# APT29: Cozy Bear

M. Kutyła, December 2024

# Agenda

- Who is APT29?
- How does APT29 operate?
- What are their goals?
- Overview of exemplary campaigns
- How can we protect ourselves against their campaigns?

# APT characteristics

## Standard offensive operations

- **Campaign duration**: Short
- **Objectives**: Achieve simple, rapid success. Focus is on immediate gain rather than long-term strategy.
- **Resources**: Minimal human, technical, skill, time, and financial resources are required.
- **Scenario**: Low input, high profit
- **Who**: script kiddies, low-skilled hackers, hacktivists, focused on achieving simple success.
- **Visibility**: Concealment is not a priority; success may even be bragged about. More advanced groups may still avoid detection.

## Advanced Persistent Threats

- **Campaign duration**: Medium to Long (even years)
- **Objectives**: Long-term, complex, often expanding in scope as the operation progresses. Objectives can shift as new intelligence or opportunities arise.
- **Resources**: Specialized, large technical resources, high level of expertise. Usually well-founded, planned.
- **Optimal Scenario**: Objectives not only financially driven, but also strategic (cyber warfare). Multi-factor and multi-objective optimization.
- **Who**: Specialists on demand (mercenaries), professional cybercriminals, state-run cells
- **Visibility**: Concealment is critical to ensure long-term success.

# Who is APT29?

- Threat group attributed to Russia’s Foreign Intelligence Service (SVR)
- Also referred to as: Cozy Bear, The Dukes, Dark Halo, SolarStorm, StellarParticle, and others (derived from SVR’s campaigns).
- Operating since at least 2008
- Targets:
  - Government network in Europe and NATO members countries,
  - Research institutes,
  - Think tanks,
  - Technology companies.
- Aim: to collect confidential information, political intelligence.

# How does APT29 operate?

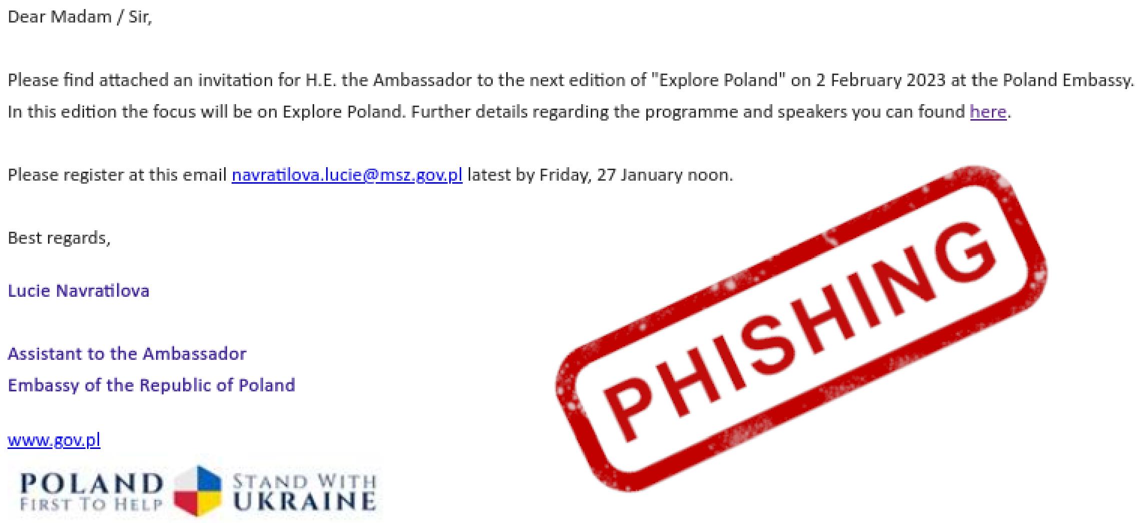
- Spear-phishing (targeted phishing)
  - Phishing is a form of social engineering and a scam where attackers deceive people into performing certain actions: revealing sensitive information or installing malware.

Example: “GRIZZLY STEPPE – Russian Malicious Cyber Activity” (2016) describing SVR compromising U.S. political party ahead of a presidential election.

- Recently: *Diplomatic Orbiter* campaign targeting diplomatic agencies worldwide

“Espionage campaign linked to Russian intelligence services” (2023) describing techniques used against embassies in numerous countries (SKW and CERT.PL)

# Example: Diplomatic Orbiter



Dear Madam / Sir,

Please find attached an invitation for H.E. the Ambassador to the next edition of "Explore Poland" on 2 February 2023 at the Poland Embassy. In this edition the focus will be on Explore Poland. Further details regarding the programme and speakers you can found here.

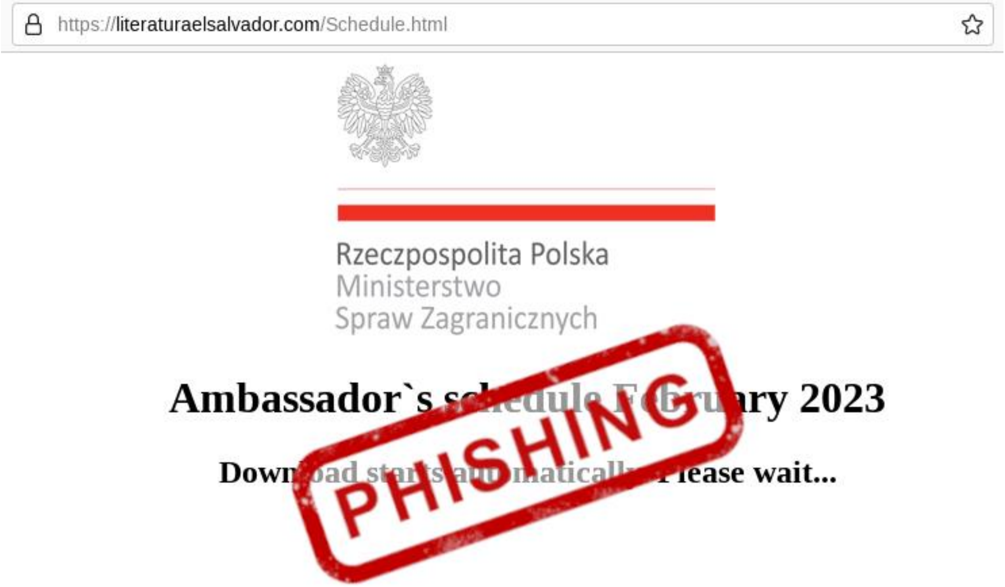
Please register at this email navratilova.lucie@msz.gov.pl latest by Friday, 27 January noon.

Best regards,

Lucie Navratilova

Assistant to the Ambassador
Embassy of the Republic of Poland

www.gov.pl

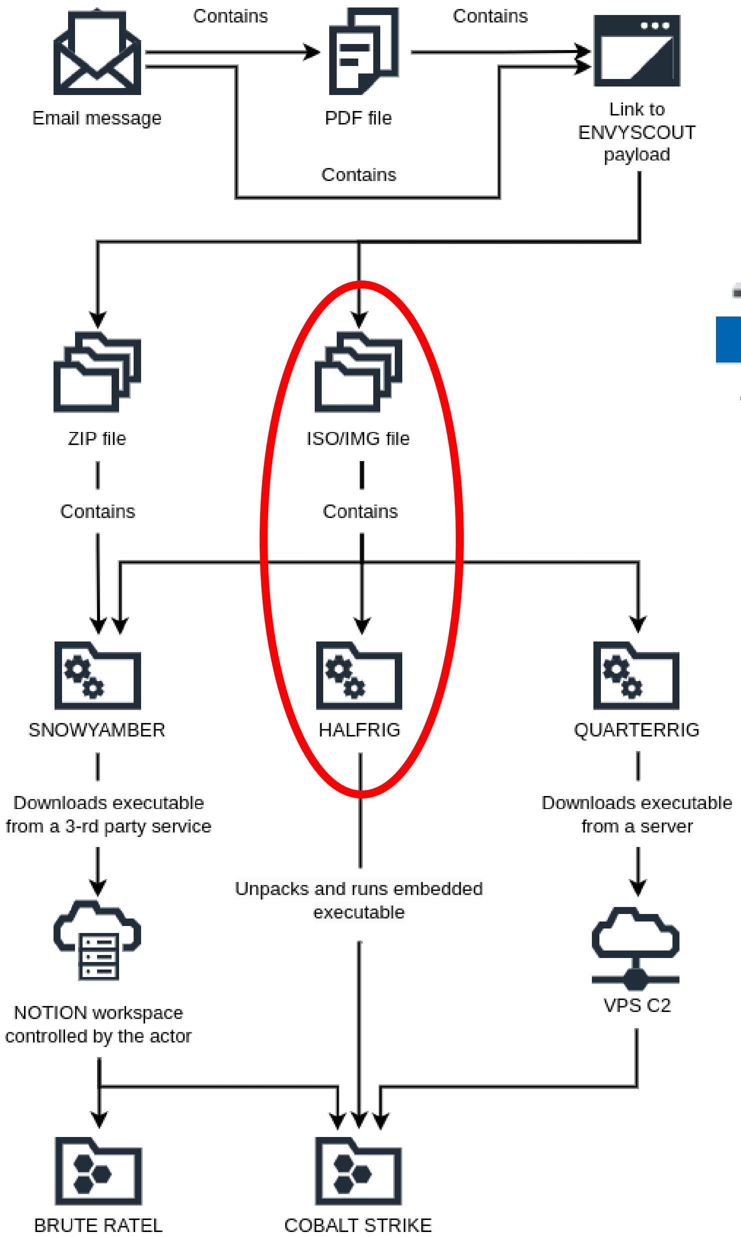


https://literaturaelsalvador.com/Schedule.html

Rzeczpospolita Polska
Ministerstwo
Spraw Zagranicznych

Ambassador`s schedule February 2023

Download starts automatically. Please wait...



Email message

Contains

PDF file

Contains

Link to ENVYSCOUT payload

Contains

ZIP file

Contains

ISO/IMG file

Contains

SNOWYAMBER

HALFRIG

QUARTERRIG

Downloads executable from a 3-rd party service

Unpacks and runs embedded executable

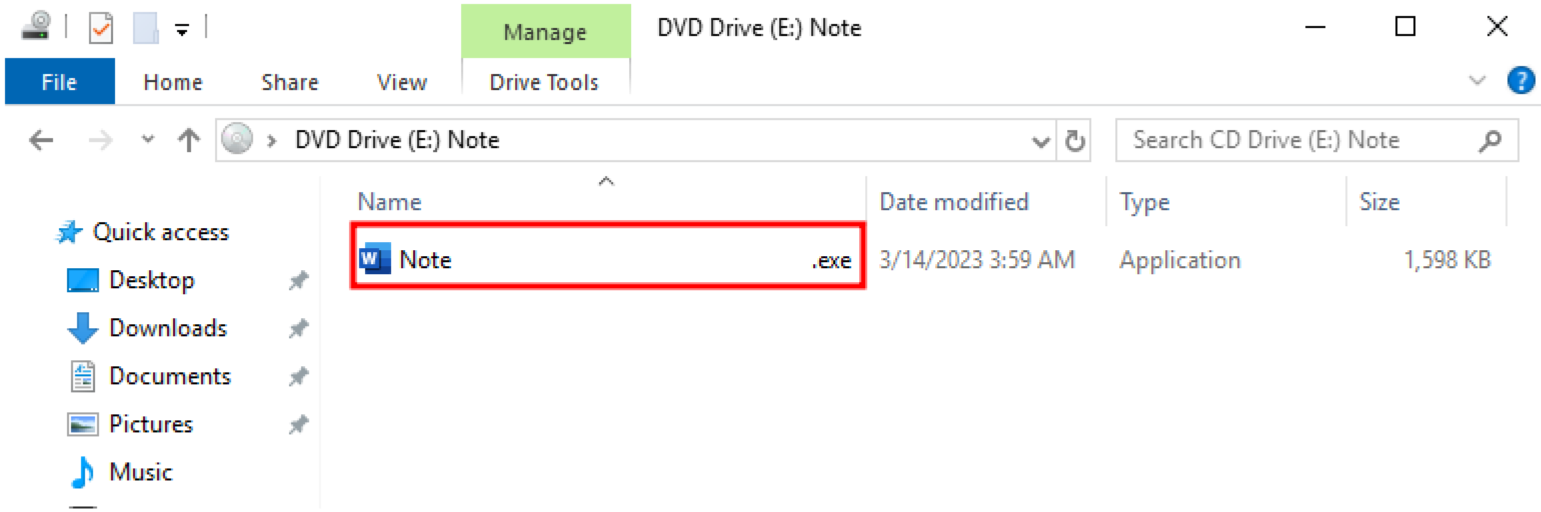
Downloads executable from a server

NOTION workspace controlled by the actor

VPS C2

BRUTE RATEL

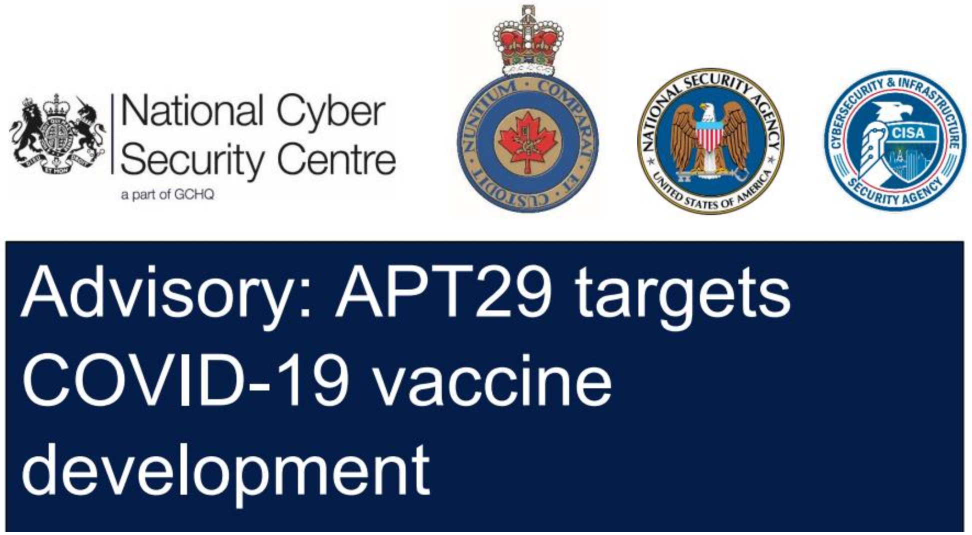
COBALT STRIKE



| Name | Date modified | Type | Size |
|---|---|---|---|
| Note .exe | 3/14/2023 3:59 AM | Application | 1,598 KB |

# Further goals & techniques

- Goals reach beyond political intelligence
- Targeting organization involved in COVID-19 vaccine development & energy companies with alignment of SVR’s responsibilities to support Russian economy



National Cyber Security Centre
a part of GCHQ

Advisory: APT29 targets COVID-19 vaccine development

How?

- Exploiting CVE in order to gain initial access
- Deploying custom malware: WellMess, WellMail, Sorefang

# Exemplary campaign: SolarWinds

- SolarWinds: software company providing system management tools for monitoring
- Orion: IT performance monitoring system, running with privileged access.
- Supply chain attack: APT29 inserted malicious code into the Orion system
- Impacted >18k customers including: US government departments (e.g., Homeland Security) and private companies (FireEye, Intel, Microsoft, Cisco…)
- Detected by FireEye

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
IT Security
Supply Chain
OT Security
Insider Threat
Physical Security
Interoperable Communications

Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise

# Exemplary campaign: TeamCity

- Targeted exploitation of a specific vulnerability (CVE-2024-42793).
- Targeting JetBrains TeamCity software since September 2023.
- TeamCity: managing and automating software compilation, building, testing, and releasing.
- Goal: to access source code, signing certificates; impact corresponding processes.

Co-Authored by:

**Russian Foreign Intelligence Service (SVR) Cyber Actors Use JetBrains TeamCity CVE in Global Targeting**

13 December 2023

v1.0

# Techniques leveraged by APT29

- Phishing,
- Malware,
- Exploiting public-facing applications,
- Leveraging external remote services,
- Compromising supply chains,
- Using valid accounts,
- Exploiting software for credential access,
- Forging web credentials: SAML tokens,
- And others – enumerated by MITRE: https://attack.mitre.org/groups/G0016/

# Prevention techniques (1/2)

- **Education and Awareness**: As people are usually the weakest link and are the first line of defense.
- **Patching and Updates**: To limit the number of attack vectors.
- **Multi-layered Security:** Isolate Internet-facing services in a DMZ.
- **Access Management**: Principle of Least Privileges.
- **Limit the attack surface**: Block obsolete or unused protocols.
- **Monitoring and Analysis**: Robust logging of Internet-facing services and authentication functions.

# Prevention techniques (2/2)

- **Enforcing strong password policies**
- **Supplier and Vendor audits**: Ensure all suppliers and vendors meet strict cybersecurity standards
- **Assume that a breach will happen:** Prepare for incident response activities, only communicate about breaches on out-of-band channels, and take care to uncover a breach’s full scope before remediating.
- **Threat Intelligence**: analyzing APT29’s tactics, techniques, and procedures; regularly updating systems with indicators of compromise; predicting potential targets…

# APT29: Cozy Bear

M. Kutyła, December 2024