# SOLARDEFLECTION C2 Infrastructure Used by NOBELIUM in Company Brand Misuse

May 3, 2022 • Insikt Group

Insikt Group

Editor's Note: The following post is an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.

This report profiles the unique infrastructure used by Russian state-sponsored threat activity group NOBELIUM. The activity was identified through a combination of large-scale automated network traffic analytics and analysis derived from open source reporting. Data sources include the Recorded Future Platform, SecurityTrails, DomainTools, PolySwarm, Farsight, Shodan, Censys, Team Cymru's Pure Signal™ and other common open-source tools and techniques. The report will be of most interest to individuals engaged in strategic and operational intelligence relating to the activities of the Russian government in cyberspace and network defenders. Some technical details from our original research have not been included in this report version in order to protect tracking techniques and ongoing research into NOBELIUM activity.

## Executive Summary

Recorded Future's Insikt Group continues to monitor Russian state-sponsored cyber espionage operations targeting government and private sector organizations across multiple geographic regions. From mid-2021 onwards, Recorded Future's midpoint collection revealed a steady rise in the use of NOBELIUM infrastructure tracked by Insikt Group as SOLARDEFLECTION, which encompasses command and control (C2) infrastructure. In this report, we highlight trends observed by Insikt Group while monitoring SOLARDEFLECTION infrastructure and the recurring use of typosquat domains by its operators.

A key factor we have observed from NOBELIUM operators involved in threat activity is a reliance on domains that emulate other brands (some legitimate and some that are likely fictitious businesses). Domain registrations and typosquats can enable spearphishing campaigns or redirects that pose a threat to victim networks and brands.

Using a combination of proactive adversary infrastructure detections, domain analysis techniques, and Recorded Future Network Traffic Analysis, we have determined that NOBELIUM's use of SOLARDEFLECTION infrastructure overlaps with other common infrastructure tactics, techniques, and procedures (TTPs) previously attributed to the group by multiple organizations including Microsoft, Fortinet, Sekoia, and Volexity. Previous open source reporting also highlighted NOBELIUM's use of cracked versions of the Cobalt Strike penetration testing tool.

## Key Judgments

- Insikt Group is confident that the identified SOLARDEFLECTION infrastructure can be attributed to the threat activity group publicly reported as NOBELIUM; this confidence is based on the use of overlapping network infrastructure previously attributed to NOBELIUM in public reporting, as well as unique variations of Cobalt Strike traditionally used by the group.
- Broader themes in SOLARDEFLECTION C2 typosquats have included the misuse of brands across multiple industry verticals, particularly in the news and media industries.
- Cobalt Strike servers related to SOLARDEFLECTION monitoring that were also previously linked to NOBELIUM activity used modified server configurations, likely in an attempt to remain undetected from researchers actively scanning for standard Cobalt Strike server features.
- NOBELIUM has made extensive use of typosquat domains in SSL certificates and will likely continue to use deceptive techniques, including typosquat redirection, when using Cobalt Strike tooling.

## Background

Analysis of recent and historical domains attributed to NOBELIUM broadly demonstrates the group's familiarity with, and tendency to emulate, a variety of media, news and technology providers. The group has abused dynamic DNS resolution to construct and resolve to randomly generated subdomains for its C2s or root domains to mislead victims. The key aspect to these attacks is the use of either email addresses or URLs that look similar to the domain of a legitimate organization. Potentially harmful domain registrations and typosquats can enable spearphishing campaigns or redirects that pose an elevated risk to a company's brand or employees. A successful spearphish is dependent on factors such as the quality of the message, the credibility of the sender address, and, in the case of a redirecting URL, the credibility of the domain name. Insikt Group has previously observed other Russian nexus groups using typosquatting in support of operations, such as those aimed at the 2020 presidential elections, to increase confidence in the validity of the

fraudulent login portal used to harvest victim credentials. This tactic has also been reported recently in open sources in connection with intrusions targeting entities in Ukraine, likely in support of Russia's invasion of the country.

Insikt Group assesses that NOBELIUM is a threat activity group operating in line with the objectives of Russia's Foreign Intelligence Service (SVR). The SVR is tasked with providing the president of the Russian Federation, the Federal Assembly, and the government with the intelligence they need to make decisions in the areas of politics, the economy, military strategy, scientific-technical strategy, and the environment. Russia's SVR defines itself as separate by allowing the Russian Main Intelligence Directorate (GRU) to focus on military intelligence operations, while the SVR focuses on political intelligence; this is, however, a very high-level view of these operations. The SVR conducts its affairs by collecting information via public and private means, with the intended goal of gathering strategic information from organizations and individuals who in turn influence strategic policy and decision-makers in targeted countries.

In 2021, Volexity published research outlining a suspected APT29 phishing operation that targeted non-governmental organizations (NGOs), research institutions, governments, and international bodies using election fraud-themed lures purporting to be sent from the United States Agency for International Development (USAID), a government agency. The same day, Microsoft also published research on wider TTPs used in the same campaign and attributed the activity to NOBELIUM, the group behind the SolarWinds intrusions. This campaign targeted sensitive diplomatic and government entities as early as February 2021. They believe the threat actor used this information to launch other highly targeted attacks as part of their broader campaign. Additional research confirmed that a cluster of infrastructure monitored by Insikt Group under the designation SOLARDEFLECTION since 2021 overlaps with this previous reporting. Ongoing detections within the Recorded Future Command and Control security feed assisted in confirming the registration of new typosquat domains tied to NOBELIUM operations. More notably, we have confirmed that several newly identified typosquats continue to adopt the naming conventions or themes that were originally flagged as likely being associated with NOBELIUM reporting as early as 2020.

Figure 1: SOLARDEFLECTION Domain Registration reference in the Recorded Future Platform (Source: Recorded Future)

The Recorded Future Platform automatically detects typosquatted domains; each newly created domain entity is evaluated for typosquatting-style similarity to other domains observed by Recorded Future. An example of this is the SOLARDEFLECTION typosquat displayed in Figure 1, which based on the domain's spelling was very likely an attempt by NOBELIUM operators to emulate the T-Mobile brand. A review of the frequency in which SOLARDEFLECTION domains were registered over the past two years confirmed NOBELIUM's tendency to register domains in cycles, occasionally taking short hiatuses which at times likely coincided with new open source reporting attributing several domains to NOBELIUM activity (as depicted within the Recorded Future timeline below).

Figure 2: SOLARDEFLECTION Typosquat Registration Timeline (Source: Recorded Future Data)

Insikt Group proactively detects SOLARDEFLECTION infrastructure through an in-depth understanding of the infrastructure TTPs that the group employs (detailed further below within the Infrastructure TTPs section). Additionally, the Command and Control data set enables us to enrich and identify any SOLARDEFLECTION IPs that we have categorized as "positive C2". We then analyze network communications to investigate how the C2 is interacting with infected machines or how it is being administered by the adversary. SOLARDEFLECTION C2s can be reviewed from within the Recorded Future Platform's Command and Control data set.

Editor's Note: The following post is an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.