Unmasking APT29: The Sophisticated Phishing Campaign Targeting European Diplomacy

By rohann@checkpoint.com

Published: 2025-04-15 · Archived: 2026-04-13 02:16:21 UTC

Executive Summary

- Check Point Research has been observing a sophisticated phishing campaign conducted by Advanced Persistent Threat (APT) 29, a Russian-linked threat group. The operation targeted diplomatic organizations throughout Europe.
- The campaign appears to continue a previous operation called Wineloader, which impersonates a major European foreign affairs ministry to distribute fake invitations to diplomatic events, most commonly wine-tasting events.
- The campaign, which was spread via phishing emails, used a new malware dubbed Grapeloader. A new variant of Wineloader was also discovered, likely used in a later stage of the campaign.

Introduction

Check Point Research (CPR) identified a significant wave of targeted phishing attacks beginning in January 2025. These attacks specifically target government officials and diplomats across Europe, employing sophisticated techniques, tactics, and procedures (TTPs) that closely resemble those associated with a previous phishing campaign called Wineloader, which was previously connected to APT29, a Russia-linked threat actor.

To understand APT29's latest campaign in-depth, read Check Point Research's comprehensive report here.

APT29, AKA Midnight Blizzard or Cozy Bear

APT29, known as Midnight Blizzard or Cozy Bear, is recognized for targeting high-profile organizations, including government agencies and think tanks. This group is also linked to the SolarWinds supply chain attack. Its operations range from targeted phishing campaigns to significant supply chain attacks, mostly employing various custom malware.

APT29 Targets European Ministries

In a recent wave of cyber attacks attributed to APT29, threat actors notably impersonated a major European foreign affairs ministry to send misleading emails inviting targets to wine-tasting events. This new phishing campaign, which emerged approximately a year after the last Wineloader campaign, primarily targeted European diplomatic entities, including embassies of non-European countries. When clicked, the emails contained malicious links that either initiated the download of a backdoor known as Grapeloader or redirected victims to the legitimate website of the impersonated European foreign affairs ministry, creating a facade of legitimacy.

Investigators uncovered the Grapeloader variants sent to specific targets and a new variant of Wineloader. The compilation timestamp of this Wineloader variant and its resemblance to the newly identified Grapeloader suggest that it was likely implemented in a later phase of the attack. This progression illustrates the evolving tactics the attackers employ, showcasing their adaptability in exploiting trusted entities to deploy sophisticated malware against unsuspecting victims.

Figure 1 – Campaign Overview

Phishing Emails

Several emails were sent from two domains, pretending to be from someone in the Ministry of Foreign Affairs. Each email had a malicious link that, when clicked, downloaded a file called wine.zip, which was the next step in the attack. The link's domain matched the sender's domain. Most of these emails were themed around wine tasting events.

Check Point Research identified several emails sent out as part of the campaign, almost all of them with the theme of a wine tasting event:

Email subjects
Wine Event
Wine Testing Event
Wine tasting event (update date)
For Ambassador's Calendar
Diplomatic dinner

The server hosting the link is thought to be well-protected against scanning and automated analysis tools. The malicious download is activated only under specific conditions, such as certain times or geographic locations.

Conclusion

In conclusion, the recent targeted phishing attacks associated with APT29, also known as Midnight Blizzard or Cozy Bear, highlight the increasing sophistication and adaptability of cyber threats facing governmental and diplomatic entities. The emergence of Grapeloader, alongside a new variant of Wineloader, underscores the evolving nature of malware, revealing more advanced stealth and evasion capabilities that pose significant challenges for detection and prevention.

Check Point Threat Emulation and Harmony Endpoint protect organizations from threats, such as those mentioned in this blog, by identifying malicious behavior before it can impact networks. They detect unknown threats and zero-day vulnerabilities, allowing users to quickly access a secure version of files while the original files are thoroughly examined. This proactive approach enhances security by ensuring quick access to safe content and effectively identifying and managing potential threats, thereby preserving network integrity.

To understand APT29's latest campaign in-depth, read Check Point Research's comprehensive report here.
