COPYRIGHT AND CONFIDENTIALITY STATEMENTS
This document is Copyright © NCC Group. All rights reserved.

The contents of this document may not be copied or duplicated in any form, in whole or in part, without the prior written permission of NCC Group.

The information in this document is subject to change without notice. NCC Group shall not be liable for any damages resulting from technical errors or omissions which may be present in this document, or from use of this document.

This document is an unpublished work protected by the United Kingdom copyright laws and is proprietary to NCC Group. Disclosure, copying, reproduction, merger, translation, modification, enhancement, or use of this document by anyone other than authorised employees, authorised users, or licensees of NCC Group without the prior written consent of NCC Group is prohibited.

CONTROL INFORMATION

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Threat Intelligence Alert: Russia/Ukraine Conflict</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Publication Date</td>
<td>24/02/2022</td>
</tr>
<tr>
<td>Classification</td>
<td>TLP: WHITE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>24/02/2022</td>
<td>Strategic Threat Intelligence Practice</td>
<td>Report Created</td>
</tr>
<tr>
<td>1.1</td>
<td>25/02/2022</td>
<td>Strategic Threat Intelligence Practice</td>
<td>TTPs Updated</td>
</tr>
<tr>
<td>1.2</td>
<td>28/02/2022</td>
<td>Strategic Threat Intelligence Practice</td>
<td>Context Updated</td>
</tr>
</tbody>
</table>
# Table of Contents

COPYRIGHT AND CONFIDENTIALITY STATEMENTS .................................................................................................................................................. 2
CONTROL INFORMATION .......................................................................................................................................................................................... 2

Context: Russia/Ukraine Conflict ................................................................................................................................................................................ 5
  Russia Recognises Donetsk and Luhansk: 21/02/2022 ........................................................................................................................................ 5
  US and UK Intelligence Agencies Disclose New Russian Malware: 23/02/2022 .................................................................................. 5
  Cyber-attacks impact Ukrainian Organisations: 23/02/2022 ......................................................................................................................... 5
  Russian Forces Enter Ukraine: 24/02/2022 ................................................................................................................................................. 6
  Further Sanctions Imposed: 26/02/2022 ......................................................................................................................................................... 6

So what? .............................................................................................................................................................................................................. 7

Now what? ....................................................................................................................................................................................................... 8

Technical Details .................................................................................................................................................................................................. 9
  Tools ........................................................................................................................................................................................................... 9
  Vulnerabilities .................................................................................................................................................................................................. 10
  MITRE ATT&CK Mapping ........................................................................................................................................................................... 12
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.

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”.

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, 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. The destructive malware is understood to delete or corrupt data, damage the master boot record and allow for the control of the internal network.

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. 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.

---

1. https://www.ft.com/content/21b8f98e-b2a5-11e4-b234-00144feab7de
2. https://www.ft.com/content/21b8f98e-b2a5-11e4-b234-00144feab7de
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. 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.  

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

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.

---

8 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%. When Iran was removed from SWIFT due to their nuclear program it resulted in it losing approximately 30% of its foreign trade\(^9\).

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.

\(^9\) [https://www.bbc.co.uk/news/business-60521822](https://www.bbc.co.uk/news/business-60521822)

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


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


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

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](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.
  

- **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.
  

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

- **CVE-2019-7609 Kibana**
  Kibana contain an arbitrary code execution flaw in the Timelion visualizer.
  

- **CVE-2019-9670 Zimbra software**
  "Improper Restriction of XML External Entity Reference vulnerability affecting Synacor Zimbra Collaboration Suite."
  

- **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.
  
• **CVE-2019-11510 Pulse Secure**

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


• **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.


• **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**


https://nvd.nist.gov/vuln/detail/CVE-2021-26857
<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance</td>
<td>Active Scanning: Vulnerability Scanning [T1595.002]</td>
<td>Russian state-sponsored APT actors have performed large-scale scans in an attempt to find vulnerable servers.</td>
</tr>
<tr>
<td></td>
<td>Phishing for Information [T1598]</td>
<td>Russian state-sponsored APT actors have conducted spearphishing campaigns to gain credentials of target networks.</td>
</tr>
<tr>
<td>Resource</td>
<td>Develop Capabilities: Malware [T1587.001]</td>
<td>Russian state-sponsored APT actors have developed and deployed malware, including ICS-focused destructive malware.</td>
</tr>
<tr>
<td>Development</td>
<td>Exploit Public Facing Applications [T1190]</td>
<td>Russian state-sponsored APT actors use publicly known vulnerabilities, as well as zero-days, in internet-facing systems to gain access to networks.</td>
</tr>
<tr>
<td>Initial Access</td>
<td>Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]</td>
<td>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.</td>
</tr>
<tr>
<td>Execution</td>
<td>Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]</td>
<td>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.</td>
</tr>
<tr>
<td>Persistence</td>
<td>Valid Accounts [T1078]</td>
<td>Russian state-sponsored APT actors have used credentials of existing accounts to maintain persistent, long-term access to compromised networks.</td>
</tr>
<tr>
<td></td>
<td>Boot or Logon Initialization Scripts: RC Scripts [T1037.004]</td>
<td>Russian state-sponsored APT actors have executed on device startup, using a modified SS1armled RC script.</td>
</tr>
<tr>
<td>Tactic</td>
<td>Technique</td>
<td>Procedure</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Credential Access</strong></td>
<td>Pre-OS Boot: System Firmware [T1542.001]</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Brute Force: Password Guessing [T1110.001]</td>
<td>Russian state-sponsored APT actors have conducted brute-force password guessing and password spraying campaigns.</td>
</tr>
<tr>
<td></td>
<td>and Password Spraying [T1110.003]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OS Credential Dumping: NTDS [T1003.003]</td>
<td>Russian state-sponsored APT actors have exfiltrated credentials and exported copies of the Active Directory database ntds.dit.</td>
</tr>
<tr>
<td></td>
<td>Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]</td>
<td>Russian state-sponsored APT actors have performed &quot;Kerberoasting,&quot; whereby they obtained the Ticket Granting Service (TGS) Tickets for Active Directory Service Principal Names (SPN) for offline cracking.</td>
</tr>
<tr>
<td></td>
<td>Credentials from Password Stores [T1555]</td>
<td>Russian state-sponsored APT actors have used previously compromised account credentials to attempt to access Group Managed Service Account (gMSA) passwords.</td>
</tr>
<tr>
<td></td>
<td>Exploitation for Credential Access [T1212]</td>
<td>Russian state-sponsored APT actors have exploited Windows Netlogon vulnerability CVE-2020-1472 to obtain access to Windows Active Directory servers.</td>
</tr>
<tr>
<td></td>
<td>Unsecured Credentials: Private Keys [T1552.004]</td>
<td>Russian state-sponsored APT actors have obtained private encryption keys from the Active Directory Federation Services (ADFS) container to decrypt corresponding SAML signing certificates.</td>
</tr>
<tr>
<td></td>
<td>Proxy: Multi-hop Proxy [T1090.003]</td>
<td>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.</td>
</tr>
<tr>
<td>Tactic</td>
<td>Technique</td>
<td>Procedure</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Command and Control</td>
<td>Data Encoding: Non-standard Encoding [T1132.002]</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Fallback Channels [T1008 ]</td>
<td>Russian state-sponsored APT actors randomly select a C2 server from contained lists of IPv4 addresses and port numbers.</td>
</tr>
<tr>
<td></td>
<td>Application Layer Protocol: Web Protocols [T1071.001]</td>
<td>Russian state-sponsored APT actors can download files via HTTP or HTTPS.</td>
</tr>
<tr>
<td></td>
<td>Encrypted Channel: Asymmetric Cryptography [T1573.002]</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Non-Standard Port [T1571 - ]</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Ingress Tool Transfer [T1105]</td>
<td>Russian state-sponsored APT actor adversaries transfer tools or other files from an external system into a compromised environment.</td>
</tr>
<tr>
<td>Defence Evasion</td>
<td>Impair Defenses: Disable or Modify System Firewall [T1562.004]</td>
<td>Russian state-sponsored APT actors have modified the Linux iptables firewall to enable C2 communication via a stored list of port numbers.</td>
</tr>
<tr>
<td></td>
<td>Masquerading: Match Legitimate Name or Location [T1036.005]</td>
<td>Russian state-sponsored APT actors have renamed its running process to masquerade as a Linux kernel thread.</td>
</tr>
<tr>
<td></td>
<td>Modify Registry [T1112]</td>
<td>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.</td>
</tr>
<tr>
<td>Tactic</td>
<td>Technique</td>
<td>Procedure</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>Tactic</td>
<td>Disable or Modify Tools [T1562.001]</td>
<td>Russian state-sponsored APT actors have modified and/or disabled security tools to avoid possible detection of their malware/tools and activities.</td>
</tr>
<tr>
<td>Discovery</td>
<td>System Information Discovery [T1082]</td>
<td>Russian state-sponsored APT actors regularly query device information.</td>
</tr>
<tr>
<td>Exfiltration</td>
<td>Exfiltration Over C2 Channel [T1041 -]</td>
<td>Russian state-sponsored APT actors are capable of uploading files to a C2 server.</td>
</tr>
<tr>
<td>Impact</td>
<td>Disk Structure Wipe [T1561.002]</td>
<td>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.</td>
</tr>
<tr>
<td>Impact</td>
<td>System Shutdown/ Reboot [T1529]</td>
<td>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.</td>
</tr>
</tbody>
</table>
Additional resources can be found here:

- 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](https://media.defense.gov/2021/jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF)
- APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations [https://www.cisa.gov/uscert/ncas/alerts/aa20-283a](https://www.cisa.gov/uscert/ncas/alerts/aa20-283a)