gift card balances and bank accounts drained or their credit cards maxed out. Had Target reacted to the breaches immediately, its cybersecurity specialists could have trailed the malware authors. After all, the hackers had embedded user names and passwords directly into the malware code.

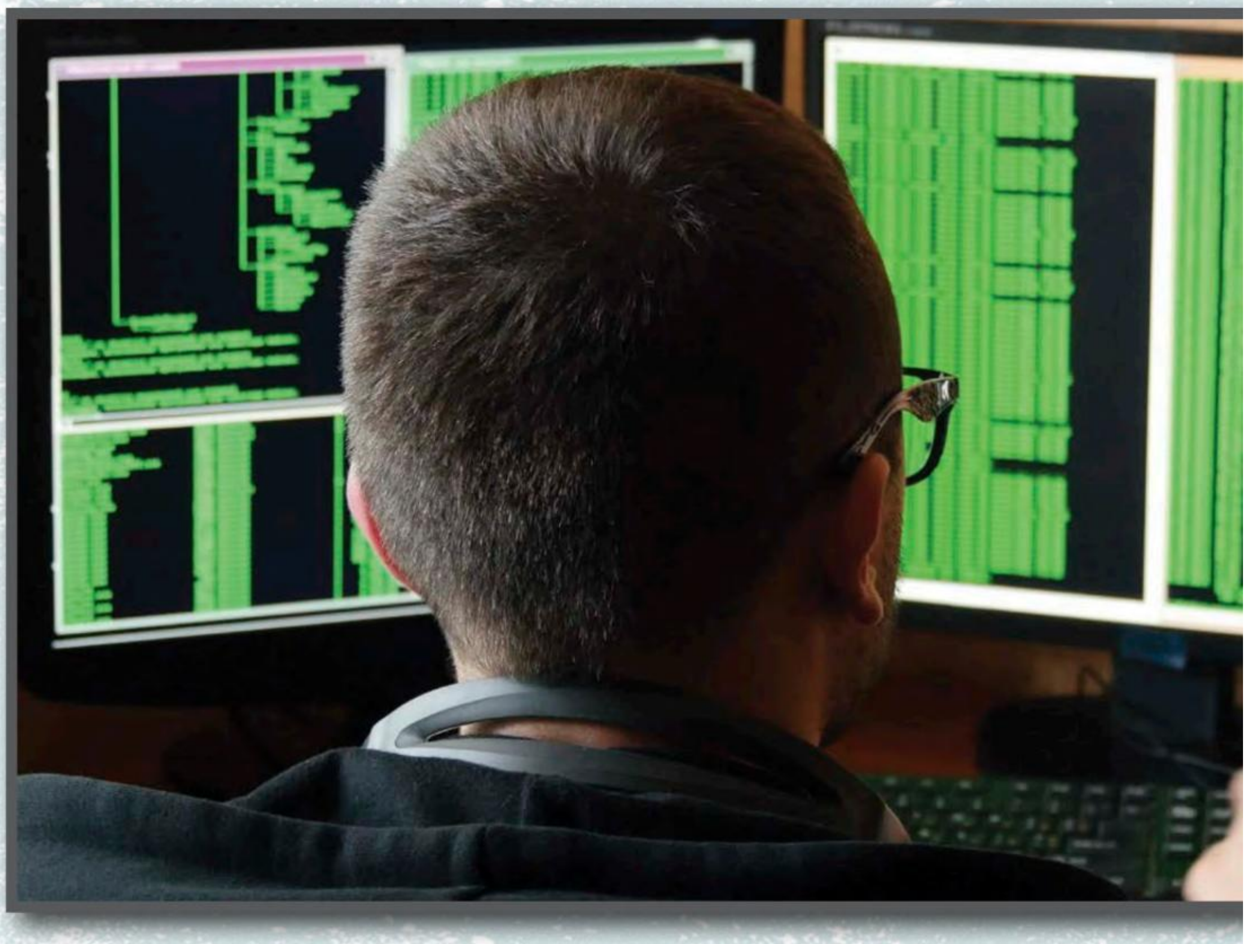
Hunting Down the Hackers

Finally, on December 12, 2013, US federal law enforcement agencies stepped in. Federal agencies had information on the stolen data and the servers—computer programs that carry out tasks for users—where the hackers were storing the stolen data.

While Target responded to customer and federal pressure to stop the theft of credit card information, the United States government's cybercrime investigators pursued the hackers who'd successfully carried out an unprecedented breach. Following a complicated web of overwhelmed proxy servers (which provide gateways between local servers and servers connected to larger networks), user names, passwords connected to video gamers, and internet protocol (IP) addresses (identifiers assigned to each computer or device), federal authorities zeroed in on Russian and Ukrainian cybercriminals they believed were responsible for all or part of the Target hacking scandal.[4] In the weeks and months to follow, other major retailers such as Home Depot and card-issuing banks such as Chase and Capitol One were hit with malware like the one that breached Target's system, indicating the malware not only worked but was shared among a network of cyber thieves.[5]

However, to date, there is no public record of the Russian and Ukrainian suspects being arrested for the massive malware attack. In early 2014, two Mexicans crossing the border into Texas were arrested when ninety fraudulent credit cards were found in their possession. Authorities believed the cards were possibly bought in connection to the card information sold by Target's hackers, but the carder—a hacker who specializes in stolen credit card information—believed to be at the center of the malware scheme seems to have fallen off the radar.[6] Andrey Hodirevski, a young Ukrainian hacker known to authorities from prior carder stings, had connections to at least one of the sites that sold the stolen credit card data. That site, rescator.cc, brazenly still operates. And though authorities have identified Rescator and other similar sites that sell stolen credit card data, some of those criminally run sites have installed their own protections, such as detecting when an undercover law enforcement agent is attempting to purchase data and infiltrate the world of the infiltrators.[7] Without definitive proof that Hodirevski is behind Rescator, and that his known or assumed associates are behind that site and others that sell credit card information, law enforcement agencies around the globe labor to pinpoint cybercriminals suspected of one of the worst security breaches in retail history. And while they labor to draw definitive lines between suspects and criminal sites, they must also continue trying to catch these underworld thieves in the act. Sites that sold credit card data used to be public, for the most part. As cybercriminals continue to learn from their mistakes, however, users of stolen credit card sites must now have log-in credentials to purchase credit card information and filter credit card data by region to escape detection. For instance, a credit or debit card belonging to a California resident

Cybercriminals devote their time not only to theft of stolen data but also to thwarting investigators trying to shut them down.



being used in New York or abroad would raise a red flag for most banks and credit card companies and even result in freezing the account while the activity is verified with the account owner. Many banks and credit card companies now ask their customers to identify authorized card users and specific dates and places a card might be used away from home in order to tailor fraud detection and prevention. By allowing customers of stolen card data to filter by region, cybercriminals undermine the systems banks and credit card companies have in place to secure customer data. Mark Lanterman obtained credentials for black-market credit card information sites after years undercover on underworld sites.

"You just hang out," Lanterman told Bloomberg in 2014. "Eventually they just think you're the same kind of scumbag they are and say, 'Yep, here's your login.'"[8]

Now that the fraudsters have installed protections against the fraud detectors, a new wave of cybercrime investigators is needed: a generation that grew up online, knows the stakes, and is ready to play the long game. Because criminals are looking for customers and cohorts with an established history of online criminal activity, crime fighters must be in for the long haul and know how to spring a trap that can ensnare a vast network of criminals who operate in the darkest corner of the underworld of crime: online.