Bigstock

2015: Cybercrime's Epic Year

BY LIMOR KESSEM • DECEMBER 8, 2015

Categories: Advanced Threats , IBM X-Force , Threat Intelligence

This year in cybercrime was… epic! Every prediction made last year has not only materialized, but exceeded expectations. Increases in attacks, technical sophistication and higher losses than ever imagined painted a new cyber reality in the past 12 months.

Limor Kessem

What was so different in 2015? Wasn't it just more of the same? Well, not quite. As the year draws to an end, we can look back at some unprecedented cases that redefined risk and loss resulting from cyberattacks. There is a common denominator that groups them as one: The mob has fully moved into the Web. Even CSO Online has said, "There is no such thing as 'disorganized cybercrime' anymore."

Cybersecurity Evangelist, IBM

Follow @icyberfighter

Limor Kessem is one of the top cyber intelligence experts at IBM Trusteer. She is a seasoned speaker and a regular blogger on the cutting-edge IBM Security Intelligence blog. Limor...

SEE ALL POSTS

LEARN MORE ABOUT CYBERCRIME'S RELENTLESS PROGRESS IN 2015 ▶

The Year in Cybercrime

Let's look at some of the cybercrime headlines that made 2015 so unique:

- The Carbanak case was a $1 billion heist that combined the elements of an APT attack, malware-facilitated fraud, ATM malware and high street crime. What's most striking about Carbanak may be the combination of the words Carberp and Anunak (two malware gangs), which means that it was not the first time this attack was carried out. The Anunak gang actually rehearsed this attack type in 2013 and again in 2014. Since it never got caught, it orchestrated its biggest heist yet in 2015. If we do not learn enough from the billion-dollar case, we stand to see an even more brazen and extravagant attack in 2016.

- The emergence of the Dyre gang and Dyre Wolf attacks also

stuck out in 2015. Stealing big money from companies is not new, and other crime gangs have done it before, but no other gang was as methodical and bold as the Dyre group. Its criminal operators appear to have been behind the theft of $5.5 million from Irish budget airline Ryanair.

- Evil Corp's Dridex attacks escalated to multimillion-dollar heists, robbing Penneco Oil of $3.5 million in one day . After gaining deserved attention from international law enforcement, Dridex's infrastructure was scheduled for a takedown attempt . But alas, the gang was evidently ready and survived the takedown only to continue and enhance its attacks on consumers and businesses.

Nowadays, security teams are not dealing with cybercriminals, thieves or a couple of black-hats who are after their customers or assets. We are dealing with full-blown evil organizations that operate in the shadows. They create advanced threats using a mix of deep technological savvy, top-notch reconnaissance and old-fashioned street crime. This results in monetary losses so grand that they are causing a shift in the economy, siphoning cash from bank accounts in Western countries, laundering money and using it to fund other criminal operations across the globe.

Learn More

To learn more about the state of organized cybercrime and the threat landscape, join us on Thursday, Jan. 14, 2016, at 11:00 a.m. EST for "Cybercrime Reloaded – A Look Back and a Look Ahead ," a retrospective view of 2015 and predictions about what we can expect to see in 2016.

Topics: Advanced Threats , Carbanak , Cybercrime , Dridex , Dyre , Dyre Wolf , Malware , Threat Intelligence