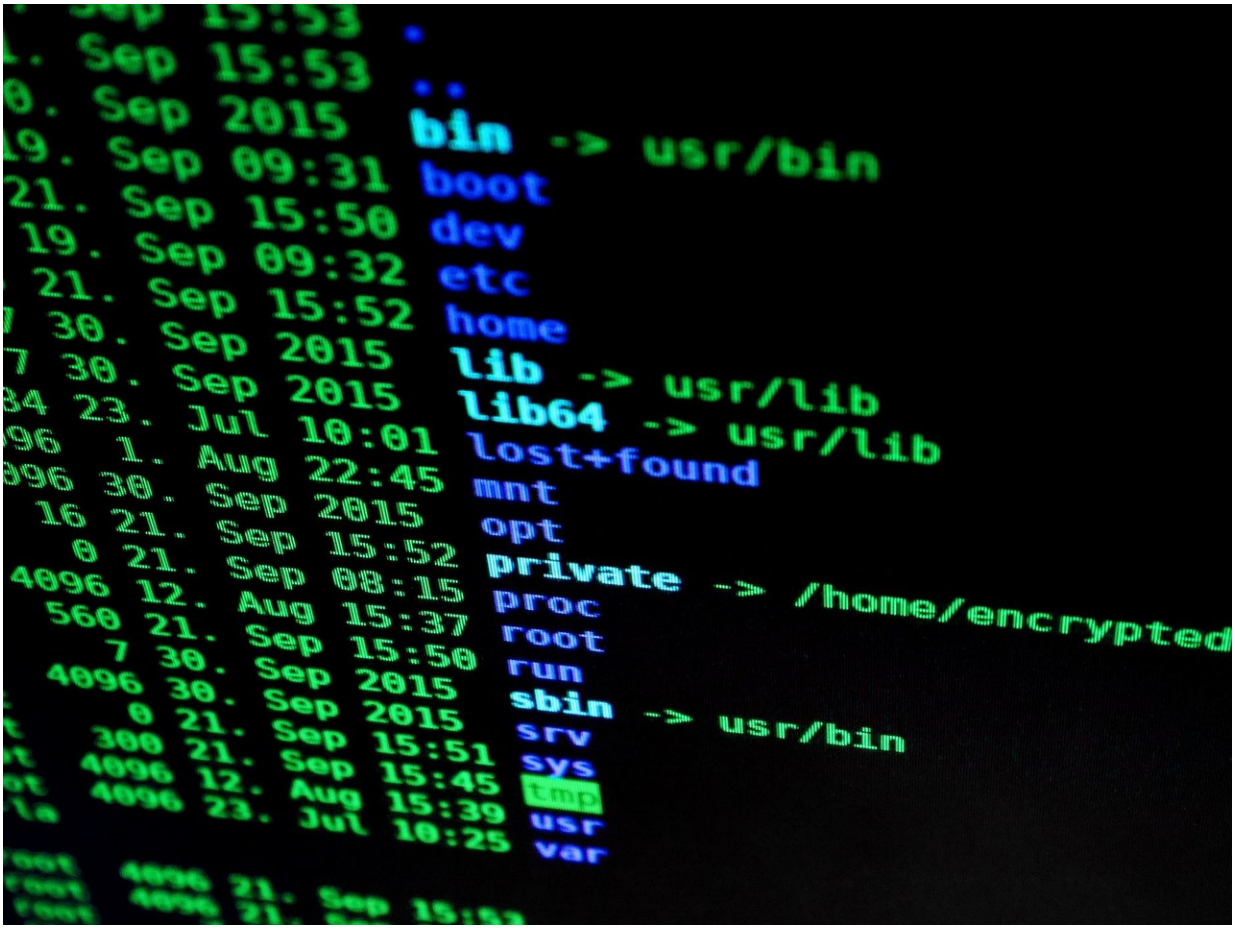
Security solution traps cyber criminals in a virtual network

September 10 2020



Credit: CC0 Public Domain

Researchers are developing a new cyber-security deception solution that

uses artificial intelligence to lure hackers away and prevent breaches of network systems.

Cybercriminal activity costs the UK billions of pounds annually and according to the Cyber Security Breaches Survey 2020 almost half of businesses reported having cyber security breaches or attacks in the last 12 months.

The "Lupovis" solution under development by the team at the University of Strathclyde's Center for Intelligent and Dynamic Communications makes the hunter become the hunted.

Sophisticated narrative

Once an attacker has penetrated a network, the system entices them by creating a sophisticated narrative designed to make the hacker believe they are successfully accessing and progressing through the system.

Lupovis, an amalgamation for the Latin words for wolf (lupus) and sheep (ovis), also offers the attacker incentives and steers them in a certain path.

The team is in the process of creating a Strathclyde spin-out company to commercialize the system focusing on critical infrastructures, starting with the energy sector as an initial market as a way of protecting energy supplies.

Principal investigator and entrepreneur Dr. Xavier Bellekens from the University of Strathclyde, said: "A successful breach can cost a company millions of pounds in terms of loss revenue, can compromise trust and cause reputational damage. After a hack, it can take a company up to hundreds of days to get back to full operation. Our solution provides an offensive deception environment, which engages with the attacker from

the minute the attacker moves within the network. Lupovis deploys decoys to engage with the attacker when a breach occurs. These decoys lure the attacker away from the assets, whether it be personal data or sensitive information, or hackers trying to shut down the system to damage business continuity. "

Artificial intelligence

The system uses Artificial Intelligence to create scenarios which lures the attacker into believing they are progressing towards assets, but which mirror the existing infrastructure. In reality, the cyber-criminal's breach into the network is being monitored by the company's Security Operations Center.

Dr. Bellekens added: "Hackers are highly sophisticated and skilled, and so for Lupovis to succeed we need to build a convincing narrative. The system engages and understands their next moves through the network and what their behavior patterns are, to divert them away from valuable assets and arrest the breach effectively. We respond to their behavior and skills level by using incentives and gamifying vulnerabilities. The gamification aspect is important as you need to keep offering incentives if you want them to move down a particular path. The longer we keep them engaged, the longer we are keeping them away from assets and are blocking the malicious actions that would stop the network functioning, maintaining business and operational continuity."

The team say the software actually keeps on learning and becomes more accurate as more data is collected by the system.

Professor Ivan Andonovic from Strathclyde, who will be a director of the spin-out company, said: "There are currently no similar solutions, as decoys are usually static, and once a decoy is exploited by a cyber-criminal, they can continue moving toward valuable assets in the network

. Lupovis offers a dynamic system turning networks from a flock of sheep to a pack of predators."

Provided by University of Strathclyde, Glasgow