Lumen Newsroom

New evidence from Lumen reveals Konni attack on Russia lasted three months

Persistent campaign began in October 2021; actor modified lures from Covid to New Year's messages

DENVER, Jan. 6, 2022 /**PRNewswire**/ -- Researchers at **Black Lotus Labs®**, the threat intelligence team at **Lumen Technologies**, discovered **new evidence** of a months-long campaign against the Russian Ministry of Foreign Affairs (MID). The highly targeted campaign included the deployment of the Konni RAT – a malicious Remote Access Trojan that researchers and governments believe is **a tool** used by the Democratic People's Republic of Korea (DPRK) since 2014.

Black Lotus Labs discovered new evidence of a months-long campaign against the Russian Ministry of Foreign Affairs.

"This activity cluster demonstrates the patient and persistent nature of advanced actors who wage multi-phased campaigns against perceived high-value networks," said Mark Dehus, director of threat intelligence at Black Lotus Labs. "If actors attempt to infiltrate the Russian Ministry of Foreign Affairs, what's to stop them from attempting to use these same tactics on other governments or high-profile businesses? For this reason, it is vital for defenders to understand advanced actors' evolving capabilities and tradecraft used to infect coveted targets."

Read the full blog **here**.

Timeline of Observed Events

The series of persistent actions against Russia's MID occurred from October to December 2021 as follows:

- In October, the actors set up spoofed hostnames to harvest credentials of an active MID account.
- In November, the attackers used social engineering to lure recipients into downloading malware disguised as software the Russian government uses to collect Covid vaccination

statuses.
- In December, the attackers used the previously acquired credentials to spear-phish high-value targets with a Happy New Year-themed message. If invoked, a loader nearly identical to the one observed in November would deploy a sophisticated infection chain resulting the Konni RAT, as previously **reported by Cluster25.**

Why This Attack is Significant

- One of the high-profile targets included Sergey Alexeyevich Ryabko, deputy foreign minister for the Russian Federation, among other Russian government officials.
- According to a cached version of the MID's website – which has since gone offline – Ryabko is responsible for bilateral relations with North and South America, non-proliferation and arms control, Iran's nuclear program and Russia's participation in the BRICS association.

Black Lotus Labs' Response

- Black Lotus Labs successfully blocked the threat actor's infrastructure across the Lumen global IP network to protect its customers and the broader internet from being targeted.
- The team continues to follow this activity to detect and disrupt similar campaigns, and it encourages other organizations to alert on these and similar indicators in their environments.

Additional Resources

- Read the **full Konni report** in Black Lotus Labs' latest blog.
- **No Longer Just Theory:** Black Lotus Labs Uncovers Linux Executables Deployed as Stealth Windows Loaders
- Suspected Pakistani Actor Compromises Indian Power Company with **New ReverseRat**
- **ReverseRat Reemerges** with A (Night)Fury New Campaign and New Developments, Same Familiar Side-Actor
- Newly Discovered **Watering Hole Attack** Targets Ukrainian, Canadian Organizations
- A Look Inside the **TrickBot** Botnet

About Lumen Technologies

Lumen is guided by our belief that humanity is at its best when technology advances the way we live and work. With approximately 450,000 route fiber miles and serving customers in more than 60 countries, we deliver the fastest, most secure platform for applications and data to help businesses, government and communities deliver amazing experiences. Learn more about the Lumen network, edge cloud, security, communication and collaboration solutions and our purpose to further human progress through technology at **news.lumen.com/home**, LinkedIn:

/lumentechnologies, Twitter: @lumentechco, Facebook: /lumentechnologies, Instagram: @lumentechnologies and YouTube: /lumentechnologies. Lumen and Lumen Technologies are registered trademarks.

SOURCE Lumen Black Lotus Labs

For further information: Media Contact: Suzanne K. Dawe, Lumen Public Relations, Connected Security | Black Lotus Labs, 720.217.5476, suzanne.dawe@lumen.com

---

Additional assets available online: **Photos (1**

https://news.lumen.com/2022-01-06-New-evidence-from-Lumen-reveals-Konni-attack-on-Russia-lasted-three-months