over a botnet, so they can then create their own competing masks from scratch. Then they just launch them through a customized browser the Genesis gangsters call Tenebris, and connect using an IP-address-mimicking proxy to make transactions that fool the fraud detection systems.

Lozhkin says the Genesis dark market has effectively turned the decades-old practice of credit card fraud (also known as 'carding') into a new, highly targeted, industrial-scale criminal activity. It's one slick high-tech operation: for instance, the Kaspersky team found the fraudsters had written algorithms that automatically price each doppelgänger, based on its fraudulent earnings potential.

Because the Genesis Store uses botnets to harvest data to construct its own fake masks, criminals can target victims directly. "A search panel lets users search for specific bots, website logins and passwords, the victim's country, operating system, date the profile first appeared on the market—everything is searchable," Kaspersky Lab says in an analysis of the offerings on Genesis that it has posted on its Securelist blog.

It appears to be popular. "We are seeing monthly increases in the numbers of [data-stealing] bots that are being sold on the market, and also in the numbers of cybercriminals that want to buy stolen information, so it's still growing," says Lozkhin.

Combating the Threat

On the front line of the antifraud industry, doppelgängers are indeed being seen as a latter-day adversary. "Our customers continue to see fraud attacks of many different types, including those using doppelgängers, and the landscape of these attacks changes daily," says David Excell, founder of Featurespace, one of the leading antifraud anomaly detection technology providers, with bases in Cambridge, U.K. and Atlanta, GA.

To fight digital payment fraud, Featurespace has developed a probabilistic machine learning platform that alerts finance firms to fraud attempts. Called the Adaptive Real-time Change Identifier (ARIC), it lets companies "construct their own doppelgänger for each consumer, in the form of an individual behavioral profile," says Excell. "Using these profiles, we're able to identify if the interaction for a customer is normal, based on how they've behaved in the past. Typically, a fraudster is revealed when they attempt to monetize their attack, because at that point, their behaviors aren't matching the ones we expect to see from the actual customer."

Like its rivals in the anomaly detection arena, Featurespace does not reveal how its proprietary algorithms spot that mismatch. However, Excell says, defending against digital fraud is about far more than the 'secret sauce' behind their ever-changing algorithms. "Protecting a financial institution from fraud is no easy task and relies on a combination of data, technology and processes," he says.

One measure finance firms can take in the war against fraud is to eschew the use of standalone disconnected businesses. "Financial institutions tend to operate multiple business units in silos, making it difficult to join systems together. This is one of the weaknesses that fraudsters often try to exploit," says Excell.

By linking data sources in such units together and having oversight of customer interactions across many channels, Excell says, "financial institutions can build individual behavioral profiles in real time to spot the unusual or incorrectly mimicked behavior of the fraudster." As an example, he points to how the channels a bank would need to integrate would include traffic on its online service, its mobile app, transactions undertaken in the branch, and also those on the phone.

It's the sunk costs in older technology, such as the kit and code in those silos, that are leaving some firms behind in the cyber arms race against fraudsters, says Ian Thornton-Trump, an IT security analyst at cybersecurity insurer and underwriter AmTrust Financial Services in New York City. "The current cybersecurity problem has little to do with security controls or their effectiveness: the arch nemesis of cybersecurity is network complexity and technological debt," he says.

The problem, he says, is that while physical network complexity has changed little, logical network complexity has gone through the roof with the addition of low-cost, off-premise, cloud-hosted software-as-a-service

ACM Member News

PRODUCING LEADERS FOR THE NEXT CS GENERATION

"I was lucky," says Huan Liu, a professor of computer science (CS) and engineering at Arizona State University (ASU), when reflecting on the trajectory of his career. "I picked computer science in college, I picked AI (artificial intelligence) when doing my Ph.D. research, I picked machine learning after I graduated, and then I moved into data mining."

Liu earned master's and Ph.D. degrees in computer science from the University of Southern California, following an undergraduate degree in computer science and electrical engineering from China's Shanghai Jiao Tong University.

Before joining the faculty at ASU, Liu worked in the Research Labs of Telecom Australia Research Labs, and was affiliated with the faculty of the National University of Singapore.

Liu's research interests are in data mining, machine learning, social computing, and artificial intelligence. He investigates interdisciplinary problems that arise in many real-world, data-intensive applications with high-dimensional data of disparate forms, such as social media.

His current research focus is on causal learning with data, detecting fake news and bots, and also how to preserve privacy in social media. He works to discover actionable patterns or insights from data, particularly social media.

Liu is highly invested in his students. His senior doctoral students guide junior members and help them to succeed, and through this process they naturally become leaders. "The key for me is to produce the next generation of top computer scientists," he says.

Liu takes pride in his graduates, pointing out that many co-authors of his published research are former students who have now moved on. "I follow my students to success."

—John Delaney