Overview of Russian GRU and SVR Cyberespionage Campaigns 1H 2022

blog.bushidotoken.net/2022/06/overview-of-russian-gru-and-svr.html

BushidoToken

(Image credit: DALL·E 2)

Background

In 2015 and 2016, the Democratic National Committee (DNC) was hacked by not one, but two Russian intelligence services, the Russian Main Intelligence Directorate (GRU) and the Russian Foreign Intelligence Service (SVR). The two advanced persistent threat (APT) groups attributed to these organizations coexisted inside the DNC's networks for months and provided valuable political intelligence to the Russian government, in the form of stolen files and emails, during the run-up to US presidential election. This audacious act of cyber-espionage brought these two APT groups, also known as FancyBear and CozyBear (coined by CrowdStrike), into the spotlight and under the microscope ever since.

On 24 February 2022, Russia invaded Ukraine and these two well-known APT groups (among many others) have been busy launching widespread intelligence gathering intrusion campaigns to support the Russian government and Russian military. This blog aims to leverage open source intelligence (OSINT) reports to highlight the recent publicly-known tactics, techniques, and procedures (TTPs) leveraged by these cyber adversaries in 1H 2022 and the significance of them. For many top enterprises, government organizations, and political entities, these hacking groups operating on behalf of the Russian GRU and SVR are priority threats whose capabilities is of the utmost concern.

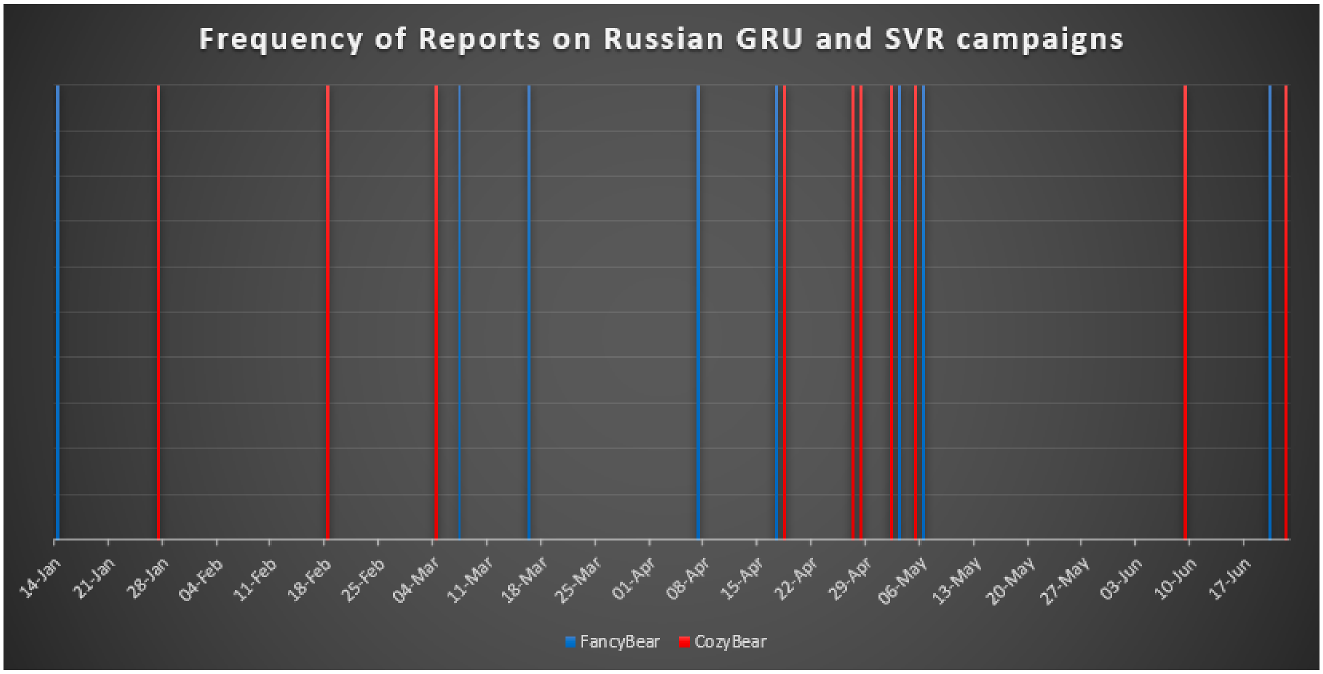

Figure 1. Timeline of reports on FancyBear and CozyBear activities

Russian GRU Unit 26165 (aka APT28, FancyBear, Strontium, Sofacy) activities in 1H 2022

- On 14 January, @billyleonard from the Google Threat Analysis Group (TAG) reported that FancyBear was behind an ongoing credential phishing campaign focused on Ukraine. The group leveraged ***.eu3[.]biz**, ***.eu3[.]org**, and **blogspot[.]com** hostnames as part of its phishing infrastructure.
- On 7 March, Google TAG disclosed that FancyBear conducted several large credential phishing campaigns targeting ukr[.]net users (UkrNet is a Ukrainian media company). This campaign included malicious links to **blogspot[.]com** sites that redirected to credential harvesting pages hosted on ***.frge[.]io**. These phishing links were also sent from email accounts that had been compromised prior by the APT group.
- On 16 March, the Computer Emergency Response Team of Ukraine (CERT-UA) issued an alert that further highlighted how UAC-0028 (CERT-UA's name for FancyBear) was phishing UkrNet accounts, but this time the APT group used the **tinyurl[.]com** URL-shortening service embedded inside a QR code the would lead to UkrNet credential havresting sites with ***.frge[.]io** and ***.m.pipedream[.]net** hostnames.
- On 7 April, the Microsoft Threat Intelligence Center (MSTIC) and the Microsoft Digital Crimes Unit obtained a court order authorizing it to take control of seven internet domains Strontium (Microsoft's name for FancyBear) used to conduct phishing attacks against Ukrainian media organizations, as well as government institutions and think tanks in the US and the EU involved in foreign policy.
- On 27 April, Microsoft's Special Report on Ukraine revealed additional details on Strontium's campaigns:

    - In August 2021, Microsoft recorded Strontium targeting defense-related organizations in Ukraine.
    - On 4 March, Microsoft specifically noted that the network of the government of Vinnytsia (a city in west-central Ukraine) was also compromised by Strontium and that sought access via phishing to other Ukrainian military personnel and regional Ukrainian government employee accounts.
    - In April, Microsoft observed Strontium and other suspected Russian nation state threat actors launch campaigns against or expand on existing access in the communications sector, targeting the IT infrastructure that supports the sector, and a major internet service provider (ISP).
- On 3 May, Google TAG provided an update on cyber activity in Eastern Europe. FancyBear was observed targeting users in Ukraine with a new variant of infostealer malware distributed via email attachments. The new FancyBear malware is a .NET executable that when ran by the victim steals cookies and saved passwords from Chrome, Edge and Firefox browsers. The data is then exfiltrated via email to a compromised email account.
- On 6 May, CERT-UA issued an alert that UAC-0028 sent malicious emails posing as CERT-UA and contained an attachment in the form of a password-protected RAR archive "UkrScanner.rar". Inside the RAR file was a Self-Extracting Archive (SFX) of the same name, which, in turn, contains a malware dubbed CredoMap. Data collected by the malware was exfiltrated via HTTP POST requests to ***.m.pipedream[.]net** hostnames.
- On 20 June, CERT-UA warned of another UAC-0082 attack, this time pushing a malicious document called "Nuclear Terrorism A Very Real Threat.rtf" via email. If opened, the document will download an HTML file with embedded JavaScript code from a ***.frge[.]io** hostname that exploits CVE-2022-30190, a remote code execution (RCE) bug in the Microsoft Windows Support Diagnostic Tool (MSDT) (aka the "Follina" exploit). If executed successfully by the victim, the exploit chain downloads the CredoMap malware. The same incident was also analysed by Malwarebytes Threat Intel (see here) and Team Cymru (see here).

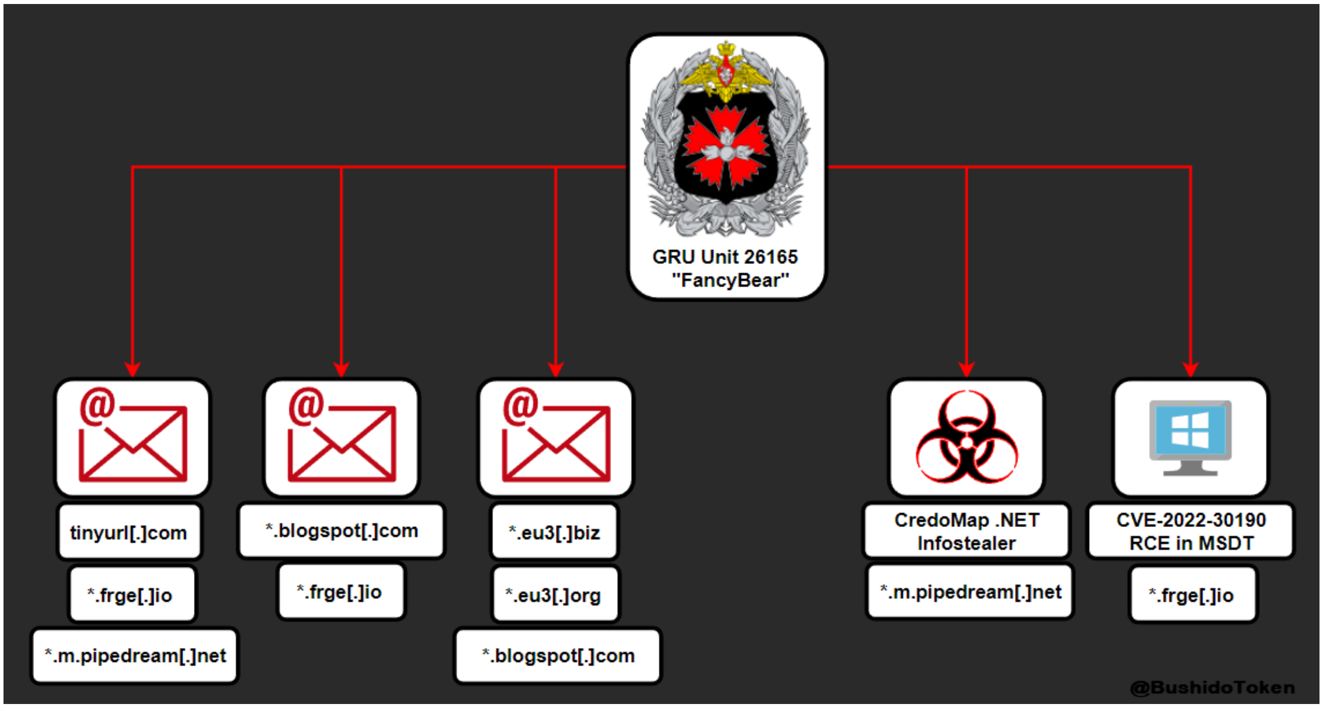

Figure 2. Summary of FancyBear campaign attributes in 1H 2022

Russian SVR (aka APT29, CozyBear, Nobelium, DarkHalo, TheDukes) activities in 1H 2022

- On 27 January, CrowdStrike published a comprehensive report on the 'StellarParticle Campaign' associated with CozyBear. The report highlighted the novel tactics and techniques leveraged by the Russian SVR hacking group throughout 2021. This included details from the SolarWinds supply chain attack, Browser cookie theft, and Microsoft Service Principal manipulation.
- On 18 February, the Shadow Chaser Group Tweeted a suspected sample of APT29 malware known as EnvyScout. The attackers leveraged the HTML smuggling technique to deliver an ISO file that, if executed, runs a DLL on the victim's device. This incident used a COVID-19 theme and reportedly was aimed at the Embassy of the Republic of Turkey.
- On 4 March, the Telsy Threat Intelligence team disclosed several suspected spear-phishing attempts against Indian government entities. The phishing attempts were tentatively attributed to Nobelium/APT29 due to the mutual use of a Cobalt Strike watermark ("1359593325") and an infection chain that matches reports by Microsoft and Volexity on Nobelium/APT29 campaigns.
- On 18 April, InQuest Labs discovered a malicious file belonging to Nobelium called "Ambassador_Absense.docx." posing as an official document from the Israeli Embassy in London. Opening the document downloads a HTML Application (.HTA) file with embedded JavaScript that decrypts and executes the payload. Once launched, the malicious payload collects data about the local system and exfiltrates it to a remote server using **api[.]trello[.]com**.

- On 27 April, Microsoft's Special Report on Ukraine revealed additional details on Nobelium's campaigns:
  - In early 2021, Microsoft observed Nobelium launching a large-scale phishing campaign against Ukrainian interests involved in rallying international support against Russian actions
  - By mid-2021, Nobelium attempted to access IT firms serving government customers in predominantly NATO member states, at times successfully compromising then leveraging privileged accounts to breach and steal data from Western foreign policy organizations.
  - As 2021 progressed, the Nobelium group, alongside several other suspected Russian nation state threat actors, sought persistent access to their particular interests among a total target pool that included Ukrainian defense, defense industrial base, foreign policy, national and local administration, law enforcement, and humanitarian organizations.
- Also on 27 April, Mandiant released a blog stating that it had gathered sufficient evidence to assess that the activity previously tracked as UNC2452, the threat group responsible for the SolarWinds compromise in December 2020, is attributable to APT29.
- On 28 April, Mandiant published a report on tracking APT29 phishing campaigns targeting diplomatic organizations in Europe, the Americas, and Asia. It included the disclosure of two new APT29 malware families uncovered in 2022, dubbed BEATDROP and BOOMMIC, and details about APT29’s efforts to evade detection through retooling and abuse of Atlassian's Trello API service: **api[.]trello[.]com**.
- On 2 May, Mandiant also disclosed a new campaign tracked as UNC3524 that has reportedly been active since December 2019. UNC3524 campaigns facilitate bulk email collection from victim environments, especially as it relates to their support of suspected espionage objectives. Notably, this threat actor leveraged a Dropbear-based backdoor, dubbed QUIETEXIT, on embedded network devices (such as VPN appliances) to access MS Office 365 or on-premises MS Exchange emails. Another interesting tactic is that UNC3524 usually accessed its victim's system from other compromised devices, usually outdated and unpatched LifeSize conference IoT cameras. Mandiant analysts tentatively attributed this campaign to APT29. However, the technical overlaps included TTPs that had already been made public and there were also some aspects aligned to APT28, which could suggest the two groups share some tooling.
- On 5 May, the Shadow Chaser Group Tweeted a suspected sample of APT29 malware that leveraged DLL side-loading as a method of executing their payload by invoking a legitimate Adobe application to execute their payload.

- On 13 May, Cluster25 published a report analyzing several CozyBear spear-phishing campaigns involving the above mentioned use of a side-loaded DLL through signed software (like Adobe suite) alongside the use of the legitimate Dropbox service **api[.]dropbox[.]com** as communication vector. The Cluster25 researchers also stated that this CozyBear campaign potentially impacted at least Greece, Italy, Turkey, and Portugal especially in the government and foreign affairs sectors.
- On 9 June, the Shadow Chaser Group Tweeted another suspect sample of APT29 malware that also leveraged DLL side-loading as a method of executing their payload by invoking a legitimate Hewlett Packard application to execute their payload.
- On 22 June, Microsoft released another report on 'Defending Ukraine: Early Lessons from the Cyber War' and included additional details about some of the SVR's campaigns. The Nobelium group has continued to target Ukrainian and NATO member states diplomatic entities with password spraying and spear-phishing attacks. Microsoft also reported that the SVR's influence operations include historical revisionism and the targeting of think tanks and academics.

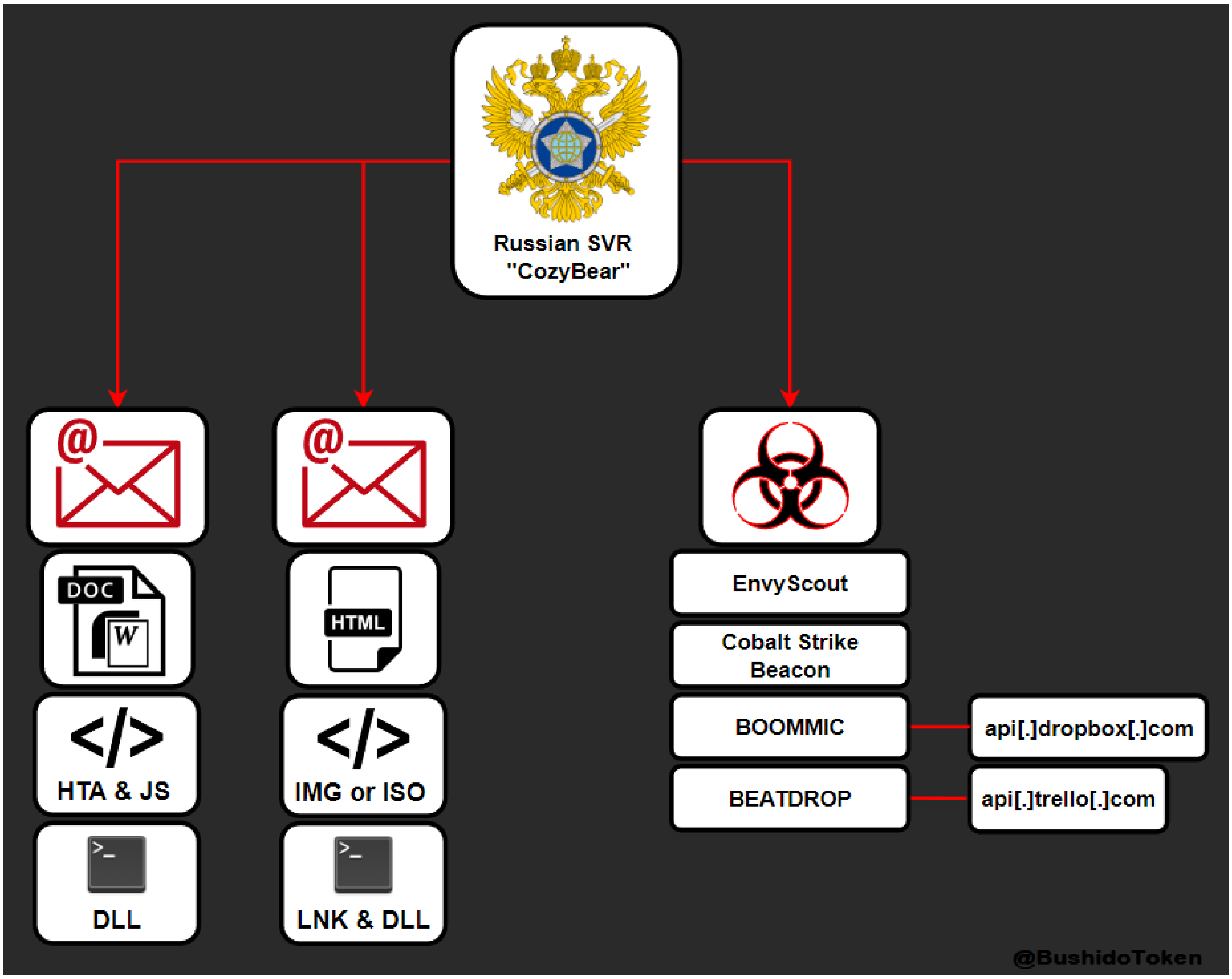

Figure 3. Summary of CozyBear campaign attributes in 1H 2022

Suggested Courses of Action

- Extract and ingest indicators of compromise (IOCs) from each the reports hyperlinked in the blog and investigate any hits
- Leverage detection rules for the APT group's malware from the reports hyperlinked in the blog to hunt through telemetry
- Extract the legitimate services used by the APT groups to support phishing and malware campaigns, hunt for them in your telemetry and investigate any hits
    - **FancyBear**: *.eu3[.]biz, *.eu3[.]org, *.blogspot[.]com, tinyurl[.]com, *.frge[.]io, and *.m.pipedream[.]net
    - **CozyBear**: api[.]trello[.]com and api[.]dropbox[.]com
- Continue to track the campaigns of FancyBear and CozyBear and mitigate appropriately
- Investigate the exposure of and expedite patching of CVE-2022-30190, a critical RCE in MSDT leveraged in the wild by multiple threat actors
- Leverage the Curated Intel GitHub repository on Ukraine Cyber Operations to track the evolving threat landscape surrounding the war

Lessons from the Conti Leaks

How Do You Run A Cybercrime Gang?