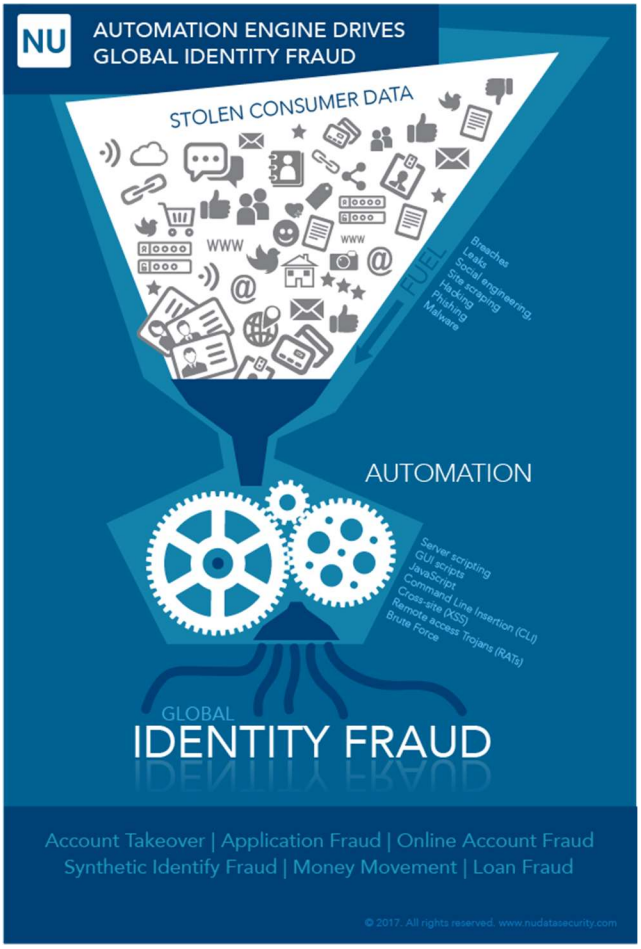
Automation: The Engine of Identity Fraud

Robert Capps, Vice President of Business Development for NuData Security



It should be crystal clear that data breaches continue to feed personal data into the online criminal underground aka the Dark Web. This data fuels the worldwide epidemic of identity fraud. And, while this user data could rightfully be considered fuel for the engine, the mechanism that truly makes this industry of cybercriminals function at scale is cheap and effective automation.

Over the 2016 holiday season, NuData scientists discovered a 400% year-over-year increase in sophisticated automation. These attacks were caught by NuDetect and had they been successful, would certainly have created a spike in application fraud and account takeover attacks.

Application fraud

Financial application fraud is where the fraudster poses as a legitimate customer using valid personal data to open new accounts for the purpose of obtaining new credit and financial products, and at times used for mortgage fraud or insurance fraud. Sometimes, but not as often, this can be a made-up (fake) person using forged credentials as in

synthentic identity fraud, or the impersonation of a deceased person with either forged or valid credentials. In the case where they're using an existing person's valid credentials the victim's credit score and financial life can be ruined in the process.

From within these fraudulent accounts, the fraudster will typically make small transactions or updates to show activity and then proceed with a large transaction or a series of medium-sized transactions designed to stay below amounts that might trigger a closer inspection.

Account takeover fraud

Account takeover (ATO) attacks consist of unauthorized access to a customer's existing account using valid credentials. The criminals will use the account for transactions or for data or asset collection to be used in other cybercrime. Either one of these types of identity fraud can range from a simple brute force type of attack using automated scripts to run through thousands of possible password combinations to test account access for a later takeover to complex and sophisticated attacks using bots that pretend to be real users by impersonation.

Over the 2016 holiday period, NuData scientists witnessed an increase in bad actors using legitimate GUI-like automation trying to manipulate how pages are used to appear more human. By masking the automation these fraudsters demonstrate a growing understanding of how threat detection systems work. They also are adjusting the mode and phasing of their attacks. For example, they will use basic bots to perform velocity type functions and complex bots to spoof IPs, or emulate devices, apps, or browsers to perform higher value transactions.

Good bots – not all bots are bad

A new trend is for cybercriminals to automate account verification activities using legitimate financial services aggregators. Couple this with the presence of many helpful scripts, bots, apps and websites deployed across the internet that requires login access to customer accounts to fulfill their promise.

Any good automation detection system must be able to distinguish between user-sanctioned ('friendly') automated activity and that which might be unfriendly or malicious. The downside of getting this wrong can be an extreme loss either from inconveniencing good customers or by letting the bad guys in the front door.

Fraud is becoming an identity issue

Application fraud, and account takeover attacks against financial institutions frequently use automation at scale and involve serious fraud such as money movement and transfer schemes ranging from the simple to elaborate.

Any time the legitimate user can't be accurately verified is an opportunity for risk to creep in. The right detection tools can provide more confidence about who is the legitimate human user, as opposed to malicious automation, and will go a long way toward reducing fraud risk.

About the author:

Robert Capps is the vice president of Business Development for NuData Security. He is a recognized technologist, thought leader and advisor with more than 20 years of experience in the design, management and protection of complex information systems – leveraging people, process and technology to counter cyber risks.