X-Force Threat Intelligence Index Report Findings and What's on The Horizon

Mitch Mayne
Public Information Officer,
IBM Security X-Force

Camille Singleton
Manager, Cyber Range
R&D Team,
IBM Security X-Force

Charles DeBeck
Strategic Cyber Threat
Analyst, IBM Security X-Force

IBM Security

IBM

Today’s topics

- Introduction
- Impact of Ukraine Crisis
- Recommendations
- Threat landscape key findings
- Questions

IBM Security

X-Force Threat Intelligence Index 2022

IBM

Impact of Ukraine Crisis

IBM Security X-Force Research Advisory: New Destructive Malware Used In Cyber Attacks on Ukraine:
https://securityintelligence.com/posts/new-destructive-malware-cyber-attacks-ukraine/

X-Force Exchange Collection: Ukraine/Russia Conflict:
https://exchange.xforce.ibmcloud.com/collection/56ed5d53e7aeca5d1624be2d181f7d0a

IBM Security recommendations

1. Develop a response plan for ransomware.
2. Implement multifactor authentication on every remote access point into a network.
3. Adopt a layered approach to combat phishing.
4. Refine and mature your vulnerability management system.
5. Adopt zero trust principles to help decrease risk of top attacks.
6. Use security automation to enhance incident response.
7. Use extended detection and response capabilities for an advantage over attackers.

Ransomware was the top attack type

21%

Ransomware's share of attacks

37%

Share of attacks by the top ransomware group REvil

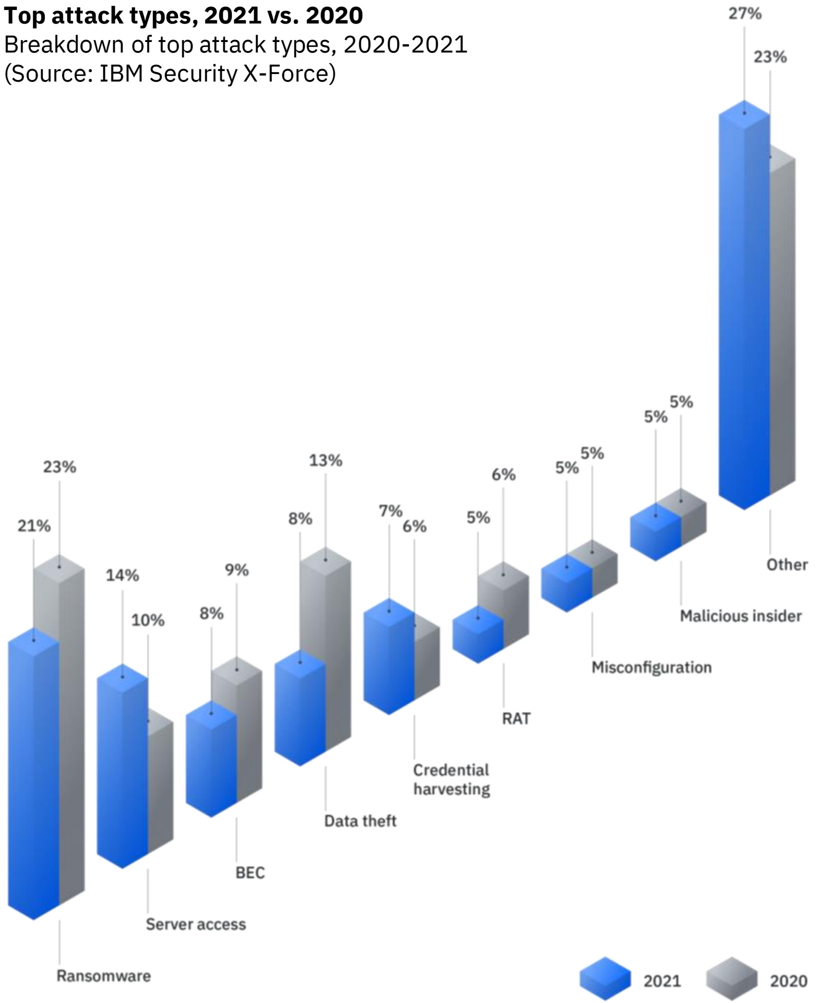
17 months

Average lifespan of a ransomware gang

Top attack types, 2021 vs. 2020

Breakdown of top attack types, 2020-2021

(Source: IBM Security X-Force)



Phishing and vulnerability exploitation the top initial infection vectors

41%

Phishing's share of attacks

33%

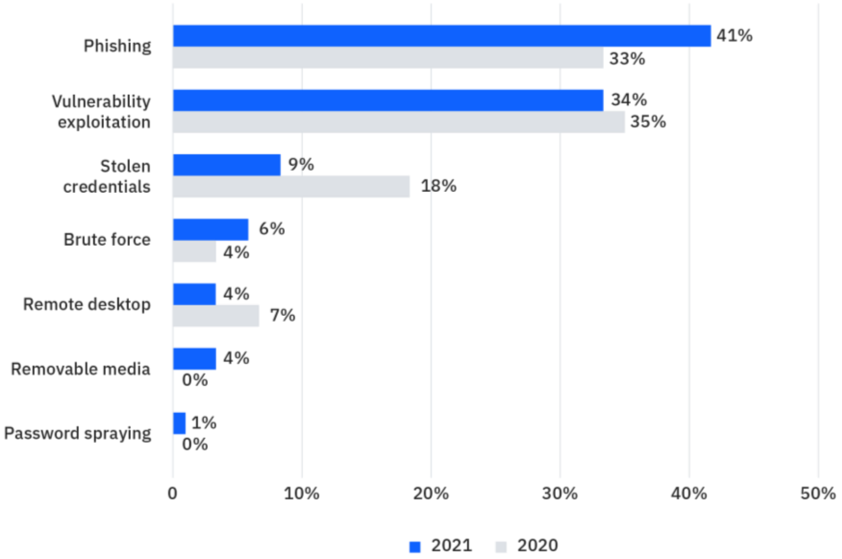
Increase in vulnerability exploitation attacks

Log4j

Second on the list of top 10 vulnerabilities

Top infection vectors, 2021 vs. 2020

Breakdown of infection vectors observed by X-Force Incident Response, 2020-2021 (Source: IBM Security X-Force)



Threats to supply chain, manufacturing, OT and IoT

61%

Manufacturing's share of compromises at OT-connected organizations

2,204%

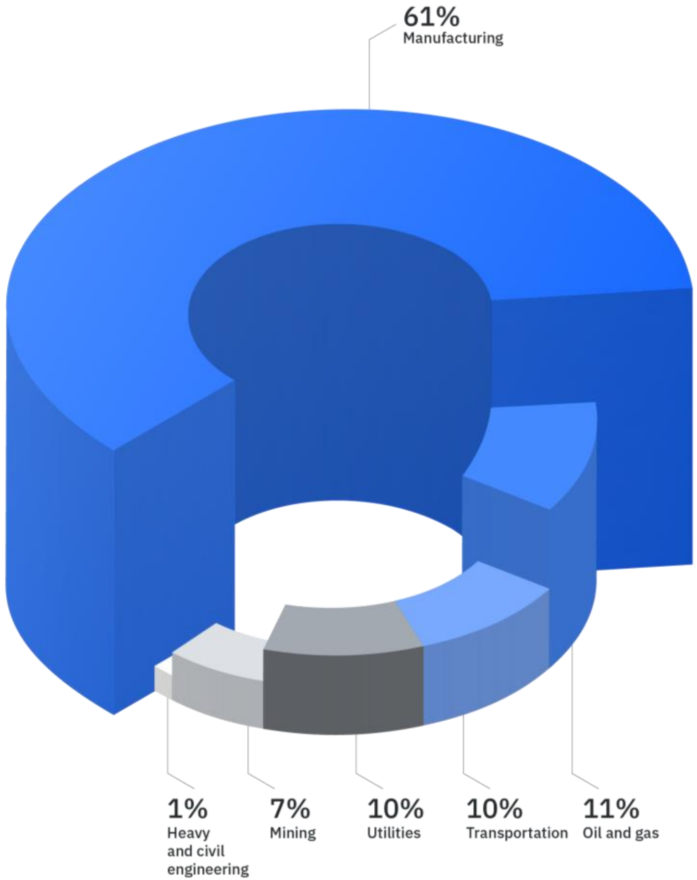
Increase in reconnaissance against SCADA Modbus devices open on the Internet

74%

Share of IoT malware from the Mozi botnet

OT industries targeted, 2021

Breakdown of attacks against six operational technology industries, as observed by X-Force IR, 2021 (Source: IBM Security X-Force)



Cloud threats and Linux malware innovation

146%

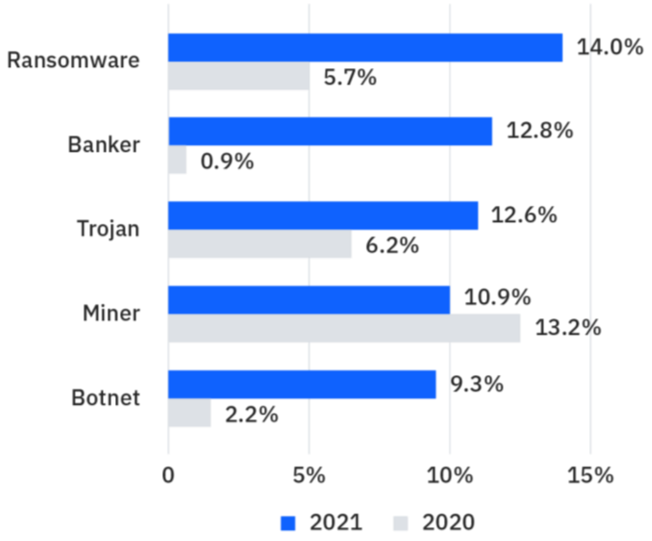
Increase in Linux ransomware with new code

Docker targeted

Malware more capable across cloud platforms

Linux malware with unique code, 2021 vs. 2020

Linux malware with unique (new) code in five categories, 2020-2021 (Source: Intezer)



Geographic trends

Asia

Experienced the most attacks of any region

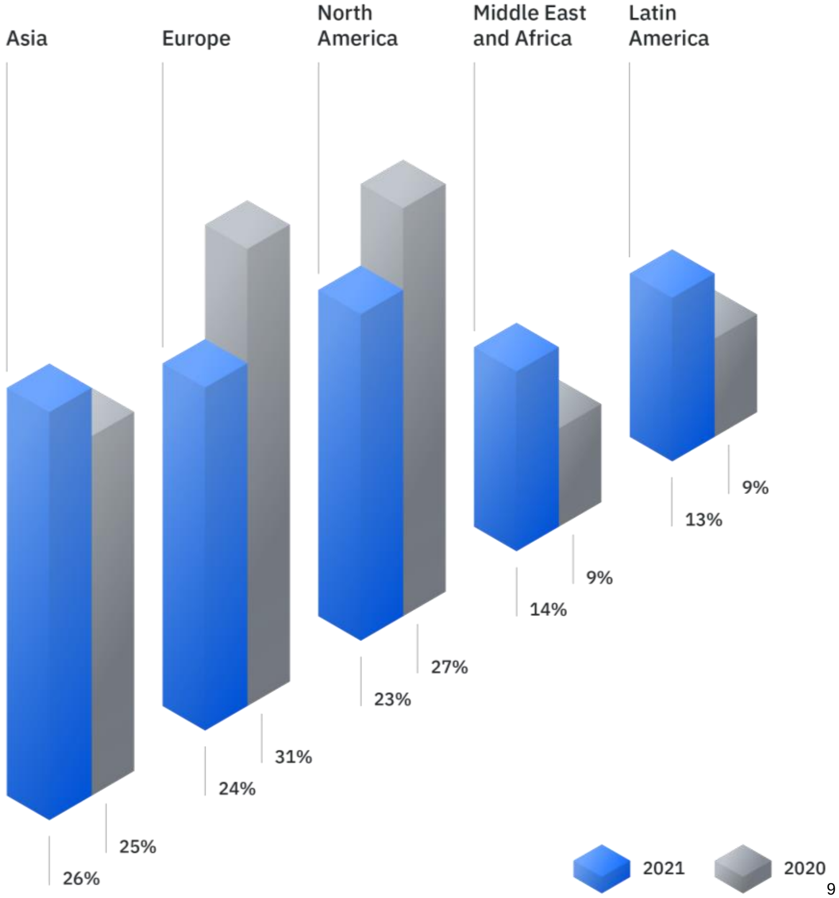
Europe

Dropped from first to second in share of attacks

North America

Third-most attacked region

Breakdown of attacks by geography, 2021 vs. 2020
(Source: IBM Security X-Force)



Industry trends

Manufacturing #1

Experienced the most attacks of any industry

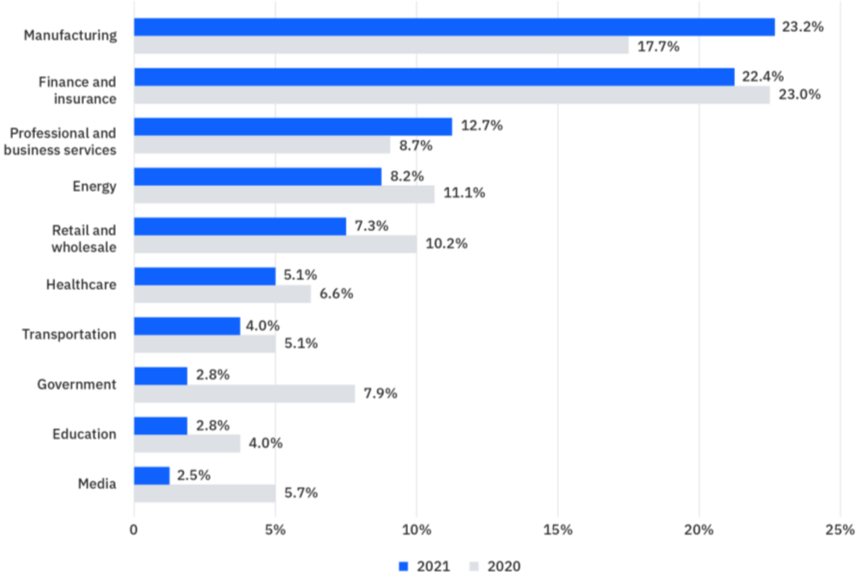
Finance and insurance #2

Doing security right

Wholesale heavily attacked

More attacked than retail in the last year

Breakdown of attacks on the top 10 industries, 2021 vs. 2020
(Source: IBM Security X-Force)



Key findings

Ransomware the top attack type

21%

Percentage of attacks that were ransomware

17 months

Average time before a ransomware gang rebrands or shuts down

Phishing and vulnerability exploitation the top attack vectors

41%

Percentage of attacks that used phishing for initial access

3X

Click effectiveness for targeted phishing campaigns that add phone calls

33%

Increase in the number of incidents caused by vulnerability exploitation

Threats to manufacturing, OT and IoT

#1

Manufacturing's rank in top attacked industries

61%

Manufacturing share of compromises in OT-connected organizations

2,204%

Increase in reconnaissance against OT

74%

Share of IoT attacks originating from Mozi botnet

Cloud, Linux threats rise

146%

Increase in Linux ransomware with new code

Asia becomes top attacked geo

26%

Share of global attacks that targeted Asia

Resources

- Report webpage: ibm.biz/xforcethreatindex

- Executive summary: ibm.biz/ExecSummaryTII

- Full report: ibm.biz/FullReportTII

- Schedule a 1:1 X-Force consult: ibm.biz/ConsultTII

- Learn more about X-Force: ibm.biz/X-Force

- If you are experiencing an incident, contact X-Force to help:
  - US hotline 1-888-241-9812
  - Global hotline (+001) 312-212-8034

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. 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 systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. 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.

IBM®