Announcements

IBM X-Force: Stolen Credentials and Vulnerabilities Weaponized Against Businesses in 2019

Consumer Tech Brands Caught in Crossfire of Phishing Attacks; Misconfigurations Accounted for Over 85% of Exposed Records; Banking Trojans and Ransomware Form Strong Bond

CAMBRIDGE, Mass., Feb. 11, 2020 /PRNewswire/ -- IBM (NYSE: IBM) Security today released the IBM X-Force Threat Intelligence Index 2020, highlighting how cybercriminals' techniques have evolved after decades of access to tens of billions of corporate and personal records and hundreds of thousands of software flaws. According to the report, 60% of initial entries into victims' networks that were observed leveraged either previously stolen credentials or known software vulnerabilities, allowing attackers to rely less on deception to gain access.

IBM's X-Force Threat Intelligence Index highlights contributing factors to this evolution, including the top three initial attack vectors:

- Phishing was a successful initial infection vector in less than one-third of incidents (31%) observed, compared to half in 2018.
- Scanning and exploitation of vulnerabilities resulted in 30% of observed incidents, compared to just 8% in 2018. In fact, older, known vulnerabilities in Microsoft Office and Windows Server Message Block were still finding high rates of exploitation in 2019.
- The use of previously stolen credentials is also gaining ground as a preferred point-of-entry 29% of the time in observed incidents. Just in 2019, the report states more than 8.5 billion records were compromised — resulting in a 200% increase in exposed data reported year over year, adding to the growing number of stolen credentials that cybercriminals can use as their source material.

"The amount of exposed records that we're seeing today means that cybercriminals are getting their hands on more keys to our homes and businesses. Attackers won't need to invest time to devise sophisticated ways into a business; they can deploy their attacks simply by using known entities, such as logging in with stolen credentials," said Wendi Whitmore, Vice President, IBM X-Force Threat Intelligence. "Protection measures, such as multi-factor authentication and single sign-on, are important for the cyber resilience of organizations and the protection and privacy of user data."

IBM X-Force conducted its analysis based on insights and observations from monitoring 70 billion security events per day in more than 130 countries. In addition, data is gathered and analyzed from multiple sources including X-Force IRIS, X-Force Red, IBM Managed Security Services, and publicly disclosed data breach information. IBM X-Force also 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.

Some of the report's key highlights include:

- **Configure it Out** —IBM's analysis found that of the more than 8.5 billion breached records reported in 2019, seven billion of those, or over 85%, were due to misconfigured cloud servers and other improperly configured systems — a stark departure from 2018 when these records made up less than half of total records.
- **Banking on Ransomware** — Some of the most active banking trojans found in this year's report, such as

TrickBot, were increasingly observed to set the stage for full-on ransomware attacks. In fact, novel code used by banking trojans and ransomware topped the charts compared to other malware variants discussed in the report.

- **Tech Trust Takeover for Phishing** — The IBM X-Force report found that tech, social media and content streaming household brands make up the "Top 10" spoofed brands that cyber attackers are impersonating in phishing attempts. This shift could demonstrate the increasing trust put in technology providers over historically trusted retail and financial brands. Top brands used in squatting schemes include Google, YouTube and Apple.

Ransomware Attacks Evolve

The report revealed trends in ransomware attacks worldwide, targeting both the public and private sectors. The report shows an uptick in ransomware activity in 2019 with IBM X-Force deploying its incident response team to ransomware incidents in 13 different industries worldwide, reaffirming that these attacks are industry agnostic.

While over 100 U.S. government entities were impacted by ransomware attacks last year, IBM X-Force also saw significant attacks against retail, manufacturing and transportation —which are known to either hold a surplus of monetizable data or rely on outdated technology and, thus, face the vulnerability sprawl. In fact, in 80% of observed ransomware attempts, attackers were exploiting Windows Server Message Block vulnerabilities, the same tactic used to propagate WannaCry, an attack that crippled businesses across 150 countries in 2017.

With ransomware attacks costing organizations over $7.5 billion in 2019, adversaries are reaping the rewards and have no incentive to slow down in 2020. In collaboration with Intezer, IBM's report states that new malware code was observed in 45% of banking trojans and 36% of ransomware. This suggests that by creating new code attackers are continuing to invest in efforts to avoid detection.

Concurrently, IBM X-Force observed a strong relationship between ransomware and banking trojans with the latter being used to open the door for targeted, high-stakes ransomware attacks, diversifying how ransomware is being deployed. For example, the most active financial malware according to the report, TrickBot, is suspected of deploying Ryuk on enterprise networks, while various other banking trojans, such as QakBot, GootKit and Dridex are also diversifying to ransomware variants.

Adversaries Spoof Tech and Social Media Companies in Phishing Schemes

As consumers become more aware of phishing emails, phishing tactics themselves are becoming more targeted. In collaboration with Quad9, IBM observed a squatting trend in phishing campaigns, wherein attackers are impersonating consumer tech brands with tempting links – using tech, social media and content streaming companies to trick users into clicking malicious links in phishing attempts.

Nearly 60% of the top 10 spoofed brands identified were Google and YouTube domains, while Apple (15%) and Amazon (12%) domains were also spoofed by attackers looking to steal users' monetizable data. IBM X-Force assesses that these brands were targeted primarily due to the monetizable data they hold.

Facebook, Instagram and Netflix also made the list of top 10 spoofed brands observed but at a significantly lower use rate. This may be due to the fact that these services don't typically hold directly monetizable data. As attackers often bet on credential reuse to gain access to accounts with more lucrative payouts, IBM X-Force suggests that frequent password reuse may be what potentially made these brands targets. In fact, IBM's Future of Identity Study found that 41% of millennials surveyed reuse the same password multiple times and Generation Z averages use of only five passwords, indicating a heavier reuse rate.

Discerning spoofed domains can be extremely difficult, which is exactly what attackers bet on. With nearly 10

billion accounts combined[1], the top 10 spoofed brands listed in the report offer attackers a wide target pool, increasing the likelihood that an unsuspecting user clicks an innocent-seeming link from a spoofed brand.

Additional key findings in the report include:

- **Retail Rebounds in Targeted Industry Rankings:** Retail has jumped to the second most attacked industry in this year's report, in a very close race with financial services which remained at the top for the fourth year in a row. Magecart attacks are among the most prominent attacks observed against retail, impacting a reported 80 e-commerce sites in the summer of 2019. Cybercriminals seem to have set their sights on consumers' PII, payment card data and even valuable loyalty program information. Retailers also experienced a large amount of ransomware attacks based on insights from IBM's incident response engagements.
- **Industrial Control Systems (ICS) and Operational Technology (OT) Attacks Soar:** In 2019, OT targeting increased 2000% year over year with more attacks on ICS and OT infrastructure than any of the prior three years. Most observed attacks involved a combination of known vulnerabilities within SCADA and ICS hardware as well as password-spraying.
- **North America and Asia — Most Targeted Regions:** These regions experienced the highest number of observed attacks as well as suffered the largest reported data losses over the past year, over 5 billion and 2 billion records exposed respectively.

The report features data IBM collected in 2019 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 IBM X-Force Threat Intelligence Index 2020, please visit: https://ibm.biz/downloadxforcethreatindex

Sign up for the IBM X-Force Threat Intelligence Index 2020 webinar on **Tuesday, February 18, 2020 at 11:00 a.m. ET**: https://ibm.biz/BdqExS

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 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Press Contact:
IBM Security Media Relations
Georgia Prassinos
gprassinos@ibm.com
(571) 365-6065

[1] Based on an IBM analysis of publicly available information

SOURCE IBM