Malicious intent

Mortgage companies face security threats from within and without

Sarah Wheeler
July 1, 2014

It's been a bad year for data breaches, and it seems like it will only be a matter of time before a data breach, on the scale of the Target breach, hits a mortgage firm. And considering the depth and breadth of personal information gathered on each and every borrower, the headline risk, not to mention the impact on mortgage customers' lives, could be far more explosive than what the retail giant felt.

The threats that financial firms face are formidable, and growing. Banks represent a huge target for cyber crime for obvious reasons — vaults of personal information are every bit as valuable as stacks of money. The wide adoption of a true digital mortgage — called for by many in the industry and regulators such as the Consumer Financial Protection Bureau — could multiply the risk of mortgage data breaches, exposing millions of homeowners to the nightmare scenario of identity theft.

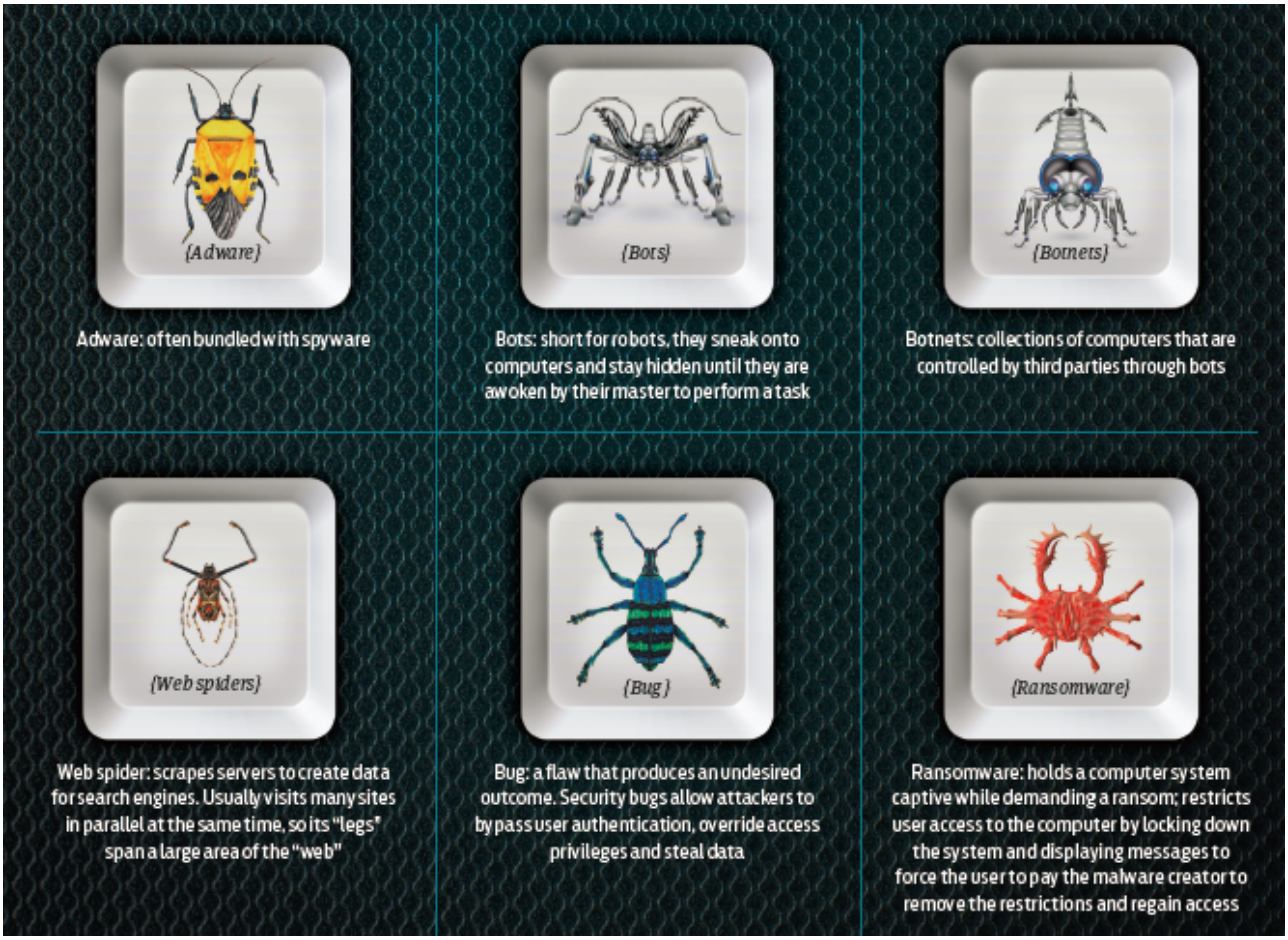
CASE IN POINT

Consider F. Trey Ordonez. A vice president at Fidelity National Title, he is scheduled to move from Dallas to Scottsdale in a few weeks and recently sold his house. He is opting to rent in Arizona, but just the thought of going through the mortgage application process causes him to shake his head. Several years ago Ordonez had his identity stolen and taxes were filed in his name and the name of his wife and daughters. He is still trying to clean up the mess.

“I haven’t looked at my credit report in years,” he said. “I’m staying in cash for as long as possible.”

While the IRS understands that Ordonez’s Social Security number is “compromised,” it wants him to pay the taxes owed from the fraudulent filing. He maintains boxes of records — proof of his innocence, he says — but it falls on deaf ears. Local, state, national — Ordonez has tried to get help at every level, yet he still he faces this nightmare alone. And there’s no end in sight.

“You can’t change your Social Security number,” he said. “I’m still no closer to learning who did this, and they still have my number.”



THE SCALE

In the Ponemon Institute's 2014 Cost of Data Breach report, 51% of CEOs surveyed said their company experienced cyber attacks daily or weekly. Symantec reported a 62% rise in the number of data breaches from 2012 to 2013.

A data breach is bad for any business, but for a bank the stakes are even higher. Think of the ordeal Ordonez has endured and imagine if the identity theft had occurred within a mortgage firm. Multiply his misery by a thousand borrowers, with every Social Security number in the hands of identity thieves. The fallout from such a breach is a looming hazard that no doubt keeps lenders up at night.

Banks and other lenders face not only the initial cost of a breach, but the reputational risk of having secure data compromised. Financial services firms are among the industries that experience the highest customer turnover as a result of a data breach, the Ponemon report stated.

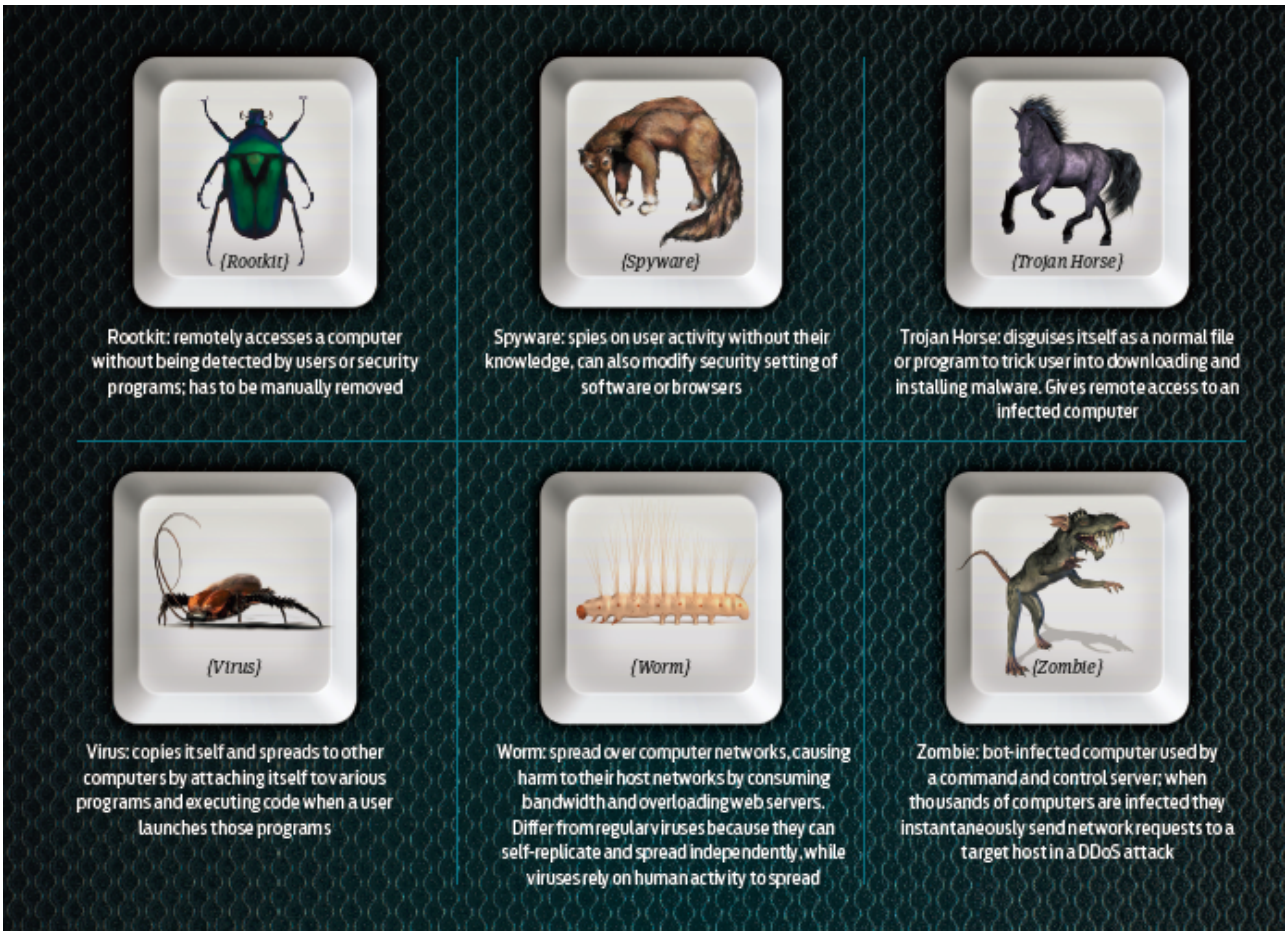
"The research reveals that reputation and the loss of customer loyalty does the most damage to the bottom line. In the aftermath of a breach, companies find they must spend heavily to regain their brand image and acquire new customers," according to the report. The average cost to a company for a security breach? $3.5 million and rising.

DIGITAL MORTGAGE AN EVEN GREATER THREAT?

With the cost of originating mortgage loans now resulting in a net loss to lenders, the digital mortgage has been hailed as a crucial part of industry survival. The CFPB has launched a pilot program for electronic closings, one

step in an end-to-end digital mortgage.

"The CFPB believes that there may be opportunities to leverage technology to solve some of the issues that cause frustrations for both consumers and professionals in the mortgage closing process," the pilot overview stated. "Specifically, the bureau hypothesizes that technology-enabled electronic closing (eClosing) solutions may have the potential to improve consumer understanding and empowerment and efficiency for all involved."



As reported in the March issue of HousingWire, the efficiencies of a paperless mortgage will enable lenders to originate loans that meet compliance regulations while costing significantly less to generate.

All good news — at a time when the industry could really use some.

Except that the threat to data security could increase dramatically the more a process is digitized. Another Ponemon study, released in June — "Data Breach: The Cloud Multiplier Effect" — surveyed 613 IT professionals and had these key findings:

- 62% of respondents do not agree or are unsure that cloud services are thoroughly vetted before deployment
- 69% believe there is a failure to be proactive in assessing information that is too sensitive to be stored in the cloud
- 71% fear their cloud service provider would not notify their organization immediately if they had a data breach involving the loss or theft of customer data
- 69% do not agree that their organization's cloud service uses enabling security technologies to protect and secure sensitive and confidential information

- 64% say these cloud service providers are not in full compliance with privacy and data protection regulations and laws

That's a sizable no-confidence vote from IT professionals, and it only echoes the concerns of others. The Cloud Security Alliance, a nonprofit with a mission to promote the use of best practices for cloud computing, outlined cloud security threats in February.

"Cloud computing introduces significant new avenues of attack," according to the CSA. "An increase in the backup and storage of sensitive and/or confidential customer information in the cloud can cause the most costly breaches. The second most costly breach occurs when one of the organization's primary cloud services providers expands operations too quickly and experiences financial difficulties."

The growing use of mobile banking apps — including mortgage apps — presents another potential vulnerability.

"Banks are recognizing that the millennial generation represents the largest demographic in the U.S. today and will comprise more than 50% of the workforce by 2017," Banktech reported in February. "Millennials have grown up in a digital and always connected environment, heavily influenced by social media and instant results."

Financial firms have been eager to capitalize on that generation's appetite for mobile, and 51% of smartphone users take advantage of mobile banking, including paying bills, depositing checks and checking balances, according to Federal Reserve data. More and more of the mortgage application and approval process is moving to mobile as well.

One of the mortgage software companies seeking to develop that trend is Roostify, a web and mobile service that offers a digitized application-to-closing process. Rajesh Bhat, Roostify's CEO, disagrees that digital mortgages are more vulnerable than a traditional paper process.

"There's a certain amount of trust in traditional paper documents that they seemingly can't be tampered with," Bhat said. "But when I applied for my first mortgage, which was very paper-intensive, I wound up faxing documents and emailing them, which are both potentially hazardous ways of transferring information.

"When information can be pulled directly from the financial institution and delivered directly, you have significantly reduced the opportunity for fraud. (With Roostify) everything is encrypted in transit, the stored information is encrypted, and we're encrypting the entire loan application provided by the borrower," he said.

In fact, Bhat would argue that the automation, which allows for strict permission on which people have the ability to view the information and take action on it, makes the data safer than a paper process.

To be sure, a paper process has its own pitfalls, and almost all transactions are some combination of paper and digital already. A study published by Travelers Insurance in March found that 73% of identity fraud still occurs from offline sources, including old fashioned theft of wallets and purses.

One of the biggest threats to data can come from within organizations, from negligent or malicious employees. Employee negligence ranges from losing control of laptops or other mobile devices to using the same passwords for both home and business applications. For lenders specifically, taking shortcuts can mean the difference between secure and wide open.

"The lowest hanging fruit is still humans," said Ken Westin, a security researcher for Tripwire, in an interview

with PC World. “As long as attacks against humans still work consistently, attackers will use them on their own, or as part of sophisticated, integrated campaigns.”

Sarah Wheeler joined HousingWire in November 2013 as Content Editor, serving Housing Wire magazine and HW.com. Sarah brings extensive experience in both newspaper journalism and marketing.