TEXAS LAWYER

Commercial Accounts Targeted by New Breed of Bank Robber

Steve Thomas

Texas Lawyer (Online)

June 7, 2016 Tuesday

In April, a new breed of bank robber hit 24 U.S. and Canadian banks, scooping up $4 million in less than two weeks before heading to Europe and stripping millions more from 17 Polish banks and one major Portuguese bank. From all reports, the bandit is just getting warmed up, with hundreds more banks on the list.

But this crook is code. Dubbed GozNym by security experts, it's the progeny of Gozi and Nymaim, two forms of malware each considered powerful and dangerous standing alone. In GozNym, they have spawned an efficient predator that feeds on financial institutions by attacking them through their weakest and most lucrative vulnerability-commercial banking customers.

First, meet the parents. Nymaim is a two-stage malware "dropper" known for its stealth and persistence. A victim clicks on an infected email attachment or triggers an exploit kit on an infected website, and Nymaim slips silently into the victim's computer, evading antivirus detection, evaluating weaknesses, monitoring activity, sending intel back home, waiting. When the time comes, Nymaim's second stage delivers a software payload of its master's choosing, often ransomware designed to lock up the computer.

Gozi is worse. Created and unleashed in 2007 by Nikita Kuzmin, a 28-year-old Russian computer scientist, Gozi was designed to silently watch as computer users log into their online bank account, then collect their credentials and send them back home so Kuzmin could drain the account. It worked so well, Kuzmin rented Gozi out to other criminals for $500 a week on black market websites, allowing his customers to access the collected credentials from his server as long as they paid their rent. When Kuzmin was caught, his server contained data for 10,000 accounts from more than 5,000 computer users, including login information for accounts at leading global banks and financial services firms.

The investigation discovered that strains of Gozi had infected more than a million computers in various countries. Its U.S. victims included NASA-even rocket scientists were not immune. Kuzmin pled guilty to various computer intrusion and fraud charges in 2011, and on May 2, 2016, Kuzmin was sentenced to 37 months in U.S. federal prison.

But in November 2015, security experts noted instances where Nymaim fetched a Gozi web-injection module and used it to launch online banking attacks. Apparently, the combination caught the attention of organized cybercriminals operating out of Russia, and they married the two into a single piece of malware. Thus GozNym was born.

And it was born with a silver spoon. Before launching GozNym, its well-financed creators developed 230 fake web pages that were identical in appearance to the log-in pages of 230 different financial institutions. They also created corresponding "web injections"-pop-up boxes or web pages that ask the user for additional information, such as the

user's mother's maiden name or the contact preferences for two-factor authentication. After all, the criminals would be signing in from a different computer. The bank would need verification. GozNym provides the criminals with every piece of information they need to fool the bank and complete the transfer.

GozNym comes equipped with the URLs of the 230 target banks in its configuration file. When the user tries to access one of those banking log-in pages, the user's browser is "redirected" to the fake page on the cybercriminals' server in Moscow, Russia. It looks like the bank's log-in page. It even has the proper security certificate indicator in the browser's address bar.

After gathering user name and password, GozNym loads web-injection pages from a different server in a different part of the world (making the intrusion harder to trace). Those web injections ask for the additional information needed to log in from a new computer. From the user's point of view, the bank is asking. Absent extraordinary care and diligence, no one knows there's a problem until the money is gone.

These are "redirection attacks," the province of well-financed organized crime employing teams of developers and using "social engineering"-the con game that dupes unsuspecting users into believing the web site is actually that of their employer's bank.

Who pays for wire fraud against a commercial bank account? In the U.S., Regulation E of the Electronic Fund Transfer Act (specifically, 12 C.F.R. §1005.6) generally protects diligent consumers from fraud losses by transferring that risk to the bank. But commercial banking customers are held to a higher standard under Article 4A of the Uniform Commercial Code.

In June 2012, Luna & Luna LLP, a real estate escrow firm in Garland, Texas, was using a commercial bank account at Texas Brand Bank, also in Garland, to hold funds belonging to the U.S. Department of Housing and Urban Development. Hackers captured Luna's log-in credentials and stole about $1.67 million from that account in multiple transfers destined for the Heilongjiang province of China, near the Russian border.

The bank replenished the funds to avoid trouble with Uncle Sam, but then sued Luna to recover the money, alleging that Luna had declined the use of "dual controls" on its many wire transfers. Luna counterclaimed, arguing that the bank's security was deficient. After three years of litigation, the case settled in late April 2016, but it illustrates the painful fallout of a successful cyberheist against a commercial account.

Exactly the kind of account GozNym targets. Cybersecurity experts say this is just the beginning. GozNym will expand and improve. Financial institutions and their commercial customers face a new world of organized crime where literal fortunes can be lost with a single click, and the ounce of prevention far outweighs any pound of legal cures.