednesday evening that computer networks in the Ukraine have been hit with a new data-wiping attack. [11] The destructive malware is understood to delete or corrupt data, damage the master boot record and allow for the control of the internal network.[12]

The malware was identified across hundreds of machines in the country, including financial organisations and government contractors. Additionally, targets outside of the Ukraine included Ukrainian government contractors with a presence in those countries. [13] It is understood that the attack is ongoing with the wiper additionally detected in Latvia and Lithuania. This is the second attack concerning a data wiper following those in January, but who is responsible is still unknown. The West has warned of the potential for Russian cyber-attacks in the Ukraine and globally, in response to the crisis.

---

[9] https://www.ft.com/content/21b8f98e-b2a5-11e4-b234-00144feab7de
[10] https://www.ft.com/content/21b8f98e-b2a5-11e4-b234-00144feab7de
[11] https://therecord.media/second-data-wiper-attack-hits-ukraine-computer-networks/
[12] https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
[13] https://www.wsj.com/livecoverage/russia-ukraine-latest-news/card/malware-detected-in-ukraine-as-invasion-threat-looms-NaVfMTy8x0v41PyZNuzo

Russian Forces Enter Ukraine: 24/02/2022

At 05:55 on 24th February, Vladimir Putin authorised a "special military operation" for the 'demilitarisation' and 'denazification' of Ukraine.[14] In the moments following the televised statement explosions were reported near major Ukraine cities, and military facilities. International outcry has followed suit and Ukraine has accused Russia of starting a full-scale war, urging the UN 'to do everything possible to stop it'. This is the first invasion on European soil since 1939, and a major humanitarian crisis is unfolding.

Critically, Putin's statement warned that any response to Russia's intentions would be met with severe consequences: *"To anyone who would consider interfering from the outside: if you do, you will face consequences greater than any you have faced in history. All relevant decisions have been taken. I hope you hear me," he said.*[15]

Further Sanctions Imposed: 26/02/2022

The leaders of the European Commission, France, Germany, Italy, the United Kingdom, Canada, and the United States have jointly announced additional sanctions on Russia. Summarised below:

- Selected Russian banks are removed from the SWIFT messaging system
- Restrictions of Russian Central Bank
- Limitations on 'Golden Passports' which allow wealthy Russians with links to the Russian Government to become citizens of other countries to gain access to their financial systems
- Identification and freezing of assets of sanctioned individuals and companies[16]

The removal from the SWIFT messaging system is significant as it was previously proposed but rejected by nations such as Germany, who were concerned about retaliatory action via the vital energy supply they receive from Russia.

What is SWIFT?

SWIFT is an acronym for the Society for Worldwide Interbank Financial Telecommunication. It exists as a member-owned cooperative based near Brussels and was founded in 1973 to end reliance on the telex system. It facilitates secure messaging for over 11,000 financial institutions and companies across 200 countries and territories. Last year the average daily message traffic was 42 million per day including orders and confirmations of payments, trades and currency exchanges. More than 1% of these messages related to Russian payments.

[14] https://www.ndtv.com/world-news/vladimir-putin-orders-strikes-in-ukraine-what-he-said-in-televised-speech-2786109

[15] https://www.theguardian.com/world/2022/feb/24/russia-attacks-ukraine-news-vladimir-putin-zelenskiy-russian-invasion

[16] https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/26/joint-statement-on-further-restrictive-economic-measures/

So what?

NCC Group Threat Intelligence team considers the following sectors most at risk:

Financial – We have already observed attacks targeting financial services within Ukraine. A potential response from Russia as the economic sanctions take hold could include targeting of financial institutions across the world. The removal from the SWIFT messaging systems could shrink Russia's economy by 5%[17]. When Iran was removed from SWIFT due to their nuclear program it resulted in it losing approximately 30% of its foreign trade[18].

The most likely attacks will include an increase in disruption and extortion through ransomware, and possibly direct sabotage activities.

Critical National Infrastructure – As with financial institutions, we have seen targeting of critical national infrastructure within Ukraine already. Expansion of this targeting to western nations is possible, with Russia seeking to hinder and distract efforts in support of Ukraine, and again disruption through ransomware is likely.

Supply Chain – The Russian based threat groups have proven themselves capable of distributing their attacks using third parties for maximum impact. As such, it is likely to see targeting of professional and commercial service providers, managed service providers and IT support services. Seeking direct access to additional victims and disruption and extortion through ransomware.

While these sectors are considered the most likely targets as directed by Russian national interest, the economic sanctions will also impact the Russian population and criminal elements are likely to respond accordingly. As such, we expect to see an increase in ransomware operations across the board. There is also concern for collateral damage, we may well see unintended proliferation of destructive malware as a spill over from this conflict. We have already observed the latest destructive wiper impacting organisations in Lithuania and Latvia, as well as the case study provided by the spread of NotPetya in 2017.

We are also observing an increase in phishing with campaigns tailored around the Russia/Ukraine conflict seeking to capitalised on the growing global attention on this crisis.

[17] https://www.bbc.co.uk/news/business-60521822
[18] https://www.forbes.com/advisor/personal-finance/swift-russia-ukraine-war/

Now what?

NCC Group has initiated threat hunting across our MDR customers using the indicators of compromised (IOCs) we have identified from external reporting. Our threat intelligence team will continue to monitor the situation as it develops, and issue situation reports with our SOCs and incident responders. Any additional IOCs identified will be fed into our threat intelligence platform to support our defensive efforts.

NCSC (UK) has called on organisations in the UK to bolster their online defences, with similar advice being issued by CISA and the Australian Cyber Security Centre (ACSC).

- Actions to take when the cyber threat is heightened - NCSC.GOV.UK
- Shields Up | CISA
- 2022-02: Australian organisations should urgently adopt an enhanced cyber security posture | Cyber.gov.au

These advisories focus on what organisations can do in order to build resilience and stay ahead of any potential threats.

Technical Details

NCC Groups Threat Intelligence team has collated the following information relating to known TTPs of Russia based threat groups to support organisations defensive posture.

Tools

AcidRain – Russian wiper malware deployed against Viasat modems - https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

PartyTicket Wiper – "Unsophisticated and poorly designed ransomware family that is likely intended to be a diversion from the Hermetic wiper attack" - https://www.zscaler.com/blogs/security-research/technical-analysis-partyticket-ransomware

HermeticWiper –New destructive malware employed in Russian cyber-attacks on Ukraine observed from 23/02/22. https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/

IsaacWiper – Destructive wiperware targeting Ukraine. https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

Cyclops Blink – New malware attributed to Russian APT group Sandworm replaces the VPNFilter malware exposed in 2018 with a more advanced framework. https://www.ncsc.gov.uk/files/Joint-Sandworm-Advisory.pdf

WhisperGate – Destructive wiper observed targeting multiple Ukrainian organisations. https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

RURansom – First true wiper malware targeted at Russia, developed by a supposed hacktivist group that condemn Russia's invasion of Ukraine. https://blog.cyble.com/2022/03/11/new-wiper-malware-attacking-russia-deep-dive-into-ruransom-malware/

CaddyWiper – First identified by ESET – any links revealing greater technical details will be updated here. https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

Wellmess and **Wellmail** – APT29 identified using custom malware to target a number of organisations globally including organisations involved with COVID-19 vaccine development. https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

GoldMax, **GoldFinder**, and **Sibot –** These three pieces of malware were by APT29 to maintain persistence and perform malicious actions in targeted attacks. https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

SUNBURST, TEARDROP and Raindrop – Malware

https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware

Vulnerabilities

Vulnerabilities known to be exploited by Russian state-sponsored APT actors for initial access include:

- **CVE-2021-32648 October CMS**

  In affected versions of the October/system package an attacker can request an account password reset and then gain access to the account using a specially crafted request.

  https://nvd.nist.gov/vuln/detail/CVE-2021-32648

- **CVE-2018-13379 FortiGate VPNs**

  An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 and FortiProxy 2.0.0, 1.2.0 to 1.2.8, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 under SSL VPN web portal allows an unauthenticated attacker to download system files via special crafted HTTP resource requests.

  https://nvd.nist.gov/vuln/detail/CVE-2018-13379

- **CVE-2019-1653 Cisco router**

  A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to retrieve sensitive information. The vulnerability is due to improper access controls for URLs. An attacker could exploit this vulnerability by connecting to an affected device via HTTP or HTTPS and requesting specific URLs. A successful exploit could allow the attacker to download the router configuration or detailed diagnostic information.

  https://nvd.nist.gov/vuln/detail/CVE-2019-1653

- **CVE-2019-2725 Oracle WebLogic Server**

  Injection vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services).

  https://nvd.nist.gov/vuln/detail/CVE-2019-2725

- **CVE-2019-7609 Kibana**

  Kibana contain an arbitrary code execution flaw in the Timelion visualizer.

  https://nvd.nist.gov/vuln/detail/CVE-2019-7609

- **CVE-2019-9670 Zimbra software**

  "Improper Restriction of XML External Entity Reference vulnerability affecting Synacor Zimbra Collaboration Suite."

  https://nvd.nist.gov/vuln/detail/CVE-2019-9670

- **CVE-2019-10149 Exim Simple Mail Transfer Protocol**

  Improper validation of recipient address in deliver message() function in /src/deliver.c may lead to remote command execution.

  https://nvd.nist.gov/vuln/detail/CVE-2019-10149

- **CVE-2019-11510 Pulse Secure**

  An unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability.

  https://nvd.nist.gov/vuln/detail/CVE-2019-11510

- **CVE-2019-19781 Citrix**

  Issue in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0 allowing Directory Traversal.

  https://nvd.nist.gov/vuln/detail/CVE-2019-19781

- **CVE-2020-0688 Microsoft Exchange**

  A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka 'Microsoft Exchange Memory Corruption Vulnerability'.

  https://nvd.nist.gov/vuln/detail/CVE-2020-0688

- **CVE-2020-4006 VMWare**

  VMWare Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector address have a command injection vulnerability.

  https://nvd.nist.gov/vuln/detail/CVE-2020-4006

- **CVE-2020-5902 F5 Big-IP**

  In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.

  https://nvd.nist.gov/vuln/detail/CVE-2020-5902

- **CVE-2020-14882 Oracle WebLogic**

  Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server.

  https://nvd.nist.gov/vuln/detail/CVE-2020-14882

- **CVE-2021-26855 Microsoft Exchange**

  Microsoft Exchange Server Remote Code Execution Vulnerability.

  https://nvd.nist.gov/vuln/detail/CVE-2021-26857

MITRE ATT&CK Mapping

Tactic	Technique	Procedure
Reconnaissance [TA0043]	Active Scanning: Vulnerability Scanning [T1595.002]	Russian state-sponsored APT actors have performed large-scale scans in an attempt to find vulnerable servers.
	Phishing for Information [T1598]	Russian state-sponsored APT actors have conducted spearphishing campaigns to gain credentials of target networks.
Resource Development [TA0042]	Develop Capabilities: Malware [T1587.001]	Russian state-sponsored APT actors have developed and deployed malware, including ICS-focused destructive malware.
Initial Access [TA0001]	Exploit Public Facing Applications [T1190]	Russian state-sponsored APT actors use publicly known vulnerabilities, as well as zero-days, in internet-facing systems to gain access to networks.
	Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]	Russian state-sponsored APT actors have gained initial access to victim organizations by compromising trusted third-party software. Notable incidents include M.E.Doc accounting software and SolarWinds Orion.
Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]	Russian state-sponsored APT actors have used cmd.exe to execute commands on remote machines. They have also used PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and to execute other commands.
Persistence [TA0003]	Valid Accounts [T1078]	Russian state-sponsored APT actors have used credentials of existing accounts to maintain persistent, long-term access to compromised networks.
	Boot or Logon Initialization Scripts: RC Scripts [T1037.004]	Russian state-sponsored APT actors have executed on device start up, using a modified S51armled RC script

Tactic	Technique	Procedure
	Pre-OS Boot: System Firmware [T1542.001]	Russian state-sponsored APT actors have maintained persistence throughout the legitimate device firmware update process. This is achieved by patching the firmware when it is downloaded to the device.
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001] and Password Spraying [T1110.003]	Russian state-sponsored APT actors have conducted brute-force password guessing and password spraying campaigns.
	OS Credential Dumping: NTDS [T1003.003]	Russian state-sponsored APT actors have exfiltrated credentials and exported copies of the Active Directory database ntds.dit.
	Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]	Russian state-sponsored APT actors have performed “Kerberoasting,” whereby they obtained the Ticket Granting Service (TGS) Tickets for Active Directory Service Principal Names (SPN) for offline cracking.
	Credentials from Password Stores [T1555]	Russian state-sponsored APT actors have used previously compromised account credentials to attempt to access Group Managed Service Account (gMSA) passwords.
	Exploitation for Credential Access [T1212]	Russian state-sponsored APT actors have exploited Windows Netlogon vulnerability CVE-2020-1472 to obtain access to Windows Active Directory servers.
	Unsecured Credentials: Private Keys [T1552.004]	Russian state-sponsored APT actors have obtained private encryption keys from the Active Directory Federation Services (ADFS) container to decrypt corresponding SAML signing certificates.
	Proxy: Multi-hop Proxy [T1090.003]	Russian state-sponsored APT actors have used virtual private servers (VPSs) to route traffic to targets. The actors often use VPSs with IP addresses in the home country of the victim to hide activity among legitimate user traffic.

Tactic	Technique	Procedure
Command and Control [TA0011]	Data Encoding: Non-standard Encoding [T1132.002]	Russian state-sponsored APT actors command messages use a custom binary scheme to encode the specific command to be executed, as well as any command parameters required
	Fallback Channels [T1008]	Russian state-sponsored APT actors randomly select a C2 server from contained lists of IPv4 addresses and port numbers.
	Application Layer Protocol: Web Protocols [T1071.001]	Russian state-sponsored APT actors can download files via HTTP or HTTPS.
	Encrypted Channel: Asymmetric Cryptography [T1573.002]	Russian state-sponsored APT actors C2 messages are individually encrypted using AES-256- CBC and sent underneath TLS. OpenSSL library functions are used to encrypt each message using a randomly generated key and IV, which are then encrypted using a hard-coded RSA public key.
	Non-Standard Port [T1571 -]	Russian state-sponsored APT actors contain a list of port numbers used for C2 communication. This list includes non-standard ports not typically associated with HTTP or HTTPS traffic.
	Ingress Tool Transfer [T1105]	Russian state-sponsored APT actor adversaries transfer tools or other files from an external system into a compromised environment.
Defence Evasion [TA0005 -]	Impair Defenses: Disable or Modify System Firewall [T1562.004]	Russian state-sponsored APT actors have modified the Linux iptables firewall to enable C2 communication via a stored list of port numbers
	Masquerading: Match Legitimate Name or Location [T1036.005]	Russian state-sponsored APT actors have renamed its running process to masquerade as a Linux kernel thread
	Modify Registry [T1112]	Russian state-sponsored APT actors have interacted with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.

Tactic	Technique	Procedure
	Disable or Modify Tools [T1562.001]	Russian state-sponsored APT actors have modified and/or disabled security tools to avoid possible detection of their malware/tools and activities.
Discovery	System Information Discovery [T1082]	Russian state-sponsored APT actors regularly query device information.
Exfiltration	Exfiltration Over C2 Channel [T1041 -]	Russian state-sponsored APT actors are capable of uploading files to a C2 server.
Impact	Disk Structure Wipe T1561.002	Russian state-sponsored APT actors corrupt or wipe the disk data structures on a hard drive necessary to boot a system; targeting specific critical systems or in large numbers in a network to interrupt availability to system and network resources.
	System Shutdown/ Reboot [T1529]	Russian state-sponsored APT actors adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine.

Additional resources can be found here:

- Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure https://www.cisa.gov/uscert/ncas/alerts/aa22-011a
- Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders https://www.cisa.gov/uscert/ncas/alerts/aa21-116a
- Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments https://media.defense.gov/2021/jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF
- Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets https://www.cisa.gov/uscert/ncas/alerts/aa20-296a
- APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations https://www.cisa.gov/uscert/ncas/alerts/aa20-283a