vinetur

SPIKEDWINE: The sophisticated scam targeting EU Diplomats with a taste for wine

How a fake wine tasting invitation compromised EU Diplomats

Monday, March 11, 2024



In a twist that sounds like it's straight out of a spy novel, EU diplomats were recently targeted in a sophisticated cyber-attack that cleverly leveraged their interest in wine. Dubbed "SPIKEDWINE," this email scam involved a phony invitation to a wine tasting event supposedly hosted by the Indian ambassador. This incident is a sobering reminder of how even the most benign of interests can be weaponized in the digital

age.

The scam unfolded in late January when diplomats across Brussels received an email invitation to a wine tasting at the Indian residence scheduled for February 2nd. The email, detailed and convincing, appeared to be from the Ambassador of India. It included a link to a PDF file, purportedly an invitation, which asked recipients to click on another link to fill out a pre-event questionnaire. However, this link was a trap, initiating the download of a malware known as WineLoader onto the unsuspecting diplomats' computers.

Cybersecurity firm Zscaler, which has been closely following this campaign, revealed the intricacies of the WineLoader malware. It's designed to evade detection by encrypting sensitive information in the computer's memory, thus slipping past security programs that scan for malicious activities. Once installed, it opens a backdoor into the victim's operating system, allowing hackers to access the compromised computer undetected.

The sophistication of the SPIKEDWINE scam is alarming. The attackers went to great lengths to remain under the radar, putting significant effort into crafting an invitation that looked legitimate and employing advanced techniques to avoid memory forensics and automated URL scanning solutions. This level of detail suggests that the attackers were not amateurs but highly skilled individuals or groups with a specific interest in accessing the confidential workings of EU diplomacy.

The origin of the SPIKEDWINE attack remains a mystery, though it's no secret that European diplomats are often the target of cyber-espionage attempts. Organizations and state actors alike aim to gain insights into the private exchanges and inner workings of EU diplomacy, and this latest attack is just one in a series of attempts to infiltrate these circles.

As the cyber threat landscape continues to evolve, incidents like SPIKEDWINE serve as a stark reminder of the need for vigilance in all forms of digital communication. Even something as innocuous as a wine tasting invitation can serve as a Trojan horse for sophisticated cyber-attacks. This incident underscores the importance of cybersecurity education and awareness, especially for individuals in sensitive positions, to prevent

such breaches and protect against the ever-present threat of digital espionage.