



Physical & Cyber Security Intelligence & Information Threat Report

Issue – November 7, 2022

I. Cyber

LinkedIn Phishing Spoof Bypasses Google Workspace Security¹

"A phishing email purportedly from LinkedIn with the subject line "We noticed some unusual activity" was discovered targeting users at a travel organization, in an attempt to pilfer their credentials on the social-media platform. The phishing campaign slipped past Google's email security controls after cheating email authentication checks via SFP and DMARC, according to Armorblox, whose email security system at the victim organization found and stopped the attack pointed at some 500 user inboxes. "The main call-to-action button (Secure my account) included within the email contains a bad URL and took victims to a fake landing page. This fake landing page ... mimicked a legitimate LinkedIn sign in page that included LinkedIn logos, language, and illustrations that mirrored true LinkedIn branding," Armorblox wrote in a post about the attack campaign."

Hackers selling access to 576 corporate networks for \$4 million²

A new report shows that hackers are selling access to 576 corporate networks worldwide for a total cumulative sales price of \$4,000,000, fueling attacks on the enterprise. The research comes from Israeli cyber-intelligence firm KELA which published its Q3 2022 ransomware report, reflecting stable activity in the sector of initial access sales but a steep rise in the value of the offerings. Although the number of sales for network access remained about the same as in the previous two quarters, the cumulative requested price has now reached \$4,000,000. For comparison, the total value of initial access listings in Q2 2022 was \$660,000, recording a drop in value that coincided with the summer ransomware hiatus that hurt demand. Initial access brokers (IABs) are hackers who sell access to corporate networks, usually achieved through credential theft, webshells, or exploiting vulnerabilities in publicly exposed hardware. After establishing a foothold on the network, the threat actors sell this corporate access to other hackers who use it to steal valuable data, deploy ransomware, or conduct other malicious activity.

II. Threat Reporting

Domestic Threat Reporting

¹ <https://www.darkreading.com/risk/linkedin-phishing-spoof-bypasses-google-workspace-security>

² <https://www.bleepingcomputer.com/news/security/hackers-selling-access-to-576-corporate-networks-for-4-million/>



Fuel Company Issues Diesel Shortage Warning, Says Conditions 'Rapidly Devolving'³

A major fuel supply and logistics company is raising a red flag on upcoming diesel fuel shortages. Mansfield Energy issued the alert on 28 October 2022, stating there was a developing diesel fuel shortage in the southeastern region of the United States. The company speculated that the shortage could be generated from "poor pipeline shipping economies" and a historically low supply of diesel reserves. "Poor pipeline shipping economics and historically low diesel inventories are combining to cause shortages in various markets throughout the Southeast," the company said. "These have been occurring sporadically, with areas like Tennessee seeing particularly acute challenges." States expected to experience serious affects of the shortage include Maryland, Virginia, Alabama, Georgia, Tennessee, North Carolina and South Carolina.

International Threat Reporting

Tower bombing caused power outage in northwest Mindanao, Philippines⁴

The National Grid Corporation of the Philippines (NGCP) on Tuesday said that areas of northwest Mindanao experienced power interruptions as a transmission line was downed following a bombing incident.

In a statement, the NGCP said its Baloi-Aurora 138 kilovolt (kV) transmission line tripped at 4:50 p.m. on October 24.

The tripping of the transmission line prompted the grid operator to implement manual load dropping (MLD) or rotational brownouts to prevent overloading of the remaining line.

U.S. Condemns 'War Crimes' After Russia Drone Attack Hits Kyiv Apartment Block⁵

The United States will hold Russia accountable for "war crimes", the White House said on Monday, hours after Russia attacked Ukrainian cities with drones during morning rush hour, killing at least four people in an apartment building in Kyiv.

Ukrainian President Volodymyr Zelenskiy, in his Monday evening video address, said there had been more attacks. "Right now, there is a new Russian drone attack. There are (drones) that have been shot down."

Internet disruptions observed as Russia targets critical infrastructure in Ukraine⁶

³ <https://www.foxbusiness.com/politics/fuel-company-issues-diesel-shortage-warning-says-conditions-rapidly-devolving>

⁴ <https://www.msn.com/en-ph/news/national/ngcp-tower-bombing-caused-power-outage-in-northwest-mindanao/ar-AA131351>

⁵ <https://www.reuters.com/world/europe/intense-fighting-flares-ukraines-donetsk-region-2022-10-17/>

⁶ <https://securityaffairs.co/wordpress/137390/cyber-warfare-2/internet-disruptions-russia-ukraine.html>



While the Russian army is conducting coordinated missile and drone strikes in Ukraine experts observed Internet disruptions in the country. Starting on the morning of Monday, October 10, the Russian army is targeting several cities in Ukraine with coordinated missile and drone strikes. The escalation is a retaliation for the bombing of a bridge connecting Crimea to Russia. The strategy adopted by Moscow consists of disrupting energy and telecoms infrastructure in multiple regions of the country. Global internet monitor NetBlocks reported widespread Internet disruptions in the country as a result of the attacks. "Network data show major sustained impacts to infrastructure across much of #Ukraine after a series of reprisal attacks by Russia; energy facilities have been targeted per President's office" reported the observatory. "Following rapid repair efforts, much of the lost connectivity was restored by Tuesday" Regions around cities (Kharkiv, Sumy, Lviv, zaporizhzhia) that were the targets of the attacks were heavily impacted. Network connectivity was observed to fall to 81% of ordinary levels in Kyiv City after the Russian attacks on infrastructure.