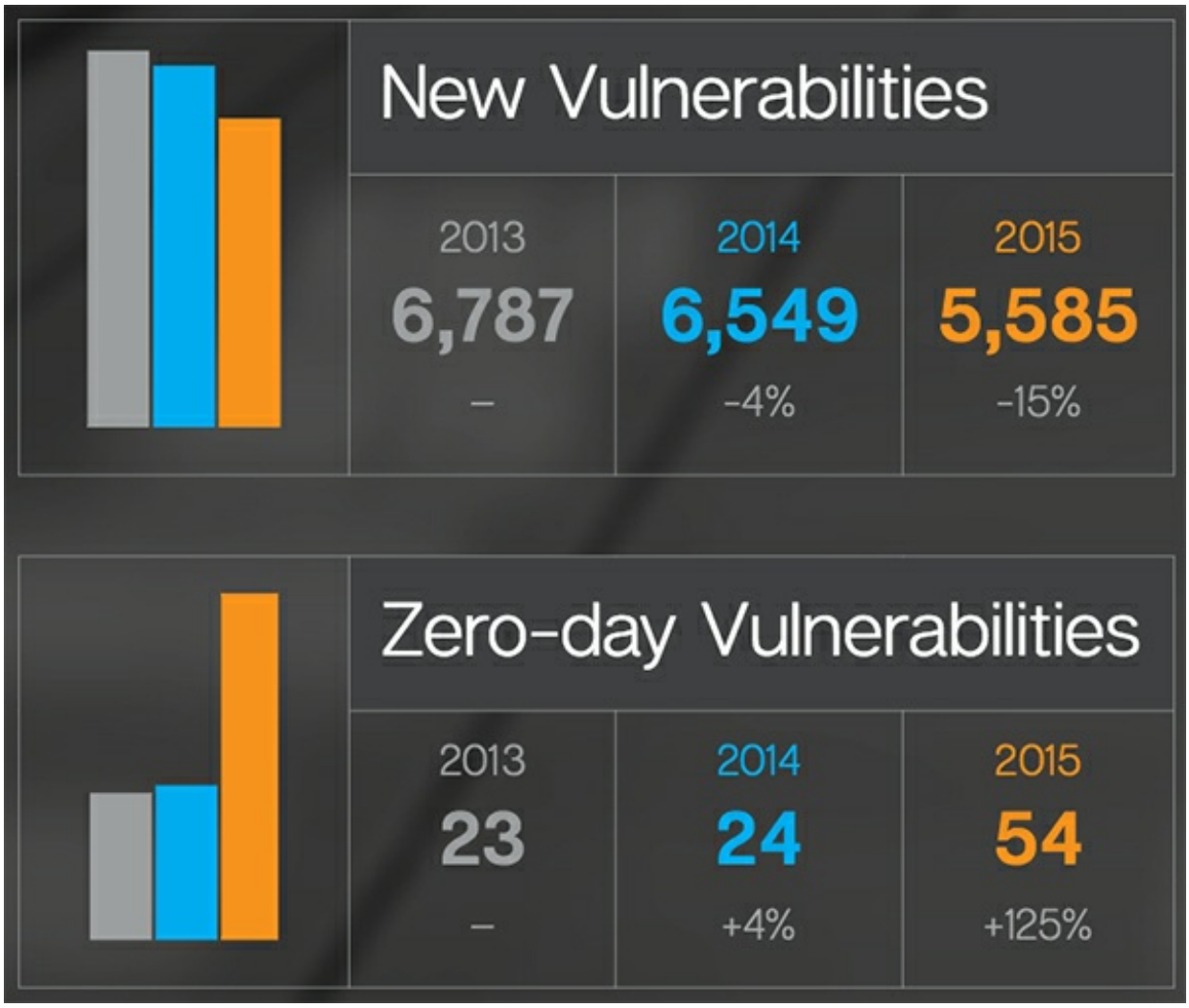
Cybercriminals are adopting corporate best practices

Help Net Security

April 12, 2016

Cybercriminals are adopting corporate best practices and establishing professional businesses in order to increase the efficiency of their attacks against enterprises and consumers. This new class of professional cybercriminal spans the entire ecosystem of attackers, extending the reach of enterprise and consumer threats and fueling the growth of online crime.

“Advanced criminal attack groups now echo the skill sets of nation-state attackers. They have extensive resources and a highly-skilled technical staff that operate with such efficiency that they maintain normal business hours and even take the weekends and holidays off,” said Kevin Haley, director, Symantec Security Response. “We are even seeing low-level criminal attackers create call center operations to increase the impact of their scams.”



Advanced professional attack groups

Advanced professional attack groups are the first to leverage zero-day vulnerabilities, using them for their own advantage or selling them to lower-level criminals on the open market where they are quickly commoditized. In 2015, the number of zero-day vulnerabilities discovered more than doubled to a record-breaking 54, a 125 percent

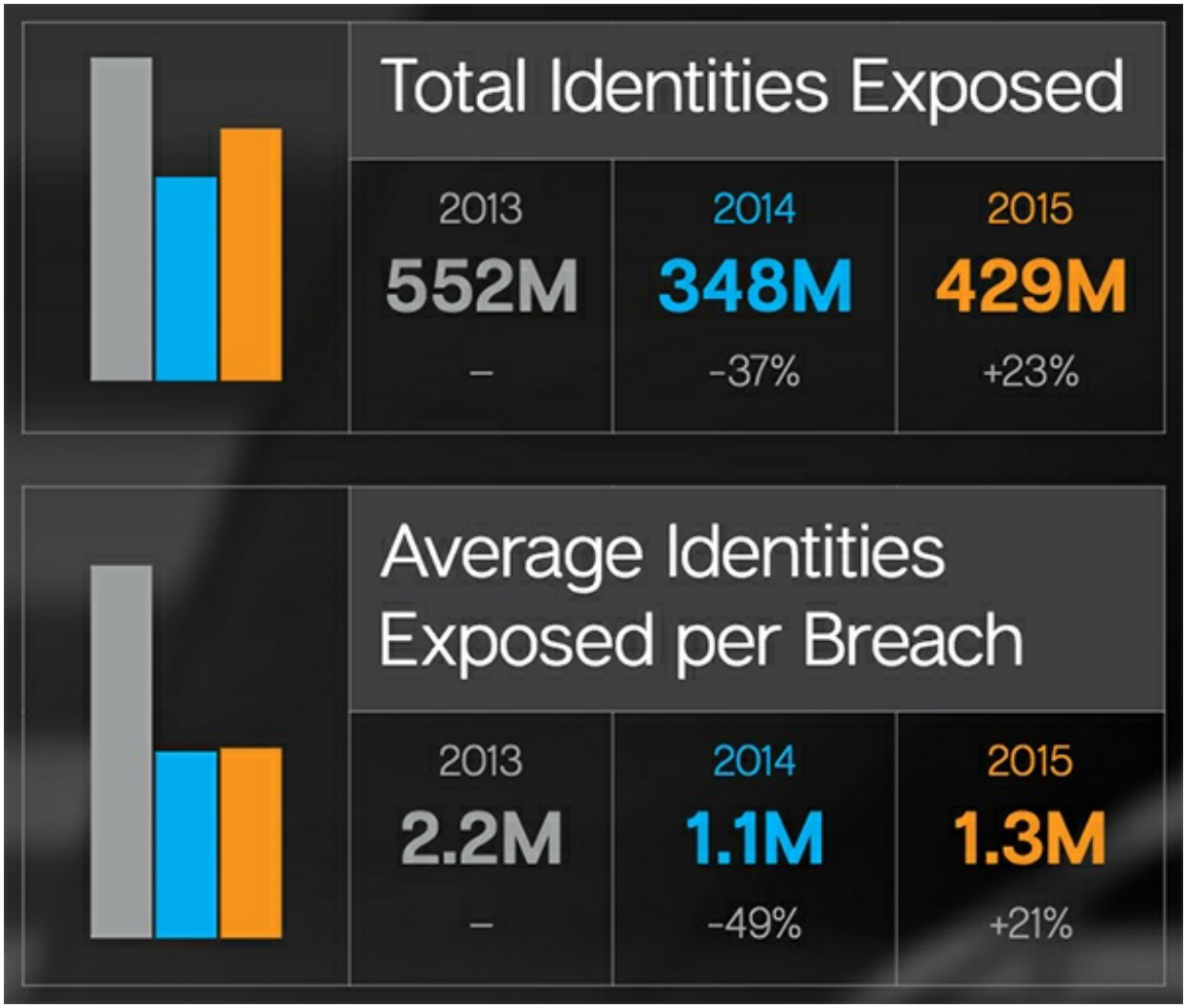
increase from the year before, reaffirming the critical role they play in lucrative targeted attacks, according to Symantec's Internet Security Threat Report.

Meanwhile, malware increased at a staggering rate with 430 million new malware variants discovered in 2015. The sheer volume of malware proves that professional cybercriminals are leveraging their vast resources in attempt to overwhelm defenses and enter corporate networks.

Over half a billion personal records stolen or lost in 2015

Data breaches continue to impact the enterprise. In fact, large businesses that are targeted for attack will on average be targeted three more times within the year. Additionally, we saw the largest data breach ever publicly reported last year with 191 million records compromised in a single incident. There were also a record-setting total of nine reported mega-breaches. While 429 million identities were exposed, the number of companies that chose not to report the number of records lost jumped by 85 percent. A conservative estimate by Symantec of those unreported breaches pushes the real number of records lost to more than half a billion.

"The increasing number of companies choosing to hold back critical details after a breach is a disturbing trend," said Haley. "Transparency is critical to security. By hiding the full impact of an attack, it becomes more difficult to assess the risk and improve your security posture to prevent future attacks."



Encryption used as a weapon to hold critical data hostage

Ransomware also continued to evolve in 2015, with the more damaging style of crypto-ransomware attacks growing

by 35 percent. This more aggressive crypto-ransomware attack encrypts all of a victim's digital content and holds it hostage until a ransom is paid. This year, ransomware spread beyond PCs to smartphones, Mac and Linux systems, with attackers increasingly seeking any network-connected device that could be held hostage for profit, indicating that the enterprise is the next target.

Scammers make you call them to hand over your cash

As people conduct more of their lives online, attackers are increasingly focused on using the intersection of the physical and digital world to their advantage. In 2015, Symantec saw a resurgence of many tried-and-true scams.

Cybercriminals revisited fake technical support scams, which saw a 200 percent increase last year. The difference now is that scammers send fake warning messages to devices like smartphones, driving users to attacker-run call centers in order to dupe them into buying useless services.

"One of the reasons that zero-day vulnerabilities are more frequent is the fact that more immature technologies like IoT emerged, and they are lacking important security features. These can be exploited, so businesses as well as consumers have to pay attention to the data those devices are collecting. Besides external attacks, companies should also consider insider threats and human error. Businesses need to have clear policies and approaches to deal with potential data leakages from inside the company," said Roman Foeckl, CEO at CoSoSys.