X-Force Threat Intelligence Index 2024

Executive Summary



IBM

Table of contents

03 Executive summary

05 Report highlights

07 Recommendations

09 About us

Executive summary

The biggest shift the IBM® X-Force® team observed in 2023 was a pronounced surge in cyberthreats targeting identities. Attackers have a historical inclination to choose the path of least resistance in pursuit of their objectives. In this era, the focus has shifted towards *logging in* rather than *hacking in*, highlighting the relative ease of acquiring credentials compared to exploiting vulnerabilities or executing phishing campaigns. Lack of identity protections was corroborated by IBM X-Force penetration testing data for 2023, which ranked *identification and authentication failures* as the second most common finding.

Additionally, X-Force observed a 100% increase in "Kerberoasting" during incident response engagements. Kerberoasting is a technique focused on compromising Microsoft Windows Active Directory credentials through Kerberos tickets. This indicates a technique shift in how attackers are acquiring identities to carry out their operations.

The prominence of *valid accounts* as a preferred initial access technique among cybercriminals—tying with phishing for the first time—was another notable development. This access technique is accompanied by an upsurge in malware designed to steal information, known as infostealer malware, activities that bolster the dark web's stolen credentials marketplace. This multifaceted shift underscores the symbiotic relationship among various elements in the cybercrime ecosystem.

It's clear that attackers have recognized the difficulty defenders have in distinguishing between legitimate user identity use and unauthorized misuse. This escalation in targeting of identities in cyberattacks underscores the critical importance for organizations to proactively identify, eliminate and audit potential attack vectors within their dynamic networks. These measures are pivotal in reducing the attack surface, unveiling latent risks and autonomously remediating incidents that are independent of impending threats.

Last year will also go down in history as a generative artificial intelligence (gen AI) breakout year. Policy makers, business executives and cybersecurity professionals are all feeling the pressure to adopt AI within their operations. And the rush to adopt gen AI is currently outpacing the industry's ability to understand the security risks these new capabilities will introduce. However, a universal AI attack surface will materialize once adoption of AI reaches a critical mass, forcing organizations to prioritize security defenses that can adapt to AI threats at scale.

In an attempt to identify key milestones that will indicate when a common AI threat landscape will mature, X-Force assessed previous technology disrupters and their threat maturity milestones. Based on the analysis, X-Force predicts threat actors will begin to target AI broadly once the market coalesces around common deployment models and a small number of vendors. This analysis suggests that AI market dominance is the milestone that will trigger attacker investment in attack toolkits targeting AI.

Despite looming gen AI-enabled threats, X-Force hasn't observed any concrete evidence of generative AI-engineered cyberattacks to date or a rapid shift in attackers' goals and objectives from previous years. Although X-Force observed a notable drop in ransomware attacks on enterprises in 2023, extortion-based attacks continue to be a driving force of cybercrime this past year. These extortion-based attacks were only surpassed by *data theft and leak* as the most common impact observed in X-Force incident response engagements globally.

The IBM X-Force Threat Intelligence Index offers these insights as a resource to IBM clients, researchers in the security industry, policy makers, the media and the broader community of security professionals and business leaders. It's our intent to keep all parties informed of the current threat landscape so they can make the best decisions for reducing risk.

Report highlights

71%

Increase year over year in volume of attacks using valid credentials
For the first time ever, abusing valid accounts became cybercriminals' most common entry point into victim environments. It represented 30% of all incidents X-Force responded to in 2023.

32%

Percentage of data theft and leak incidents
Data theft and leak rose to the most common impact for organizations, indicating more groups are favoring this method to obtain financial gains.

11.5%

Drop in enterprise ransomware incidents
Despite remaining the most common action on objective (20%), X-Force observed a drop in enterprise ransomware incidents. This drop is likely to impact adversaries' revenue expectations from encryption-based extortion as larger organizations are stopping attacks before ransomware is deployed and opting against paying and decrypting in favor of rebuilding if ransomware takes hold.

266%

Upsurge in use of infostealers
X-Force has observed threat groups who have previously specialized in ransomware showing increasing interest in infostealers. And a number of prominent new infostealers recently debuted and demonstrated increased activity in 2023, such as Rhadamanthys, LummaC2 and StrelaStealer.

30%

Share of security misconfigurations among web application vulnerabilities identified
X-Force penetration testing engagements revealed that the most observed web application risk across client environments globally was security misconfigurations. Of these misconfigurations, the top offenses included allowing concurrent user sessions in the application, which could weaken multifactor authentication (MFA) through session hijacking.

84%

Percentage of critical infrastructure incidents where initial access vector could have been mitigated
For a majority of incidents on critical infrastructure that X-Force responded to, the initial access vector could have been mitigated with best practices and security fundamentals, such as asset and patch management, credential hardening and the principle of least privilege.

32%

Percentage of incidents that involved malicious use of legitimate tools
Nearly one-third of incidents that X-Force responded to were cases where legitimate tools were used for malicious purposes, such as credential theft, reconnaissance, remote access or data exfiltration.

25.7%

Share of manufacturing attack incidents within the top 10 attacked industries
Manufacturing was once again the top attacked industry in 2023 for the third year in a row, representing 25.7% of incidents within the top 10 industries. Malware was the top action on objective observed at 45%. Ransomware accounted for 17% of incidents.

50%

Market share threshold likely to trigger attacks against AI platforms
X-Force analysis indicates that the establishment of AI market dominance will signal AI attack surface maturity. This analysis suggests that once a single AI technology approaches 50% market share, or when the market consolidates to three or less technologies, the cybercriminal ecosystem will be incentivized to invest in developing tools and attack paths targeting AI technologies.

31%

Increase in attacks year over year in Europe
Europe also experienced the highest percentage of incidents (32%) out of the five geographic regions. Malware was the most observed action on objective accounting for 44% of incidents.

Recommendations

In 2023, the combination of a rise in infostealers and the abuse of valid account credentials to gain initial access has exacerbated defenders' identity and access management challenges. The threat landscape's newly found focus on identities highlights organizations' risks that exist on devices outside of their visibility. Enterprise credential data can be stolen from compromised devices through credential reuse, browser credential stores or accessing enterprise accounts directly from personal devices.

The speed of an intrusion has increased due to effective, repeatable attack paths—as seen with the massive exploitation of MFT tools and Kerberoasting attacks—and the growing efficiency in the criminal marketplace through realized competitive advantage. And while ransomware and other malware continue to plague organizations, cybercriminals have begun to explore how to leverage AI in their operations.

Given these trends, how should organizations respond and where should they start?

Reduce the risk of credential harvesting attacks
Deploying EDR tools on all servers and workstations in your environment helps detect malware, including infostealers and ransomware. The tools can also detect anomalous behavior, such as the exfiltration of data, querying of sensitive information or the creation of new accounts or folders on sensitive systems.

Leverage experts to learn more about how to build and operationalize threat hunting within your environment. If resources are limited, extend your team by using AI to handle up to 85% of alerts and gain 24x7 protection with threat detection and response services. Additionally, use threat intelligence to identify key opportunities for mitigating new and emerging threats from attackers looking to steal your credentials.

Harden your credential management practices to protect your system or domain credentials by implementing MFA and strong password policies to include use of passkeys, and leverage hardened system configurations that make accessing credentials more difficult. Credential harvesting attacks are also often carried out through phishing and watering hole attacks.

Routinely provide employee education with updated phishing techniques used by attackers. Scrutinize all third-party traffic—treat it as untrusted until otherwise verified. Watering hole attackers often leverage legitimate resources to deliver their malware.

Reduce blast radius
Cybersecurity blast radius refers to the potential impact of an incident given the compromise of particular users, devices or data. For example, if an account with administrative privileges is compromised, the blast radius is greater than if a normal nonprivileged account is given the ability to move laterally and access additional data across the network.

Given the importance of data security and identity management in the current threat landscape, organizations should consider implementing solutions to reduce the damage that a data security incident could potentially cause.

Strategies to reduce blast radius:

- Implement a least-privileged framework.
- Provide identity and network segmentation.
- Implement data security and protection solutions.
- Provide continuous monitoring and incident response.

Know your dark web exposure
Attackers may leverage harvested credentials for their own exploits, trade them on the dark web—or both. The data that's available about your organization on the dark web highlights the risk that resides outside your network perimeter's control. Employ dark web capabilities that:

- Find at-risk credentials and session keys.
- Check your executive's digital identities to find overexposure of PII, criticism against executives and fraudulent profile creation in social networks.
- Scan social networks, channels related to your sector, and blogs and advertising for unauthorized brand use.
- Identify leaked priority, confidential and sensitive data.
- Assess forums, credit card markets, Telegram channels, chat rooms and discussions, code repositories, document and file repositories, surface web crawlers, and paste sites checking for credential exposure and stolen session keys.

Remove fragmented identity silos
Properly deploying a product-agnostic identity fabric can extend modern security and detection and response capabilities to outdated applications and systems. Simplify identity management through a single identity and access management (IAM) provider to administer identity governance, manage workforce and consumer identity and access, and control privileged accounts. Streamline the undertaking with identity and security experts to help you define and manage solutions across hybrid cloud environments, transform governance workflows and demonstrate compliance.

Implement a DevSecOps approach and testing
X-Force found that the most observed web application risk across client environments globally in 2023 was security misconfigurations and, of those found, the top offenses included allowing concurrent user sessions in the application. Limit the possibility of session hijacking by implementing a DevSecOps approach and use secured, encrypted connections (HTTPS) and implement session timeouts and prompt for reauthentication. Engage penetration testing services to test your applications, networks, hardware and personnel to identify vulnerabilities and weaknesses across all your assets.

Have a plan
Despite organizations' best efforts to reduce the risk of attack, incidents can happen. Having incident response plans that are customized for your environment is key to reducing the time to respond, remediate and recover from an attack. Those plans should be regularly drilled and include a cross-organizational response, incorporate stakeholders outside of IT and test lines of communication between technical teams and senior leadership. Finally, testing your plan in an immersive, high-pressure cyber range exercise can greatly enhance your ability to respond to an attack.

Establish secured AI+ business models
Securing AI is broader than AI itself. Organizations can leverage existing guardrails to help secure the AI pipeline. The key tenets to focus on are securing the AI underlying training data, the models, and the use and inferencing of the models, but also the broader infrastructure surrounding the models. The same access points that cybercriminals are leveraging to compromise enterprises pose the same type of risk to AI. And as organizations offload operational business processes to AI, they also need to establish governance and make operational guardrails central to their AI strategy.

About us

IBM X-Force

IBM X-Force is a threat-centric team of hackers, responders, researchers and analysts. The X-Force portfolio includes offensive and defensive products and services, fueled by a 360-degree view of threats.

In an age of relentless cyberattacks, a connected everything and increasing regulatory mandates, organizations need a focused security approach. X-Force believes the threat should be the focal point. Through penetration testing, vulnerability management and adversary simulation services, the IBM X-Force Red team of hackers assumes the role of threat actors to find security vulnerabilities—exposing your most important assets. Through incident preparedness, detection and response and crisis management services, the IBM X-Force Incident Response team knows where threats may hide and how to stop them. X-Force researchers create offensive techniques for detecting and preventing threats, while X-Force analysts collect and translate threat data into actionable information for reducing risk.

With a deep understanding of how threat actors think, strategize and strike, X-Force can help you prevent, detect, respond to and recover from incidents and focus on business priorities.

If your organization would like support strengthening your security posture, schedule a one-on-one briefing with an IBM X-Force expert.

IBM Security

IBM Security® adapts to your ever-expanding footprint and works in step with you to keep you on the right track. We help you ensure that you're always staying one step ahead—with greater speed and greater accuracy—with our dynamic AI and automation capabilities. Feel confident that you're making the right moves today and tomorrow with insights from our trusted team of industry-leading experts. From predicting threats to helping to protect data; working across vendors, or around the world; no matter where your business is headed, IBM Security can help you to strive for ambitious business goals, while exploring pivotal new technologies and helping minimize unexpected threats.

Contributors

Christopher Caridi

John Dwyer

Georgia Prassinos

Kat Metrick

Austin Zeizel

Joshua Chung

Dave McMillen

Benjamin Shipley

Charlotte Hammond

Golo Mühr

Ole Villadsen

Joseph Fasulo

Claire Zaboeva

Melissa Frydrych-Dean

Richard Emerson

Camille Singleton

Michelle Alvarez

Andy Piazza

Karlina Bakken

Yannick Bedard

Christopher Bedell

Johnny Shaieb

Scott Lohr

Scott Moore

Guy Vincent Jourdan

Vio Onut

Julien Cassagne

Battalion AI

To learn more, contact your IBM Business Partner:

8173050605 | Info@BattalionAI.com

http://www.BattalionAI.com

© Copyright IBM Corporation 2024

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
February 2024

IBM, the IBM logo, IBM Security, and X-Force are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

The client is responsible for ensuring compliance with all applicable laws and regulations. IBM does not provide legal advice nor represent or warrant that its services or products will ensure that the client is compliant with any law or regulation.

