yorku.ca

How York researchers are strengthening cybersecurity

alexhuls

6–7 minutes

ByAlex HulsApril 24, 2026

York University researchers are exploring how to better secure a digital world increasingly shaped by the Internet of Things (IoT) by understanding how malicious bots operate and developing stronger defences against them.

IoT devices are everyday objects that connect to the internet so they can send, receive and act on data. They range from home thermostats and baby monitors to traffic sensors, medical equipment and industrial controls. Many operate quietly in the background and are rarely updated or closely monitored, making them especially attractive targets for cybercriminals.

“As devices proliferate globally, so do the botnets that exploit them,” says **Arash Habibi Lashkari**, a professor in the Faculty of Liberal Arts & Professional Studies and Canada Research Chair in Behaviour-Centric Cybersecurity (BCCC). Botnets are networks of compromised devices that have been quietly taken over by attackers and can be coordinated to carry out cyberattacks, often without the device owner’s knowledge.

Arash Habibi Lashkari

While cybersecurity tools already exist to protect IoT systems, Lashkari says many struggle to keep pace with today's threat landscape. Designed for specific networks or environments, these tools are often not suited to the scale or complexity of a borderless digital world, where malicious activity moves easily across regions and frequently reuse similar behaviours in different contexts.

As a result, security frameworks often rely on AI to sift through vast volumes of data and spot patterns too complex or fast-moving for humans to catch. This, however, comes with a shortcoming: AI can flag suspicious activity, but without explaining how or why a particular behaviour is considered malicious.

"That's the primary gap of the 'black box' nature of AI in cybersecurity," says Lashkari, referring to systems that can produce answers without making their reasoning visible to humans. "Understanding these gaps is critical, because a detection system that cannot explain why it flagged a behaviour is difficult to trust."

Lashkari set out to resolve that gap. He and his colleagues aimed to find a way to analyze how botnets operate and build an identification approach to act on that knowledge. In doing so, it can produce results that human analysts can interpret, trust and apply across different networks.

In research now published in *Supercomputing*, Lashkari and his colleagues built and tested a recognition and profiling system using real-world IoT network traffic. Working through BCCC, the team examined how compromised devices communicate across sustained activity, focusing on patterns that could be clearly interpreted.

This allowed the researchers to move beyond individual attacks and focus on broader behavioural patterns, including whether botnets

operating in different environments might still act in similar ways.

Lashkari says they expected to see some similarities across botnets, but were still surprised by how consistently those patterns appeared. Even when attacks targeted different technologies or deployments, compromised devices tended to follow the same underlying behaviours, including recognizable bursts of activity. That consistency matters, he explains, because knowing how one botnet operates can help identify and defend against others, even in very different settings.

Lashkari says the real importance of that finding lies in what it enables. “It suggests that a breakthrough in understanding a specific botnet profile – the recurring patterns in how compromised devices communicate and behave – can be generalized to protect critical infrastructure worldwide,” he says.

That potential is not theoretical. To act on it, Lashkari and his colleagues developed a system that identifies IoT botnets based on behavioural patterns observed across repeated interactions. The system flags suspicious activity while also showing which specific behaviours triggered the alert, giving security teams visibility into why a device was identified as malicious.

While the system itself is presented as a research framework rather than a ready-to-deploy product, much of the underlying IoT data and profiling resources developed through the BCCC are publicly available, allowing other researchers to study, test and build on the approach.

Lashkari says this approach is especially important because malicious cyber activity is constantly evolving. As security systems improve, attackers adapt their tactics, often reshaping malicious activity to blend in with normal internet traffic. By focusing on patterns that persist across sustained behaviour, rather than relying on fixed indicators that quickly

become outdated, the behaviour-based system can help security teams recognize emerging threats even as attackers change how they operate.

“The hope is that this work will serve as a cornerstone for more transparent, collaborative security frameworks,” Lashkari says. By promoting explainable tools and shared datasets, the team aims to shift industry practice away from simply blocking IP addresses, and toward understanding and anticipating how adversaries behave.

Lashkari says that need is unlikely to fade. As attackers continue to adapt, often operating slowly or subtly to avoid detection, focusing on behavioural patterns across time may become increasingly important. In an internet-connected world, he says, effective defence will depend not just on smarter identification, but on tools that help security teams know what they are dealing with.

Tags: