IBM **Security**

X-Force Threat Intelligence Index 2022: Executive Summary

IBM

Contents

Executive summary

The world continues to grapple with a lasting pandemic, shifts to work-from-home and back-to-office, and geopolitical changes spawning a constant drone of mistrust. All of this equates to chaos, and it is in chaos that cybercriminals thrive. In 2021, IBM Security® X-Force® saw how threat actors opportunistically used a shifting landscape to adopt tactics and techniques to successfully infiltrate organizations across the globe.

The IBM Security X-Force Threat Intelligence Index maps new trends and attack patterns we observed and analyzed from our data—drawing from billions of datapoints ranging from network and endpoint detection devices, incident response (IR) engagements, domain name tracking and more. This report represents the culmination of that research based on data collected from January to December 2021.

We offer these findings as a resource to IBM clients, researchers in the security industry, policy makers, the media and to the broader community of security professionals and business leaders.

Given the volatile landscape and the evolution of both threat types and threat vectors, you need threat intelligence insights to stay ahead of attackers and fortify your critical assets more than ever.

Report highlights

Top attack type: Ransomware was again the top attack type in 2021, although the percentage of attacks X-Force remediated that were ransomware decreased nearly 9% year-over-year. REvil—a ransomware type X-Force also refers to as Sodinokibi—was the most common ransomware strain X-Force observed for a second year, making up 37% of all ransomware attacks, followed by Ryuk at 13%. Law enforcement activity has probably been the primary force driving down ransomware and IoT botnet attacks in 2021, but this does not preclude a potential resurgence in 2022.

Supply chain vulnerabilities: Supply chain security was pushed to the forefront of government and policymakers' attention, with the Biden administration's executive order on cybersecurity, and guidance from the U.S. Department of Homeland Security, CISA, and NIST doubling down on zero trust guidance. These guidelines put a spotlight on vulnerabilities and trusted relationships. Vulnerability exploitation was the top initial attack vector in manufacturing, an industry grappling with the effects of supply chain pressures and delays.

Most phished brands: X-Force closely tracked how cybercriminals are using phishing kits throughout 2021, and our research revealed that Microsoft, Apple and Google were the top three brands criminals attempted to mimic. These mega brands were used repeatedly in phishing kits, with attackers likely seeking to capitalize on their popularity and the trust many consumers place in them.

Top threat groups: Suspected Iranian nation-state threat actor ITG17 (MuddyWater), cybercriminal group ITG23 (Trickbot), and Hive0109 (LemonDuck) were some of the most active threat groups X-Force intelligence analysts observed in 2021. Threat groups worldwide were seeking to augment their prowess and infiltrate more organizations. Malware they used was embedded with greater defense-evasion techniques, in some cases hosted via cloud-based messaging and storage platforms to get through security controls. These platforms were abused to hide command and control communication in legitimate network traffic. Threat actors also continued to develop Linux versions of malware, to enable them to cross over to cloud environments more easily.

Key stats

21%

Ransomware share of attacks
Ransomware was the number one attack type observed by X-Force last year, decreasing to 21% of attacks from 23% in the previous year. REvil ransomware actors (aka Sodinokibi) were responsible for 37% of all ransomware attacks.

17 months

Average time before a ransomware gang rebrands or shuts down
Ransomware gangs studied by X-Force had an average lifespan of 17 months before rebranding or disbanding. REvil, one of the most successful gangs, shut down in October 2021 after 31 months (two and a half years).

41%

Percentage of attacks exploiting phishing for initial access
Phishing operations emerged as the top pathway to compromise in 2021, with 41% of incidents X-Force remediated using this technique to gain initial access.

33%

Increase in the number of incidents caused by vulnerability exploitations from 2020 to 2021
Four out of the top five vulnerabilities exploited in 2021 were new vulnerabilities, including the Log4j vulnerability CVE-2021-44228—which was ranked number two, despite only being disclosed in December.

3X

Click effectiveness for targeted phishing campaigns that add phone calls
The click rate for the average targeted phishing campaign was 17.8%, but targeted phishing campaigns that added phone calls (vishing or voice phishing) were three times more effective, netting a click from 53.2% of victims.

146%

Increase in Linux ransomware with new code

The percentage of Linux ransomware with unique (new) code increased year-over-year by 146%, according to Intezer, indicating an increase in the level of Linux ransomware innovation.

#1

Manufacturing industry rank for attacks

Manufacturing replaced financial services as the top attacked industry in 2021, representing 23.2% of the attacks X-Force remediated last year. Ransomware was the top attack type, accounting for 23% of attacks on manufacturing companies.

61%

Manufacturing share of compromises on OT-connected organizations

Sixty-one percent of incidents at OT-connected organizations last year were in the manufacturing industry. In addition, 36% of attacks on OT-connected organizations were ransomware.

2,204%

Increase in reconnaissance against OT

Attackers increased their reconnaissance of SCADA Modbus OT devices accessible via the internet by 2,204% between January and September 2021.

74%

Share of IoT attacks originating from Mozi botnet

In 2021, attacks against IoT devices originated from the Mozi botnet 74% of the time.

26%

Share of global attacks that targeted Asia

Twenty-six percent of all attacks had targets in Asia in their crosshairs. Asia was the most attacked geography of 2021.

Risk mitigation recommendations

The threats we have presented in this report have the potential to cause concern, as the report underscores the grave and increasing threat from ransomware, renewed threats from BEC and phishing, and highlights several zero-day exploits threat actors have exploited over the past year. However, our intention is for this information to empower organizations as they better understand the current threat landscape, and help build confidence in the actions they need to take to combat these threats.

Some security principles X-Force has found helpful in combating today's cyber threats include a zero trust approach, automation of incident response, and extended detection and response capabilities.

Zero trust assists in decreasing risk of top attacks

Zero trust is a paradigm shift, a new way of approaching security problems, that assumes a breach has already happened and aims to increase the difficulty for an attacker to move throughout a network. At its core is understanding where critical data resides and who has access to this data, and creating robust verification measures throughout a network to ensure only the right individuals are accessing that data in the right way.

Research by X-Force threat researchers confirms that principles related to a zero trust approach—to include implementation of MFA and the principle of least privilege—have the potential to decrease organizations' susceptibility to the top attack types identified in this report, particularly ransomware and BEC.

Applying the principle of least privilege to domain controllers and domain administrator accounts in particular can increase barriers for ransomware actors, as many of these actors seek to deploy ransomware to a network from a compromised domain controller. In addition, implementing MFA increases the difficulty for cybercriminals seeking to take over email accounts by requiring that they provide further authentication beyond stolen credentials.

Learn more about how to build a zero trust approach →

Security automation enhances incident response

The X-Force incident response team addresses hundreds of incidents every year, in a variety of geographies, assisting in-house incident response analysts and addressing a range of attack types. Speed is of the essence, whether that means identifying and eradicating threat actors before they can deploy ransomware on a network, or quickly and efficiently resolving issues to create bandwidth for the next incident. In this fast-paced environment, security automation is key—outsourcing to machines tasks that might take a human analyst or team hours, and identifying mechanisms for improving workflows.

In mid-2021, IBM donated a threat hunting automation tool to the Open Cybersecurity Alliance, aimed at assisting security operations center (SOC) analysts to quickly conduct forensic investigations and address cyber incidents. In addition, the X-Force IR team uses IBM Security QRadar SOAR to enhance its incident response capabilities.

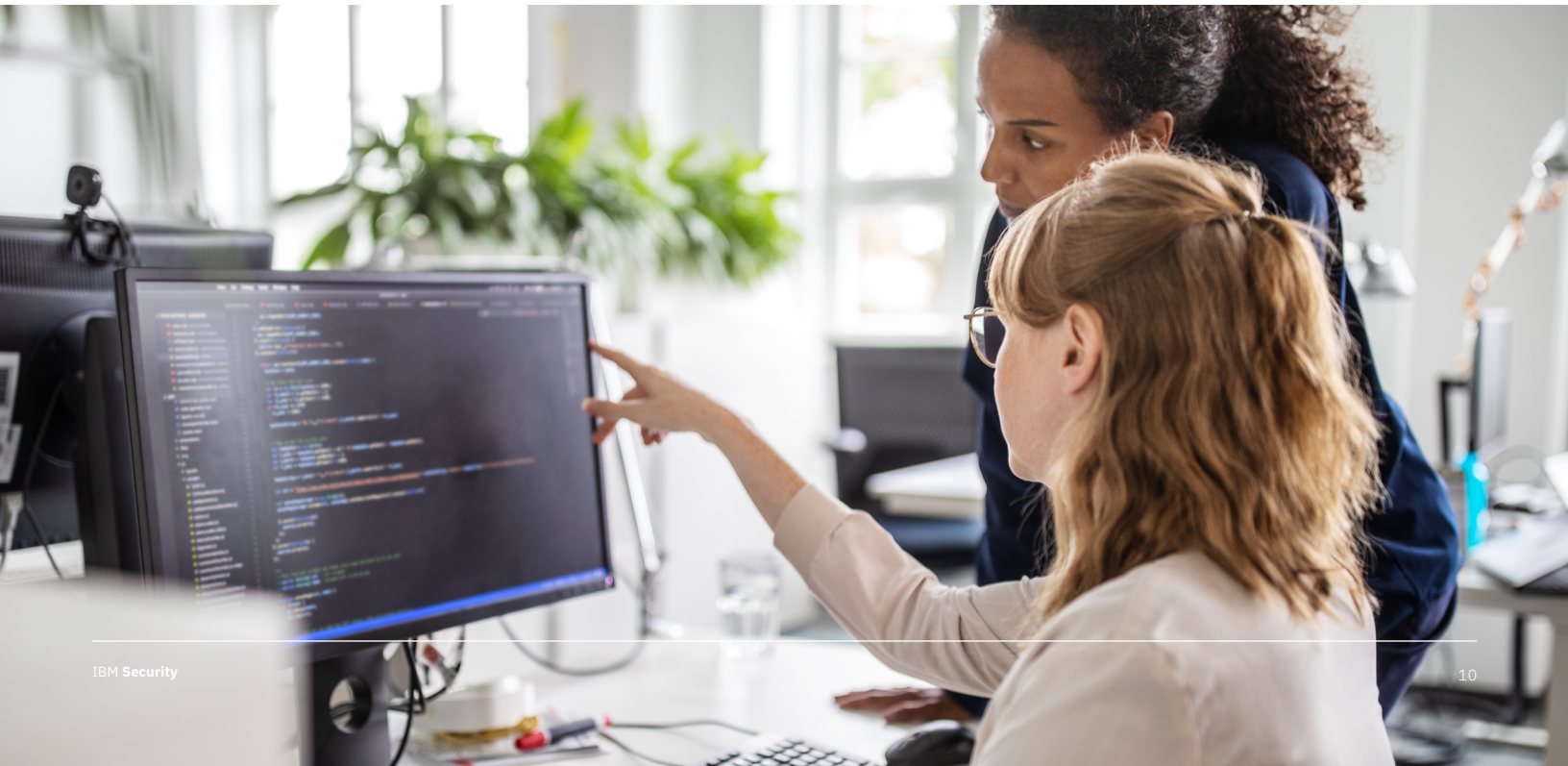
Learn more about IBM's incident response services →

Extended detection and response provides a significant advantage over attackers

Detection and response technologies—particularly when several different solutions are combined into an extended detection and response (XDR) solution—provide organizations with a significant advantage in identifying and eradicating attackers from a network before they are able to reach the final stage of their attack, such as ransomware deployment or data theft.

In multiple instances, when the X-Force IR team has deployed an endpoint detection and response (EDR) or XDR solution on a client's network, IR has immediately gained additional insight that has assisted in identifying attacker activities and quickly addressed them. XDR technologies are probably helping to drive the increase in server access and other attack types X-Force observes that indicate an attacker was identified and stopped before the operation could achieve its intended conclusion.

Learn more about IBM Security QRadar XDR →



Recommendations

The following recommendations include specific actions organizations can take to better secure their networks against the threats presented in this report.

Develop a response plan for ransomware. Every industry and every geography is at risk of a ransomware attack, and how your team responds in the critical moment can make all the difference in the amount of time and money lost in a response.

- Include in your response plan immediate containment actions, what stakeholders and law enforcement officials should be informed, how your organization will safely store and restore from backups, and an alternate location from where critical business functions can be run during remediation.
- Include in your plan a scenario of data theft and leak as part of the ransomware attack—this is a very common tactic used today, seen in a very high percentage of ransomware attacks X-Force remediates.
- Use ransomware drills to also think through whether your organization would pay a ransom and what factors would alter your calculus for that decision.
- Ensure your ransomware response plan includes a specific contingency for a cloud-related incident, as it may require additional tools and skills.
- Avoid data corruption due to malware or ransomware attacks with flash storage solutions that help prevent data loss, promote operational continuity, and lower infrastructure costs.
- X-Force's Definitive Guide to Ransomware gives additional detailed advice on how to respond to a ransomware attack. X-Force's incident response team can also conduct a ransomware readiness assessment for your organization to help build and test a ransomware incident response plan. The X-Force Command Center similarly prepares organizations for a ransomware attack, taking into account both the business and technical response required.

Implement multifactor authentication on every remote access point into a network. X-Force has observed more organizations implementing MFA more successfully than ever before. This is literally altering the threat landscape, forcing threat actors to find new ways of compromising networks rather than leveraging stolen credentials, and decreasing the effectiveness of email takeover campaigns.

- MFA can decrease the risk of several different attack types, including ransomware, data theft, BEC, and server access.
- In addition, identity and access management technologies are making MFA implementation easier every year—both for implementation teams and for end-users.

Adopt a layered approach to combat phishing. Unfortunately, there is no one tool or solution that will prevent all phishing attacks today, and threat actors continue to refine social engineering and anti-malware detection techniques to circumvent established controls. Thus, we recommend implementing several layers of solutions that have a higher chance of catching phishing emails.

— First, effective user awareness and education is key and should include real-world examples.

— Second, employ an email software security solution to put a machine to the task of identifying and filtering out malicious messages.

— Third, implement several defenses that can help to catch malware or lateral movement quickly should a phishing email slip through, including behavioral-based anti-malware detection, endpoint detection and response (EDR), intrusion detection and prevention solutions (IDPS), and a security information and event management (SIEM) system.

Refine and mature your vulnerability management system. Vulnerability management is an art—from identifying which vulnerabilities are most applicable to your organization's network architecture, to identifying how to deploy them without breaking anything in the process.

— Having a team dedicated to vulnerability management and making sure this team is well-resourced and supported can make all the difference in ensuring your network is protected from potential vulnerability exploitation.

— We recommend prioritizing any of the vulnerabilities mentioned in this assessment that are applicable to your organization.

— IBM's X-Force Exchange also includes a repository of vulnerabilities and associated criticality levels to assist you in identifying vulnerabilities of most concern, and X-Force Red can provide specialized vulnerability scanning and management services.

Learn more from the full report →

About IBM Security X-Force

IBM Security X-Force is a threat-centric team of hackers, responders, researchers and analysts. Our portfolio includes offensive and defensive products and services, fueled by a 360-degree view of threats. With X-Force as your security partner, you can affirm with confidence that the likelihood and impact of a data breach are minimal.

IBM Security X-Force Threat Intelligence combines IBM security operations telemetry, research, incident response investigations, commercial data, and open sources to aid clients in understanding emerging threats and quickly making informed security decisions.

Additionally, the X-Force Incident Response team provides detection, response, remediation, and preparedness services to help you minimize the impact of a data breach.

X-Force combined with the IBM Security Command Center experiences trains your team—from analysts to the C-suite—to be ready for the realities of today's threats. X-Force Red, IBM Security's team of hackers, provides offensive security services, including penetration testing, vulnerability management and adversary simulation.

Throughout the year, IBM X-Force researchers also provide ongoing research and analysis in the form of blogs, white papers, webinars and podcasts, highlighting our insight into advanced threat actors, new malware, and new attack methods. In addition, we provide a large body of current, cutting-edge analysis to subscription clients through our X-Force Threat Intelligence solutions.

Schedule a consultation with one of our X-Force experts →

About IBM Security

IBM Security works with you to help protect your business with an advanced and integrated portfolio of enterprise security products and services, infused with AI and a modern approach to your security strategy using zero trust principles—helping you thrive in the face of uncertainty. By aligning your security strategy to your business; integrating solutions designed to protect your digital users, assets, and data; and deploying technology to manage your defenses against growing threats, we help you to manage and govern risk that supports today's hybrid cloud environments.

Our new modern, open approach, the IBM Cloud Pak for Security platform, is built on RedHat Open Shift and supports today's hybrid multicloud environments with an extensive partner ecosystem. Cloud Pak for Security is an enterprise-ready containerized software solution that enables you to manage the security of your data and applications—by quickly integrating your existing security tools to generate deeper insights into threats across hybrid cloud environments—leaving your data where it is, allowing easy orchestration and automation of your security response.

For more information, contact your IBM Business Partner

Secure ISS

0448761634 | icooper@secure-iss.com

https://secure-iss.com/

Contributors

Camille Singleton
Charles DeBeck
Joshua Chung
Dave McMillen
Scott Craig
Scott Moore
Charlotte Hammond
John Dwyer
Melissa Frydrych
Ole Villadsen
Richard Emerson
Guy-Vincent Jourdan
Vio Onut
Stephanie Carruthers
Adam Laurie
Michelle Alvarez
Salina Wuttke
Georgia Prassinos
John Zorabedian
Mitch Mayne
Limor Kessem
Ian Gallagher
Ari Eitan

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2022