IBM X-Force Report: Ransomware Doesn't Pay in 2018 as Cybercriminals Turn to Cryptojacking for Profit

Report also finds more than half of cybercriminal attacks pivot away from malware-based attacks; targeted business email compromise campaigns on the rise

CAMBRIDGE, Mass., Feb. 26, 2019 /PRNewswire/ -- IBM (NYSE: IBM) Security today announced results from the annual 2019 IBM X-Force Threat Intelligence Index, which found that increased security measures and awareness are driving cybercriminals to alter their techniques in search of a better return on investment (ROI). As a result, the report details two major shifts, including decreased reliance on malware and a decline in ransomware, as criminals increased their use of other cybercrime techniques with the potential for greater ROI.

IBM X-Force also observed that the number of cryptojacking attacks – the illegal use of an organization's or individual's computing power without their knowledge to mine cryptocurrencies – were nearly double those of ransomware attacks in 2018. With the price of cryptocurrencies like Bitcoin hitting a high of nearly $20,000 going into 2018, lower-risk/lower-effort attacks secretly using a victim's computing power were on the rise. In fact, IBM spam researchers only tracked one ransomware campaign in 2018 from one of the world's largest malware spam distribution botnet, Necurs.

The IBM X-Force Threat Intelligence Index also found that cybercriminals were changing their stealth techniques to gain illegal profits. IBM X-Force saw an increase in the abuse of administrative tools, instead of the use of malware. More than half of cyberattacks (57 percent) leveraged common administration applications like PowerShell and PsExec to evade detection, while targeted phishing attacks accounted for nearly one third (29 percent) of attacks.

"If we look at the drop in the use of malware, the shift away from ransomware, and the rise of targeted campaigns, all these trends tell us that return-on-investment is a real motivating factor for cybercriminals. We see that efforts to disrupt adversaries and make systems harder to infiltrate are working. While 11.7 billion records were leaked or stolen over the last three years, leveraging stolen Personally Identifiable Information (PII) for profit requires more knowledge and resources, motivating attackers to explore new illicit profit models to increase their return on investment," said Wendi Whitmore, Global Lead, IBM X-Force Incident Response and Intelligence Services (IRIS). "One of the hottest commodities is computing power tied to the emergence of cryptocurrencies. This has led to corporate networks and consumer devices being secretly highjacked to mine for these digital currencies."

IBM X-Force Threat Intelligence Index comprises 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.

Additional findings include:

- **BEC Continues to Pay the Bills:** Phishing campaigns made heavy use of targeted Business Email Compromise (BEC) scams, which accounted for 45 percent of the phishing attacks tracked by X-Force.
- **Transportation Emerges as Industry to Watch (for Cyberattacks):** The transportation industry became the second-most attacked sector in 2018 – moving up the ranks from 10th in 2017.

- **Vulnerability Reporting on the Rise:** Nearly one third (42,000) of all 140,000 vulnerabilities tracked by IBM X-Force, were reported in just the past three years. In fact, IBM X-Force Red finds an average 1,440 unique vulnerabilities, per organization.
- **Misconfigurations Still Plague Organizations:** Publicly disclosed misconfiguration incidents increased 20 percent year-over-year. Interestingly, there was a 52 percent decrease in the number of records compromised due to this threat vector.

Cybercriminals Hack Systems to Make Money on Business' Dime

Cybercriminals have developed tools and tactics to infect both corporate servers and individual users with coin-mining malware to mine cryptocurrencies. In turn, these infections hijack computing power, resulting in increased CPU usage and slowed devices. This cryptojacking trend is virtually exploding, and cybercriminals have the advantage as the two of the most common infection vectors are phishing and injecting code into websites with weak security controls.

IBM X-Force has discovered that illicit cryptojacking attacks are on the rise while ransomware seems to be on the decline. Over the course of 2018, attempts to install ransomware on X-Force monitored devices in Q4 (Oct.-Dec.) declined to less than half (45 percent) of the attempts in Q1. Instead, cryptojacking attacks more than quadrupled in the same timeframe by 450 percent.

The Rise of Criminal PowerShell Power Users

Increasing awareness of cybersecurity issues and stricter security controls are making it harder for cybercriminals to establish footholds on target systems. As a result, the use of malicious software in attacks appears to be on the decline. More than half (57 percent) of attacks analyzed by X-Force in 2018, did not leverage malware and many involved the use of non-malicious tools including PowerShell and PsExec to evade detection. Those who made the most frequent use of malware were major cybercriminal gangs and advanced persistent threat (APT) groups.

In cases where networks were compromised by attackers, IBM X-Force saw a shift to cybercriminals abusing administrative tools, instead of malware, to achieve their goals. Core to these techniques is the advanced use of PowerShell, a tool capable of executing code from memory and providing administrative access directly to a device's core. IBM X-Force IRIS has also observed attackers running Windows Management Interface Command (WMIC) queries, which are then used to automate the remote execution of PowerShell commands and scripts, among other functions designed to run queries, search databases, access user directories, and connect to systems of interest.

Transportation Industry an Increasing Cybercrime Target

Cybercriminals aren't just changing how they hack, but also who they target. The Financial Services industry remained the most attacked sector of 2018 accounting for 19 percent of all attacks observed by IBM X-Force IRIS. However, the Transportation Industry—which did not even make the top 5 list last year—moved to the second most attacked sector in 2018, with attempted attacks increasing three-fold since the year prior.

It is not just a matter of the sheer volume of attacks, but also in the caliber of victims. X-Force saw more public disclosures in 2018 than in previous years in the transportation industry. These disclosures likely encouraged hackers as they may reveal that these companies are vulnerable to cyberattacks and that they hold valuable data such as customer data, payment card information, PII, and loyalty reward accounts.

Recommendations and Remediations

The X-Force Threat Intelligence Index report offers recommendations for organizations to increase preparedness through preventive measures such as threat hunting — proactively searching networks and endpoints for advanced threats that evade prevention and detection tools. Additionally, risk management models need to

consider likely threat actors, infection methods and potential impact to critical business processes. Organizations also need to be aware of risks arising from third parties, such as cloud services, suppliers and acquisitions.

The report also emphasizes remediation and incident response. Even organizations with a mature security posture may not know how to respond to a security incident. Effective incident response is not only a technical matter; leadership and crisis communications are key to rapid response and quickly resuming business operations.

The report features data IBM collected between January 1, 2018 and December 31, 2018, 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 2019 IBM X-Force Threat Index please visit: https://www.ibm.com/security/data-breach/threat-intelligence.

View the IBM X-Force Threat Intelligence Index interactive infographic at: https://xforceintelligenceindex.mybluemix.net/ and sign up for the 2019 IBM X-Force Threat Intelligence Index webinar on Friday, March 29, 2019 at 10:00 AM ET https://ibm.biz/Bd2VcT

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.

Media Contact:

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

SOURCE IBM