



Home » Cyber Crime » IBM: Ransomware, Insider Threats Top 2015 Cyber-Trends

IBM: Ransomware, Insider Threats Top 2015 Cyber-Trends

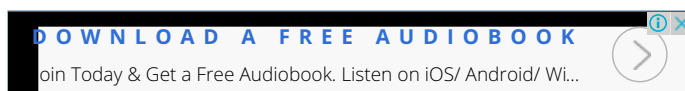
Posted on November 20, 2015 by Wire_Services in Cyber Crime, Cyber Fraud, Hackers In The News, Hacking, Wired Service // 0 Comments



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

Search

To search, type and hit enter

Follow This Story On Your Social Media



Recent Stories



Cybercrime: How it affects you

March 9, 2015 // 0 Comments

Cybercrime is the fastest growing and most dynamic area of crime. Ever-increasing reliance on cyber technology is allowing criminals to operate with virtual impunity across a [Read More..]



Protected: Public arrests of 56

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 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

Join the mailing list

email address

Submit

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."

Source: <http://www.infosecurity-magazine.com/news/ransomware-insider-threats-2015/>

Share this:



Related

Social Media, Mobile Phones Top Attack Targets
September 25, 2013
In "Cell Phone Security"

Who is Threatening the Security of Your Network?
April 25, 2012
In "Spyware/ Cyber Snooping"

Dark corners of digital world: Virtual extortion, identity theft, online bullying
October 29, 2013
In "Cyber Bully"

Leave a comment

You must be logged in to post a comment.

hackers sends a clear message – but will the hackers listen?

March 9, 2015 // 0 Comments

There is no excerpt because this is a protected [Read More..]



Protected: License plate readers let police keep tabs on more drivers

March 9, 2015 // 0 Comments

There is no excerpt because this is a protected [Read More..]



Protected: Singularity 1on 1: Marc Goodman on Future Crimes

March 9, 2015 // 0 Comments

There is no excerpt because this is a protected [Read More..]



Protected: Policy needed to protect citizens against cyber crime: RBI ED

March 9, 2015 // 0 Comments

There is no excerpt because this is a protected [Read More..]



Protected: Five arrested in nationwide cyber crime swoop led by 'Britain's FBI'

March 9, 2015 // 0 Comments

There is no excerpt because this is a protected [Read More..]



Protected: BOB HEISSE: Regional Crime Report offerings are expanding

March 9, 2015 // 0 Comments

There is no excerpt because this is a protected [Read More..]



Protected: LAPD uses its helicopters to stop crimes before they start

March 9, 2015 // 0 Comments

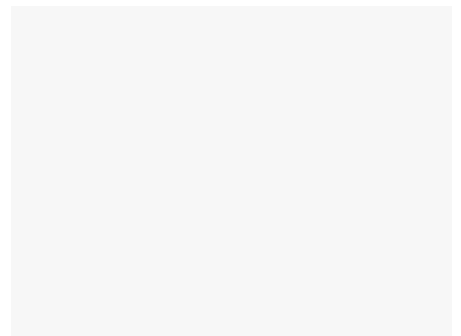
There is no excerpt because this is a protected [Read More..]



Protected: Dynamic 'CSI:CYBER' shifts paradigms and makes crime-fighting cool again

March 9, 2015 // 0 Comments

There is no excerpt because this is a protected [Read More..]



Website/IP enterasys.com may be hackable, #hackerproof

November 20, 2015 // 0 Comments

Personal Notes: No Personal Notes Industry: Technology Vulnerabilities: 4 Scan Date/Time: 2015-11-20 15:27:08 Scan: You can go to <http://www.AmlHackerProof.com/Results> and do [Read More..]



GQ publisher in contempt of court with phone-hacking article

November 20, 2015 // 0 Comments

The publisher of GQ magazine has been found guilty of contempt of court over a "very seriously prejudicial" article about the phone-hacking trial of Rebekah Brooks and [Read More..]



Which nation is the most prolific hacker?

November 20, 2015 // 0 Comments

State sponsored hacking is, truth be told, something of a mixed bag of motives, capability and success. It can be quite difficult, even for government agency and IT security [Read More..]



IBM: Ransomware, Insider Threats Top 2015 Cyber-Trends

November 20, 2015 // 0 Comments

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 [Read More..]



Warning to holiday cyber shoppers: don't get hacked

November 20, 2015 // 0 Comments





The email that showed up on my desktop at work seemed to be what it said from the PayPal Team—"Security Measures" confirming my user account, and all I had to do to [Read More..]

Listen To National Cyber Security Radio

Check Out Technology Podcasts at Blog Talk F
nationalcybersecurity on BlogTalkRad



Spy On Anyone You Like


Streetwise 500,000* Stun Gun \$34.95

LMCDSignalPro: Lawmate Signal Wireless Detector \$495.00
 HCClockToon: Small Desk Clock
HCClockToon: Small Desk Clock \$155.00
 2GB MiniSD
2GB MiniSD \$10.00



JOLT 20,000,000* Mini Stun Gun PINK
\$25.95

Tips: Auction Fraud

Before you bid, contact the seller with any questions you have. Review the seller's feedback. Be cautious when dealing with individuals outside of your own country. Ensure you understand refund, return, and warranty policies. Determine the shipping charges before you buy. Be wary if the seller only accepts wire transfers or cash. If an escrow service is used, ensure it is legitimate. Consider insuring your item. Be cautious of unsolicited offers. Source: IC3.gov

Internet Extortion

Security needs to be multi-layered so that numerous obstacles will be in the way of the intruder. Ensure security is installed at every possible entry point. Identify all machines connected to the Internet and assess the defense that's engaged. Identify whether your servers are utilizing any ports that have been known to represent insecurities. Ensure you are utilizing the most up-to-date patches for your software.

Tips: Third Party Receiver of Funds

Do not agree to accept and wire payments for auctions that you did not post. Be leery if the individual states that his country makes receiving these type of funds difficult. Be cautious when the job posting claims "no experience necessary". Be cautious when dealing with individuals outside of your own country.

Tips: Credit Card Fraud

Ensure a site is secure and reputable before providing your credit card number online. Don't trust a site just because it claims to be secure. If purchasing merchandise, ensure it is from a reputable source. Promptly reconcile credit card statements to avoid unauthorized charges. Do your research to ensure legitimacy of the individual or company. Beware of providing credit card information when requested through unsolicited emails. Source: IC3.gov

Tips: Nigerian Letter or "419"

Nigerian Letter or "419"
If the "opportunity" appears too good to be true, it probably is. Do not reply to emails asking for personal banking information. Be wary of individuals representing themselves as foreign government officials. Be cautious when dealing with individuals outside of your own country. Beware when asked to assist in placing large sums of money in overseas bank accounts. Do not believe the promise of large sums of money for your cooperation. Guard your account information carefully. Be cautious when additional fees are requested to further the transaction. Source: IC3.gov

Phishing/Spoofing

Be suspicious of any unsolicited email requesting personal information. Avoid filling out forms in email messages that ask for personal information. Always compare the link in the email to the link that you are actually directed to. Log on to the official website, instead of "linking" to it from an unsolicited email. Contact the actual business that supposedly sent the email to verify if the email is genuine.