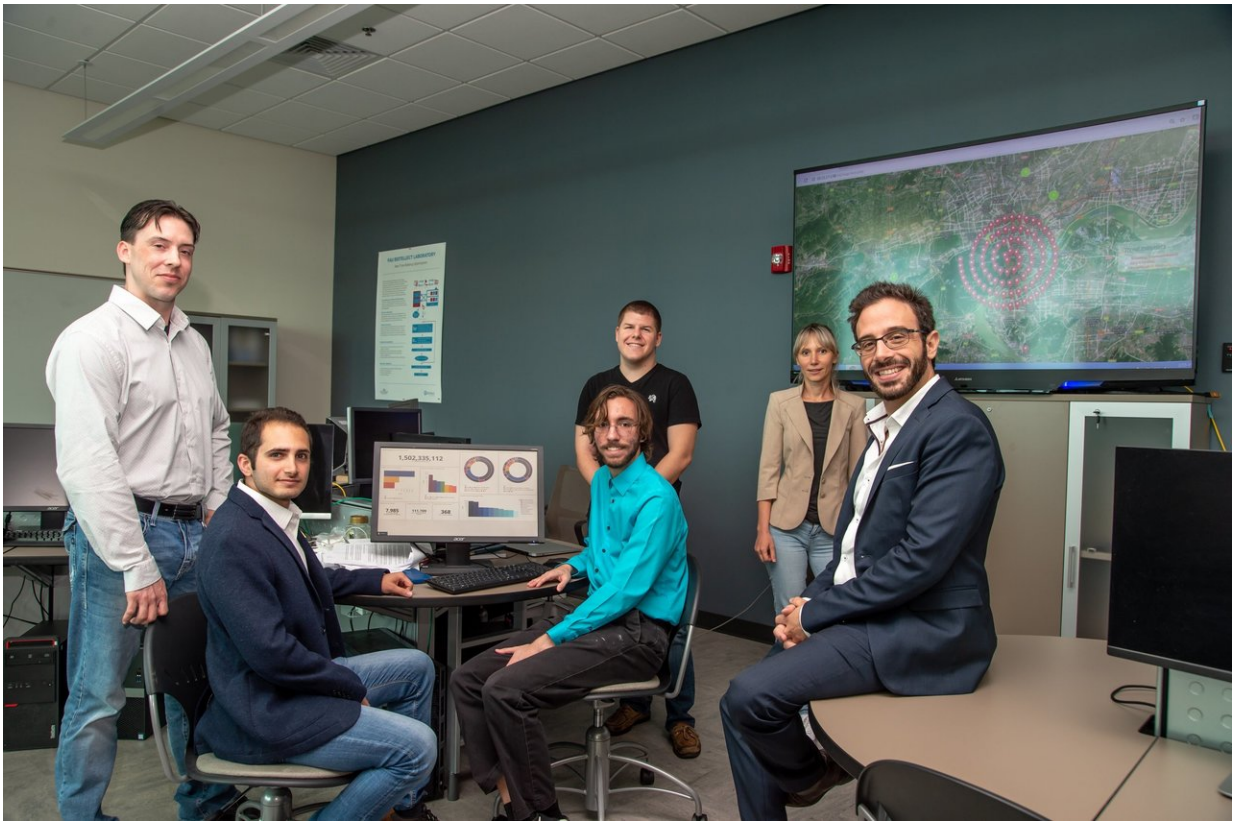
Report provides 24-hour view of cyberattacks in Florida, US

June 20 2018



(From the left) - Members of the FAU Cyber Threat Intelligence Laboratory and FloridaSOAR: Kurt Friday; Morteza SafeiPour; Eric Oster (seated); Dominic Cassisa; Nataliia Neshenko; and Elias Bou-Harb, Ph.D. (seated), assistant professor and director in FAU's College of Engineering and Computer Science. Credit: Florida Atlantic University

The Internet of things (IoT) - smartphones, vehicles, smart buildings, home appliances and other devices that use electronics, software and sensors—have transformed the way people around the world live and work. But not without risks. Data breaches and cyberattacks affect millions of businesses and households each year, hindering the integrity of critical systems, leaking private information and paralyzing Internet infrastructures.

Researchers from Florida Atlantic University's College of Engineering and Computer Science have generated a first-of-its-kind, large-scale analysis of the magnitude of compromised IoT devices worldwide and recently launched FloridaSOAR (security operation and response). The program has been designed to detect exploitations as soon as they are encountered, and then store and share that relevant threat information with IoT operators across the globe. FloridaSOAR can pinpoint malicious attacks and infections in near "real-time" by targeted sectors and Internet services providers within cities and counties in the United States and around the world.

Elias Bou-Harb, Ph.D., an assistant professor and director of the Cyber Threat Intelligence Laboratory at FAU and FloridaSOAR in FAU's Department of Computer and Electrical Engineering and Computer Science, has received a $175,000 research grant from the National Science Foundation to work on proactive inference of malicious IoT events.

"We know that most attacks originate from infected machines on the Internet," said Bou-Harb. "The technical challenge of dealing with this issue has been obtaining access to large volumes of data that represent an Internet scale perspective of this problem. FloridaSOAR is addressing this issue with large scale data analysis of a very specific type of traffic that is providing a global, Internet-wide look at infections."

Bou-Harb and his team recently scrutinized more than 5 terabytes of Internet-scale data to provide a unique 24-hour glimpse of cyberattacks and threats in Florida and the U.S. Results from this new report show that within a 24-hour timeframe:

- There were 250,779 malicious activities in the U.S.
- The top 10 infected states were California, New York, Texas, Florida, Illinois, Virginia, Georgia, New Jersey, Ohio and Michigan.
- California had 51,208 attacks; New York had 23,739 attacks; Texas had 18,342 attacks; and Florida had 15,694 attacks.
- Targets hit the hardest were power utilities, water facilities and manufacturing, with Georgia, California, Oregon, New York and Texas at the top of the list.
- In Florida, counties with the highest infection rates were Miami-Dade (4,074), Orange (1,667), Broward (1,663), Hillsboro (1,281), and Palm Beach County (903).
- Florida cities with the highest infection rates for all hosts were Miami, Orlando, Tampa, Hialeah, Jacksonville and Fort Lauderdale with Boca Raton ranking in the No. 10 spot.
- Florida cities with the highest IoT infection rates were Miami, Orlando, Tampa, Jacksonville, Hialeah, Fort Lauderdale and Boca Raton.
- In Florida, IoTs most affected by malicious activities were webcams, routers, firewalls, voice over IP and storage devices.
- In Florida, for denial-of-service (DDoS) attacks (perpetrators target a machine or network to make it unavailable to its intended users), the top targeted industries were Internet service providers, data services and telecommunications.
- Florida counties with the most DDoS victims for all hosts were Miami-Dade, Palm Beach, Orange and Broward; for IoT victims it was Miami-Dade, Orange, Palm Beach and Broward.
- Florida cities with the most DDoS victims for all hosts were

Miami, Orlando, Boca Raton and West Palm Beach; for IoT victims it was Miami, Orlando, Boca Raton and Hollywood.

Bou-Harb's NSF-funded project is three-fold: to detect compromises in consumer sectors to remediate privacy issues and provide resiliency to critical infrastructure; to understand how these attacks are coordinated and launched; and to place the information generated in an accessible database that other IoT operators can use for remediation. To that end, the research team is building the techniques, algorithms and methods needed to detect coordination patterns and strategies used by cyber attackers.

"Professor Bou-Harb's work in the Cyber Threat Intelligence Laboratory and through FloridaSOAR will have a tremendous impact on addressing a rampant issue that affects millions," said Nurgun Erdol, Ph.D., chair of FAU's Department of Computer and Electrical Engineering and Computer Science. "Moreover, this program will help to train diverse and highly qualified professionals in the cybersecurity field who are in great demand in the industrial world."

It is estimated that there will be about 6 billion Internet users worldwide by 2022 or 75 percent of the projected world population of 8 billion.

Provided by Florida Atlantic University