17 NOV 2015 NEWS

IBM: Ransomware, Insider Threats Top 2015 Cyber-Trends

Tara Seals US/North America News Reporter, Infosecurity Magazine
Email Tara

2015 has been a challenging year as insider threats and malware as well as stealthy and evolving attacks affected enterprises. Taking stock, IBM Security has identified the top four cyber-threat trends of the year: amateur hacker carelessness, ransomware, insider threats and C-suite attention.

The first notable trend is amateur hackers exposing sophisticated criminals in onion-layered attacks. While 80% of cyberattacks are driven by highly organized and sophisticated online crime rings, it is often inexperienced hackers ("script kiddies") who unknowingly alert companies to these larger, sophisticated hackers lurking on a network or inside an organization. These amateur hackers leave clues like unusual folders or files in a temporary directory, deface corporate web materials, and more. When organizations look into these mischievous attacks, they often find much more complex attacks.

"As the name suggests, an onion-layered security incident is one in which a second, often significantly more damaging attack is uncovered during the investigation of another more visible event," the firm said in its Q4 2015 IBM X-Force Threat Intelligence Quarterly report. "The security team has to carefully peel back layers of forensic information in order to determine the root cause of each event under scrutiny."

Also, it's almost undeniable that 2015 was the year of ransomware, with this type of infection ranking as the most commonly encountered infection. In fact, the FBI reported Cryptowall ransomware attacks have netted hackers more than $18 million from 2014-2015. IBM researchers believe that it will remain a common threat and profitable business into 2016, migrating to mobile devices as well.

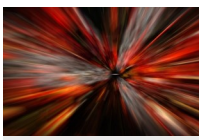
"For ransomware to succeed, attackers rely on a multitude of security and procedural breakdowns. In some cases, clients had recurring infections during the year," IBM said. "This was because, although some of the factors leading to infection were addressed and resolved, nothing was done to resolve the fundamental breakdowns that facilitated the initial infection."

Those breakdowns include not backing up data, poor patching procedures and a lack of user awareness.

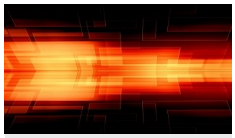
The report also noted the ongoing danger of malicious attacks from inside a company. This is

Why Not Watch?

27 AUG 2015
Ransomware: How to Avoid Extortion



30 JUL 2015
Addressing the Security Risks of Negligent Insiders



9 JUL 2015

3 SEP 2015

a continuation of a trend seen in 2014 when IBM's 2015 Cyber Security Intelligence Index revealed that 55% of all attacks in 2014 were carried out by insiders, individuals with insider access to an organization's system, knowingly or by accident.

A series of patterns emerged from the ERS team's investigations:

• There were shared accounts with administrative privileges.

• Password sharing between team members was not discouraged.

• Passwords were routinely set to never expire.

• Passwords were "easy."

The common thread is that accountability was not enforced.

"Bad password policies seriously compromised the efficacy of termination procedures," IBM said. "Whenever a system or network administrator left the organization, disabling their personal accounts did not limit their ability to perform unauthorized activity on the network via one or more of the shared accounts they had routinely used in their job. As a result, ex-employees with ill will toward former employers held powerful weapons they could use to express their resentment. They simply needed a way to get back into the network."

And, the final trend could be entitled, "C-Suite Cares." In 2015, cybersecurity became a true concern at the boardroom level with more positions of power asking questions about their organizations' security posture. In fact, a recent survey of CISOs by SMU and IBM, revealed that 85% of CISOs said upper-level management support has been increasing, and 88% said their security budgets have increased.

"Organizations today are going back to the basics. The major cybersecurity trends of 2015—the challenge of recognizing stealth attackers on the network, ransomware, malicious insider attacks and growing management attention to enterprise security readiness—can largely be addressed by focusing on security 101," IBM said. "Think patch management, user education, proper password procedures and standard security practices."

Photo © asylum

How Outsiders Become Insiders: Understanding and Combating Today's Threats

Secure Tomorrow Today – (ISC)2 Congress EMEA 2015, An Insider's Look

Related to This Story

Bugat Malware Adds GameOver Functionality

Critroni/Onion Is Most Sophisticated Ransomwar Yet

Tales of the Cyber Underground: Inside the Underground Ransomware Market

Experts Discover File-Encrypting Android Ransomware

Kovter Adult Website Ransomware Doubles

What's Hot on Infosecurity Magazine?

Read | Shared | Watched | Editor's Choice

1 20 NOV 2015 NEWS
Cyber Crooks Use Terror Attack Fea to Go Spear Phishing

2 20 NOV 2015 NEWS
Q3 Sees 21 Million New Malware Samples

3 20 NOV 2015 NEWS
One Size Does Not Fit All in Security Threat Response

4 30 JAN 2015 NEWS
Adult Site Xhamster Hit by 'Huge' Malvertising Attack

5 19 NOV 2015 NEWS
Fraud Concerns Keep US Shoppers Away from Mobile Payments

6 19 NOV 2015 NEWS
Insider Breaches: 40% of Firms Thir They'll be Hit