IBM X-Force Report: Fewer Records Breached In 2017 As Cybercriminals Focused On Ransomware And Destructive Attacks

Human error responsible for two-thirds of compromised records including historic 424% jump in misconfigured cloud infrastructure

CAMBRIDGE, Mass., April 4, 2018 /PRNewswire/ -- IBM Security (NYSE:IBM) today announced results from the 2018 IBM X-Force Threat Intelligence Index which found the number of records breached dropped nearly 25 percent in 2017, as cybercriminals shifted their focus on launching ransomware and destructive attacks that lock or destruct data unless the victim pays a ransom.

Last year, more than 2.9 billion records were reported breached, down from 4 billion disclosed in 2016. While the number of records breached was still significant, ransomware reigned in 2017 as attacks such as WannaCry, NotPetya, and Bad Rabbit caused chaos across industries without contributing to the total number of compromised records reported.

Other key findings include:

- A historic 424 percent jump in breaches related to misconfigured cloud infrastructure, largely due to human error;
- For the second year in a row, the Financial Services industry suffered the most cyberattacks against it, accounting for 27 percent of attacks across all industries.

The IBM X-Force Threat Intelligence Index is comprised of insights and observations from data analyzed via hundreds of millions of protected endpoints and servers across nearly 100 countries. IBM X-Force runs thousands of spam traps around the world and monitors tens of millions of spam and phishing attacks daily while analyzing billions of web pages and images to detect fraudulent activity and brand abuse.

"While breached records are a good indication of cybercriminal activity, it doesn't tell the full story of 2017," said Wendi Whitmore, Global Lead, IBM X-Force Incident Response and Intelligence Services (IRIS). "Last year, there was a clear focus by criminals to lock or delete data, not just steal it, through ransomware attacks. These attacks are not quantified by records breached, but have proven to be just as, if not more, costly to organizations than a traditional data breach. The ability to anticipate these attacks and be prepared will be critical as cybercriminals will continue to evolve their tactics to what proves most lucrative."

Ransomware Attacks Put Pressure on Incident Response

Ransomware and destructive attacks, such as WannaCry, NotPetya, and Bad Rabbit, not only grabbed headlines in 2017, but also brought major organizations to a halt as cybercriminals took over and locked critical infrastructure in healthcare, transportation, and logistics, among others. Overall, ransomware incidents have cost organizations more than $8 billion[1] in 2017 as cybercriminals launched debilitating attacks that were focused on locking critical data instead of compromising stored records.

This trend puts increased pressure on organizations to be properly prepared with incident response strategies to limit the impact of an attack. An IBM Security study last year found that a slow response can impact the cost of an attack as incidents that took longer than 30 days to contain cost $1 million more than those contained within 30 days.

Human Error Remains a Weak Link

In 2017, cybercriminals continued to take advantage of human error and mistakes in infrastructure configurations to launch attacks. In fact, the report shows that inadvertent activity such as misconfigured cloud infrastructure was responsible for the exposure of nearly 70 percent of compromised records tracked by IBM X-Force in 2017. The report shows that there is a growing awareness among cybercriminals of the existence of misconfigured cloud servers. For example, 2017 saw an

incredible 424 percent increase in records breached through misconfigurations in cloud servers.

Beyond misconfigured cloud, individuals lured via phishing attacks represented one-third of inadvertent activity that led to a security event in 2017. This includes users clicking on a link or opening an attachment laced with malicious code, usually shared via a spam campaign launched by cybercriminals. The report found that in 2017, cybercriminals relied heavily on the Necurs botnet to distribute millions of spam messages over a span of just a few days in some instances. For example, over a two-day period in August, IBM X-Force research observed four separate Necurs campaigns spamming 22 million emails.

Cybercriminals Find Success Targeting Financial Services Customers

In years past, Financial Services has been the most targeted industry by cybercriminals. In 2017, it fell to the third-most attacked (17 percent) – behind Information & Communications Technology (33 percent) and Manufacturing (18 percent) – yet saw the most security incidents (27 percent) – those requiring further investigation – compared to other industries.

While Financial Services organizations have invested heavily in cybersecurity technologies to protect organizations, cybercriminals focused on leveraging banking Trojans specifically targeting consumers and end users across the industry.

For example, the IBM X-Force Threat Intelligence Index report found that in 2017, the Gozi banking Trojan and its variants were the most prevalently used malware against the Financial Services industry. The Gozi malware specifically targets customers as it takes over initial banking login screens with prompts for consumers to enter other personal information that is then shared directly with the attacker.

The use of Gozi, considered to be run by a skilled cybercrime operation, highlights how organized crime is overtaking all other classes of actors in the financial malware-facilitated fraud scene.

The report features data IBM collected betweenJanuary 1, 2017 and December 31, 2017, to deliver insightful information about the global threat landscape and inform security professionals about the threats most relevant to their organizations. To download a copy of the 2018 IBM X-Force Threat Index please visit: https://www.ibm.com/account/reg/us-en/signup?formid=urx-31271

Sign up for the IBM X-Force Threat Index webinar onThursday, April 5 at 11am EDT https://bit.ly/2E2KYSb

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and has been granted more than 8,000 security patents worldwide. For more information, please check www.ibm.com/security, follow IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Media Contact

Kelly Kane
IBM Security Media Relations
+1-413-297-2668
kkane@us.ibm.com

[1]Cyence/Reinsurance News, Re/insurance to take minimal share of$8 billion WannaCry economic loss:AM Best, May 2017

SOURCE IBM