The Year in Cybercrime: Exploiting the Weakest Link

Analysis

November 30, 2016 | 09:04 GMT

The weapons used to conduct cyberattacks are relatively new, but the tactics employed have been around for centuries. (KIRILL KUDRYAVTSEV/AFP/Getty Images)

Forecast

---- Hackers will continue to rely on social engineering tactics to exploit their victims.

---- State and state-sponsored actors will turn increasingly to cybercrime to advance their national interests.

---- Technological improvements to counter cybercrime will not protect against human vulnerability.

Analysis

Editor's Note: This analysis was produced by Threat Lens, Stratfor's unique protective intelligence product. Designed with corporate security leaders in mind, Threat Lens enables industry professionals to anticipate, identify, measure and mitigate emerging threats to people and assets around the world.

The rise of the internet and related technologies has transformed the world, revolutionizing nearly all aspects of everyday life, including crime. In September, the Global Cyber Security Leaders summit in Berlin highlighted the cyberattack tactics that pose the greatest concern to security professionals. Many of these coincide with the threats that we have covered over the past year on Threat Lens, Stratfor's new security portal. Some transcend criminal activity and involve state or state-sponsored actors using tricks of the cybercriminal trade to advance their countries' agendas. Though the weapons used to conduct cyberattacks are relatively new — and rapidly evolving — the tactics have been around for centuries. Over the past year, several major crimes have combined the new platforms and greater access that the information age affords with the age-old art of social engineering. The tactics described below are by no means the most sophisticated of their kind, but they have proved to be some of the most successful and enduring.

An Online Heist in Bangladesh

One of the first cyberattacks of the year was also one of the most troubling. In February, suspected North Korean hackers managed to finagle $81 million in transfers from Bangladesh's central bank — well short of the attempted $1 billion, but an impressive sum nonetheless. The hackers first gained access to Bangladesh Bank's Society for Worldwide Interbank Financial Telecommunication (SWIFT) system, which banks use to make and track transfers. Posing as officers from Bangladesh Bank, the hackers then used the SWIFT software to request transfers from the central bank's accounts with the New York Federal Reserve to various entities around Asia.

The SWIFT platform is an attractive target for hackers because it handles tens of millions of transfer requests each day across virtually the entire global financial industry. (SWIFT is so widely used that the U.S. government has sought the service's cooperation to block terrorist financing and enforce sanctions against rival countries such as Iran.) Gaining access to a bank's SWIFT account is tantamount to obtaining the keys to its vault, but it was not enough to pull off the crime without a hitch. Once the hackers had entered Bangladesh Bank's secured networks, studied the institution's common practices and gained access to SWIFT, they tweaked software on SWIFT's servers to cover their tracks.

The attack's meticulous planning and execution suggest that it was the work of an organized team with a state sponsor, and investigators later found the attack deployed code similar to that used in past cybercrimes linked to North Korea. On their own, North Korea's well-known financial woes would certainly provide a motive for a major theft like the Bangladesh Bank heist. But for Pyongyang, there is the added allure of attacking part of the international financial

system that has kept sanctions on the country for its nuclear weapons program. Though the sanctions against North Korea have never gone so far as to restrict its SWIFT access, they have all but cut the country's economy off from the rest of the world. As a target, SWIFT offered a perfect opportunity for Pyongyang to antagonize the international financial services sector and make some money in the process.

Despite its technical proficiency, the attack was also opportunistic. Investigations found significant security failures in Bangladesh Bank's networks that the hackers likely exploited. Still, the theft was unique in that it targeted SWIFT using an old trick known as the fake CEO scam, or as the FBI calls it, the Business Email Compromise — something of a misnomer since the tactic long predates email. In fact, one of the most famous examples of the scam was carried out by phone. Gilbert Chikli swindled millions of dollars out of various companies in the mid-2000s by calling employees and, posing as their company executive, instructing them to transfer money to certain accounts — all his — under the guise of official business. In the Bangladesh Bank case, the perpetrators used the same strategy with slightly different tactics, infiltrating the bank's email network, likely through a phishing attack, and using the SWIFT system to order money transfers to dozens of accounts. After the heist, the FBI and SWIFT noted an uptick in both CEO scams and attacks on the financial messaging service over the past year. But the Bangladesh Bank incident is the first reported theft to use the tactics in tandem, to devastating financial effect.

Taking Data Hostage

The past year has seen a rise in ransomware attacks, in which perpetrators gain access to and seize files, and sometimes entire devices, freezing them until their owner pays a ransom. In conducting these attacks, cybercriminals typically go after a high volume of targets ill-equipped to deal with such a strike and demand a relatively small sum of money from each, usually in bitcoin or another digital currency. Even people without the savvy to set up a ransomware ploy on their own can purchase kits online for a few hundred dollars and get their money's worth after a single successful strike. Most of the high-profile ransomware cases this year targeted hospitals, which lost access to critical files for the duration of the attacks. Some victims, such as the Hollywood Presbyterian Medical Center in Los Angeles, opted to pay a relatively inexpensive ransom ($17,000 in this case) rather than deal with the cost and inconvenience of retrieving the data with help from information technology personnel. In April, a NASCAR team also found it more expedient to pay its $500 ransom to get back an estimated $2 million worth of information just days before a race worth millions more in advertising.

But paying a ransom does not guarantee that the locked data will be recovered. In many instances, ransomware operators leave files frozen after receiving payment out of negligence or incompetence. Furthermore, even if the data is retrieved, the attack may have compromised its integrity. Ransomware attacks are fairly easy to overcome, however. The tactic compels businesses to pay up by disrupting workflow — for instance, preventing a hospital from

accessing patient files or a NASCAR team from seeing the wind-tunnel data it needs to adjust the aerodynamics on a car. If that data is backed up somewhere accessible, the victim will have less need to comply with attackers. San Francisco's light rail, the Muni Metro, demonstrated the value of that strategy Nov. 26, when a ransomware attack disabled its ticketing system — though only temporarily. Instead of forking over the ransom, Muni Metro's IT department worked around the problem and got the system back up and running the next day. In the meantime, riders were allowed to use the light rail for free.

So far, reported cases of ransomware have all been fairly modest in strategy and execution; attackers seem to be casting a wide net and charging their victims indiscriminately. In the future,

though, more sophisticated attackers may do their research, targeting major banks, government agencies or strategic industries and demanding payments commensurate with the value of the locked data. Ransomware is still an opportunistic weapon, but with more deliberate planning and pre-operational intelligence, criminals could easily use it in a targeted application for a bigger payout, much as "tiger kidnappers" leverage their victims to get hefty rewards.

The Physical Dangers of Phishing

This year has also demonstrated the enduring popularity — and efficacy — of phishing and spear-phishing, cyberattack techniques that rely on social engineering to gain illicit access to networks and information. In August, following a yearlong doping scandal that eventually barred 118 Russian athletes from participating in the 2016 Summer Olympics, the World Anti-Doping Agency reported that Russian-backed hackers had used a phishing attack to infiltrate its networks. The attackers then stole information about athletes in the agency's database, including Yulia Stepanova, the Russian runner who blew the whistle on her country's doping program.

Though the hack in general seemed to be an attempt to incriminate other athletes, the intruders released personal details about Stepanova, such as her home address, in an apparent act of intimidation. Stepanova subsequently announced in a press conference that "if something happens to us … it's not an accident." No ill has befallen her or her family, but she had good cause for worry: The director of Russia's anti-doping agency died suddenly in February, two months after he tendered his resignation in response to the scandal. Even without evidence of foul play in his death, its timing was enough to spook Stepanova, and the passive threat against her illustrates the possible physical applications of a cyberattack.

Similarly, a spear-phishing attack on Ahmed Mansoor, an Emirati human rights activist, could have had grave repercussions offline. In August, Mansoor received a series of enticing text messages in which the anonymous sender included a hyperlink said to lead to new revelations about torture in the United Arab Emirates' prisons. Having been the target of previous spear-phishing attacks, Mansoor knew better than to click on the link and instead forwarded the messages to a Canadian research group. The group determined that the text was an attack containing software that could have allowed his attackers control over his cellphone and the means to track his movement. Though it is unclear what the assailants planned to do with the information, given his controversial line of work, it is easy to imagine that they might have tried to do their victim physical harm.

Intent Without Ability

On the other side of the screen, Charles Eccleston pleaded guilty in February to charges that he had been involved in a spear-phishing scheme. Using his position as a scientist at the U.S. Department of Energy, Eccleston sent emails to employees at nuclear labs infected with what he thought was malware. (The incident was actually part of an FBI sting operation against Eccleston, who had been identified as a threat after approaching foreign governments and

offering to sell them the email addresses of all Department of Energy employees.) As an insider, Eccleston had access to and knowledge of contacts in sensitive positions that enabled him to tailor his emails to make them more specific and believable — traits that distinguish more sophisticated spear-phishing from phishing. But like the dozens of aspiring jihadists who have been wrapped up in similar FBI stings over the years, Eccleston lacked the know-how to carry out the attack. He had to seek outside help to weaponize his privileged position, which led him to an undercover agent.

As cyber weapons become more accessible and easier to use, would-be attackers such as Eccleston may have an easier time carrying out attacks on their own. This would pose a big problem for counterintelligence agencies. After all, had authorities not identified him ahead of time, Eccleston could have used his insider knowledge to introduce hostile intelligence assets into Department of Energy and related networks.

Tried-and-True Tactics

Throughout the year, these attack methods have stolen headlines and set the cybersecurity world abuzz, but they are far from the only threats lurking online. Hacks into email servers at sensitive times — for instance, during the U.S. presidential race — commanded the world's attention this year, and similar attacks will remain a popular tool. A distributed denial of service attack that shut down major media websites in October demonstrated the vulnerabilities that the internet of things has introduced by connecting more and more devices, risks that will only increase as the technology expands. Several unlimited attacks on ATMs over the year have also highlighted the growing intersection between cyber and traditional crime, a trend that will likely continue.

To combat the proliferating risks they face in the cyber realm, countries around the world will keep honing their technical prowess. But as with physical threats, the most advanced weapons will not necessarily be the most effective against cyberthreats. As technological defenses improve, cybercriminals will continue to focus their attacks on the most vulnerable link in the technological chain: the human.