Physical & Cyber Security Intelligence & Information Threat Report

Issue – September 30, 2022

I. *Cyber*

Ukraine warned the international community that Russian state-sponsored threat actors are planning "massive cyberattacks" against critical infrastructure in Ukraine and its allies.[1]

The Russian government is planning “massive cyberattacks” against Ukrainian critical infrastructure facilities to “increase the effect of missile strikes on electrical supply facilities,” the Ukrainian government said Monday.

The Russians are also planning to “increase the intensity of the DDoS attacks on the critical infrastructure of Ukraine’s closest allies, primarily Poland and the Baltic state,” the country’s Defense Intelligence agency said in a statement posted to a Ukrainian government website.

The U.S. Department of Justice has charged Iranian nationals with a string of cyber attacks against critical infrastructure, including power companies and local governments.[2]

The Justice Department said Wednesday that three Iranian citizens have been charged in the United States with ransomware attacks that targeted power companies, local governments and small businesses and nonprofits, including a domestic violence shelter.

The charges accuse the hacking suspects of targeting hundreds of entities in the U.S. and around the world, encrypting and stealing data from victim networks, and threatening to release it publicly or leave it encrypted unless exorbitant ransom payments were made. In some cases, the victims made those payments, the department said.

Policymakers eye incentives to fund better OT cybersecurity[3]

After decades of being treated as an afterthought, cybersecurity in the operational technology realm is finally getting the attention it deserves in Washington.

---

[1] https://www.cyberscoop.com/ukrainians-warn-of-massive-cyberattacks/

[2] https://apnews.com/article/technology-iran-violence-new-jersey-united-states-76c970bd4f1cdac3dc6bffa7ce925961

[3] https://www.scmagazine.com/analysis/critical-infrastructure/policymakers-eye-incentives-to-fund-better-ot-cybersecurity

To fix the problem, federal agencies and policymakers are eyeing a mix of voluntary collaboration and financial incentives to prod critical infrastructure entities to slowly replace past technologies and processes that have traditionally prioritized availability and reliability over security.

II. *Threat Reporting*

Domestic Threat Reporting

Anonymous Image Board User Shares a Technique to Acquire and Modify "Latex Balloons" with "Mylar" Ribbons to "Strain the Grid" in California[4]

Anonymous image board user shared a technique to acquire and modify "latex balloons" with "mylar" ribbons. Source posted the reply in a thread encouraging viewers to do their "part" to strain the electrical grid in California. Source recommended releasing the modified balloons "individually or in bunches" and claimed if "enough of these get released" people "everywhere are [expletive]."

Source replied to an anonymous thread titled, "It's time we Strain the Grid" that discussed ways to increase individual energy consumption in California. The original post encouraged viewers to do their "part to [hashtag]StrainTheGrid" and shared an image of a California Governor's Office of Emergency Services "Emergency Alert" asking residents to conserve energy. The original thread received 333 replies and contained 77 images.

Source directed viewers to "Buy a couple of cans of party balloon helium" from the "party supplies section" of a "big box mart". Source stated, "Buy the larger but cheap latex balloons, prefer white and colorless" and avoid "dark colors" as "Dark latex balloons lose helium faster". Source then directed viewers to visit a "weed growing supply shop" to purchase "long rolls of mylar sheeting used to make spaces more reflective" and to "Cut mylar into long thin ribbons". Source instructed others to "Work out how much ribbon" the "balloons can carry but still lift at a reasonable rate". Source claimed that with the addition of the mylar ribbons, the balloons should rise at a "modest steady climb of around 1 to 3 yards a second" to be ideal. Source stated, "Release them individually or in bunches. Enough of these get released by enough people and dolphins everywhere are [expletive]"."

Scammers Targeting Customers of Energy Company, Demanding Virtual Currency Payments[5]

The FBI's Criminal Investigative Division and FBI Philadelphia, in coordination with the Office of Private Sector (OPS), prepared this LIR to alert the energy sector about tactics, techniques, and procedures (TTP) used to target and defraud customers of funds by telephonically requesting payment via cryptocurrency for account balances. It is likely the unidentified culprits will employ the same TTP under the pretext of other energy companies throughout the United States.

The FBI's Criminal Investigative Division and FBI Philadelphia, in coordination with the Office of Private Sector (OPS), prepared this LIR to alert the energy sector about tactics, techniques, and procedures (TTP)

[4] DHS Open Source Intelligence Report OSIR-04001-0610-22

[5] Office of Private Sector Liaison Information Report LIR 220822007

used to target and defraud customers of funds by telephonically requesting payment via cryptocurrency for account balances. It is likely the unidentified culprits will employ the same TTP under the pretext of other energy companies throughout the United States.
• In July 2022, an identified victim was contacted telephonically by an unknown person purporting to represent a Pennsylvania-based energy company. The unidentified perpetrator stated between the victim's personal and business accounts with the energy company that he owed $1,700. The perpetrator then texted the victim a QR code and instructed the victim to travel to a cryptocurrency kiosk outside Philadelphia, PA to pay the $1,700.

• A victim was telephonically contacted in July 2022 by an unknown person claiming to represent a Pennsylvania-based energy company, informing him that his electricity would be suspended if he did not pay his bill. The victim was directed to make payment using cryptocurrency and eventually made three equal payments of $3,450, totaling $10,350.

The FBI has identified several potential indicators that may assist customers in recognizing perpetrators attempting to defraud them under the guise of their respective energy companies (these indicators should be observed in context and not individually, as no one indicator is determinative of illicit activity):

• Calls from energy companies instructing customers to pay via cryptocurrency,

• Calls from energy companies instructing customers to travel to specific locations to pay a bill,

• Energy companies requesting payment of a bill that does not match recipient's balance and asking for payment via a specific platform or method, and

• When using an established company phone number, the inability to reach the person from which the communication was relayed.

International Threat Reporting

Drone activity observed near Total offshore installation in North Sea[6]

TotalEnergies said on Thursday it had observed "unauthorized drone activity" near one of its offshore oil and gas installations in the North Sea.

Denmark, has like other countries in the region, raised its safety level for its power and gas sector after several countries said two Russian pipelines to Europe spewing gas into the Baltic Sea had been attacked.

"There have been observations of unauthorized drone activity at the Halfdan B oil and gas field in the North Sea," a spokesperson said in a written comment, adding the activity had been observed on Wednesday.

"We have taken the necessary steps in accordance with our security procedures and are in close dialogue with the authorities."

[6] https://news.yahoo.com/drone-activity-observed-near-total-163842016.html