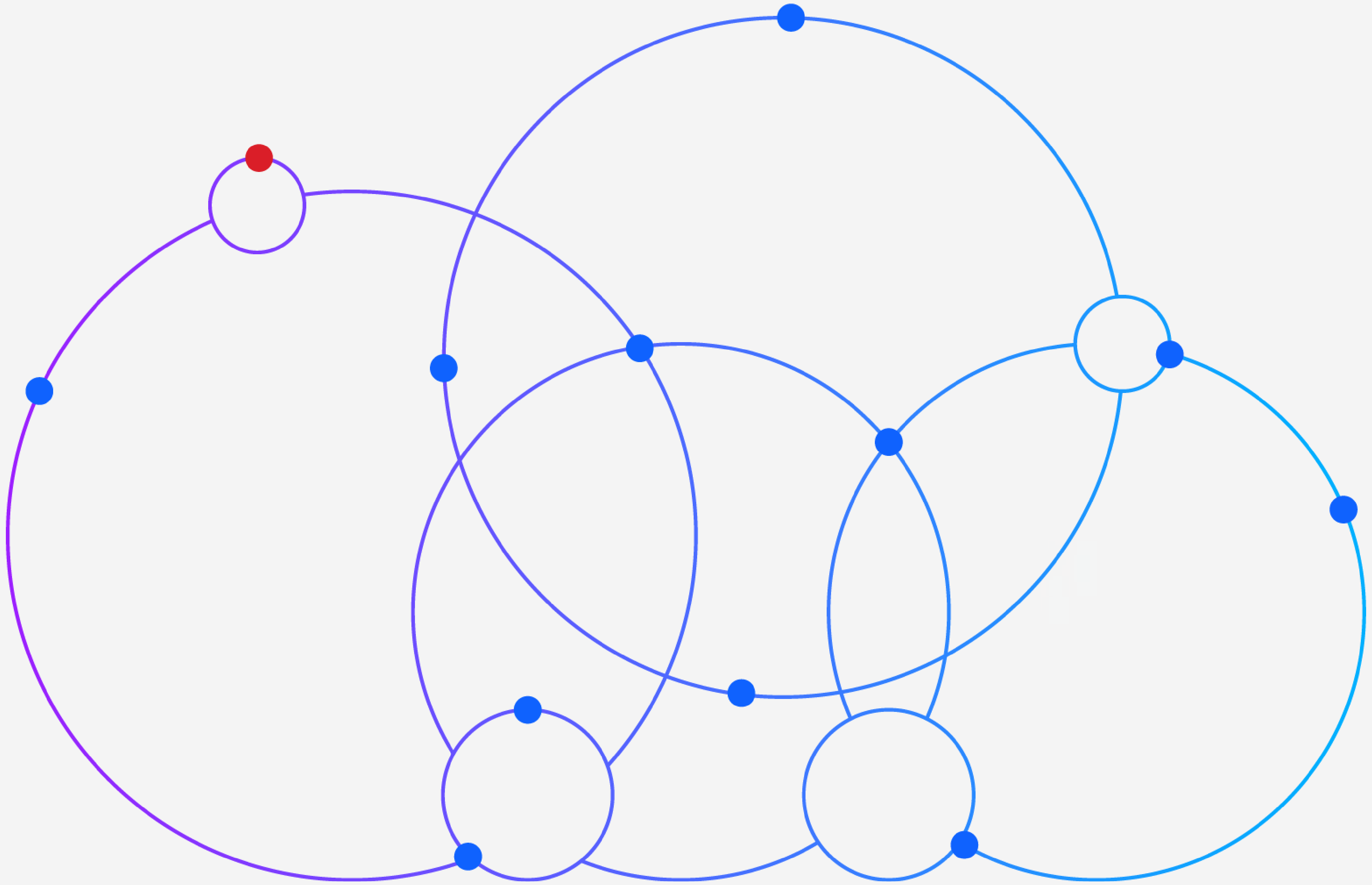
IBM X-Force Cloud Threat Landscape Report 2023



Contents

Introduction

The IBM® X-Force® team produces the Cloud Threat Landscape Report, now in its fourth year of publication, to aid clients and the broader community with their cloud security strategy. This report uses research based on a review of data from multiple cloud service providers (CSPs).

To produce this report, the X-Force team reviewed data compiled between June 2022 through June 2023 and gleaned from the following sources:

- IBM X-Force threat intelligence
- IBM X-Force Red penetration tests
- IBM X-Force incident response (IR) engagements
- Red Hat® Insights
- Dark web analysis by the X-Force team and data provided by report contributor Cybersixgill

Our findings reveal the various ways we've observed threat actors compromising cloud environments and the types of malicious activities they pursue when inside. With 82% of data breaches involving data stored in cloud environments, organizations must learn how they can effectively prepare and react to security incidents involving their cloud environments.[1]

Next chapter >

Key takeaways

Misuse of legitimate credentials plagues the cloud landscape

- IR data indicates that the use of valid credentials was the most common initial access vector in cloud security incidents, occurring in 36% of cases.
- The X-Force team discovered plaintext credentials located on user endpoints in 33% of engagements involving cloud environments.

Container security concerns are on the rise

- The X-Force Red team reported a large uptick in custom resource definition use in organizations' Kubernetes clusters, which can become security concerns if implemented poorly or without the appropriate level of security-inclusive development processes.

Vulnerabilities are increasingly being discovered and disclosed

- The X-Force team tracked 632 new cloud-related common vulnerabilities and exposures (CVEs) during the reporting period. This number is a 194% increase from the prior year.

The impact felt by the exploitation of these CVEs is varied

- Just over 40% of the CVEs discovered during the reporting period could allow an attacker to either obtain information (21%) or gain access (20%).

Cloud is still a hot commodity on the dark web

- Credentials comprised nearly 90% of cloud assets for sale on the dark web during the reporting period.
- The average price for these credentials was USD 10.68, representing a slight decrease from the previous reporting period.

194%

increase of new cloud-related CVEs from the prior year

02

X-Force insights from the field

The X-Force team reviewed all engagements involving cloud-related incidents during the reporting period and identified the following most common attack vectors and industry trends impacting cloud infrastructure:

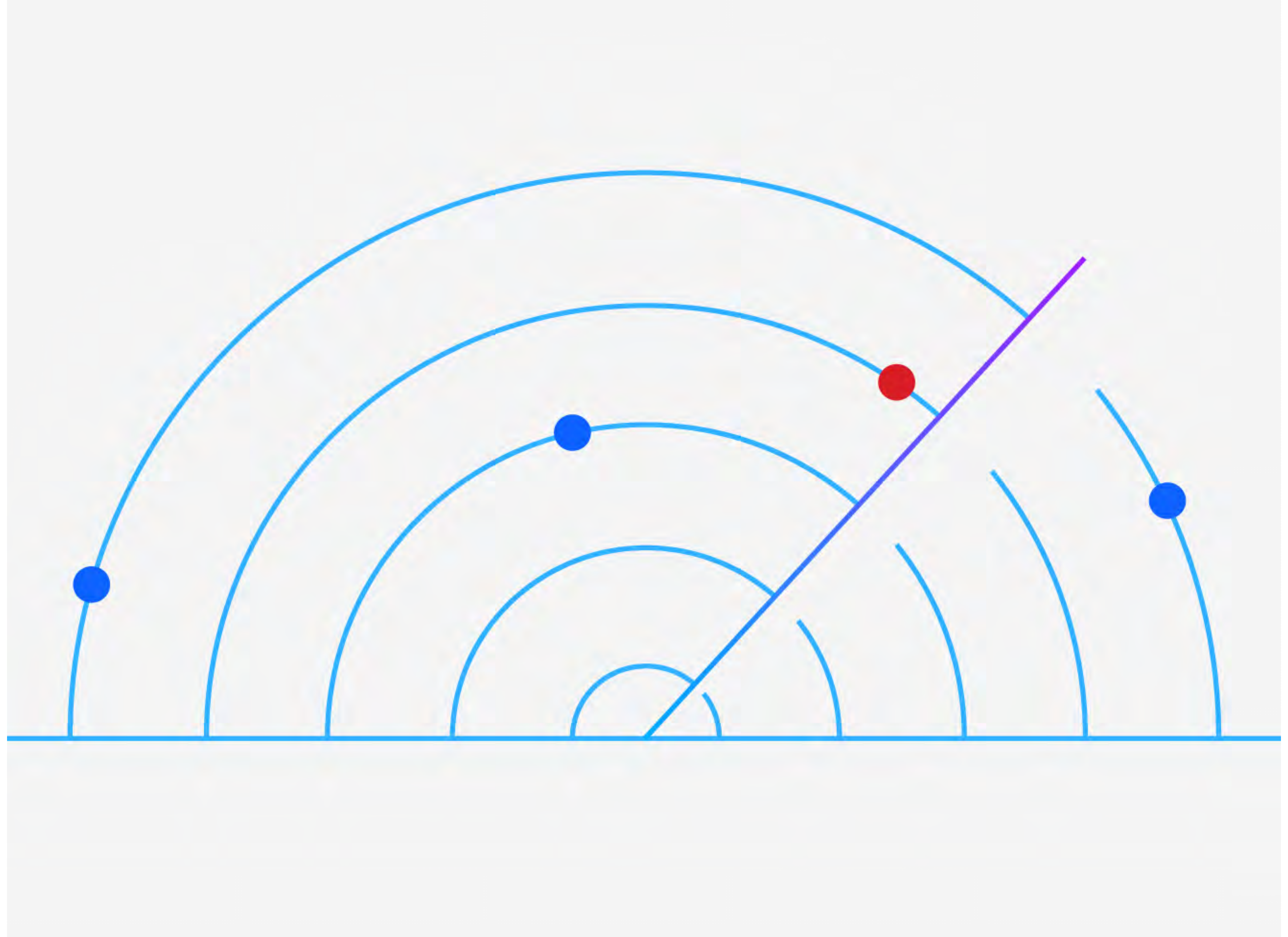
- The use of valid cloud credentials (T1078.004[2]) was the most observed initial access vector in cloud environments, seen in 36% of cases the X-Force team responded to. The exploitation of public-facing applications (T1190[3])—along with phishing and spear phishing links (T1566.002[4])—tied for second place, both representing approximately 14% of incidents.
- Media and entertainment led all industries, with 21% of all cloud-related incidents that the X-Force team responded to during the reporting period.
- Given the distributed nature of cloud computing, every geographic region of the world experiences cloud attacks. According to X-Force IR data, Europe experienced 64% of cloud-related incidents, followed by North America at 29%. Data from Red Hat Insights further supports these findings, showing that European organizations accounted for 87% of malware scans, followed by North America at 12%.

Initial access vectors

The use of valid credentials
Threat actors looking to traverse a network or burrow deeper inside a victim's environment will often do so by using legitimate credentials either discovered during an attack or harvested prior to targeting a specific victim. In cases where cloud infrastructure is part of the attack surface, these credentials could be used to access cloud-specific resources without raising appropriate levels of suspicion.

The X-Force team discovered plaintext credentials located on user endpoints in 33% of engagements involving cloud environments. In particular, there was a high frequency of service account credentials stored on endpoints, and many were overprivileged. Excessively privileged users can be defined as those who have more permissions than they need to do their job or task. Compromised credentials caused over one-third of cloud-related incidents that the X-Force team observed, suggesting that businesses are challenged to balance user access needs and security risks. Organizations can benefit from AI-powered identity protections that help identify behavioral anomalies in depth and verify users' identity.

Read X-Force threat activity report summaries →



Exploiting public-facing applications
The exploitation of vulnerabilities in public-facing applications is a tried-and-true access vector for threat actors in cloud and local environments alike. Cloud applications are typically more challenging for organizations to manage due to the increasing number of applications and services used in a modern cloud or hybrid cloud environment. If implemented improperly, it's possible to overlook an outdated application running in the cloud, or worse, be unaware that the application is even in use.

In 2022, the Apache Log4j vulnerability[5] had a significant impact across all sectors due to the extremely wide deployment of the Log4j library. Disclosed in December of 2021, this vulnerability was easy to exploit, making it a popular choice for multiple threat actors to use in their toolkit. For these reasons, we still see Log4j being abused well into 2023. As part of our partnership with the Red Hat Insights team, the X-Force team analyzed files tied to a phishing email campaign that included malicious cryptomining bash scripts attempting to exploit the Log4j vulnerability in Linux® systems.

Proxyjacking: The X-Force team has observed adversaries installing proxyware—a legitimate network segmentation tool—on unsuspecting victims' systems to resell the victims' computer bandwidth. Research suggests that a proxyjacking campaign could net threat actors roughly USD 9.60 within 24 hours for one IP address, and deploying it by Log4j could provide USD 220,000 in profit per month.[6] Additionally, proxyjacking can result in victims being hit with large cloud provider charges due to the increase in unexpected web traffic. Further, proxyjacking is harder to detect than cryptomining because cryptomining can be detected by monitoring CPU usage.

36%

of cloud security incidents the X-Force team responded to where the use of valid credentials was the initial access vector

Continual exploitation of virtual environments: Aligning with the X-Force team's observations, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI issued a joint advisory in early 2023 in response to an ongoing ransomware campaign dubbed ESXiArgs. The threat actors in this ransomware campaign were exploiting vulnerabilities in VMware ESXi servers (CVE-2021-21974[7]) to gain access, deploy ransomware and encrypt files on ESXi servers, potentially making virtual machines (VMs) unusable.

Malware families and cloud-based file hosting: X-Force malware reverse engineers have observed threat actors widely using cloud-based file hosting services, such as Dropbox, Microsoft OneDrive or Google Drive, to distribute malicious software that appears legitimate, including:

- Grandoreiro banking trojan using Microsoft Azure
- RokRAT backdoor using OneDrive
- ITG18, also known as Yellow Garuda malware, using OneDrive, Dropbox and Google Drive
- Marlin backdoor using OneDrive
- Graphite malware using OneDrive
- Generic malware using OneDrive[8]

Container security

This year, X-Force researchers have seen a large uptick in the use of custom resource definitions (CRDs). A growing number of organizations are more capable and willing to create custom resources in their Kubernetes clusters. They often do so without a normal security-inclusive application development process because they're using internal application programming interfaces (APIs). This process allows for new capabilities in the Kubernetes clusters. Some CRDs are off-the-shelf solutions that come with a great deal of support, while others are lower-effort components made in-house or with minimal support from the community. Exploitability of these CRDs can be exceptionally easy or exceptionally difficult.

Actions on objective: Mining, RATs and bots

Although cloud environments have been targeted for attempted data extortion, much of the threat activity over the period analyzed appeared to concentrate on using compromised access to cloud resources for cryptomining. Similar to the trend we highlighted in last year's report, in 2023, the X-Force team observed the XMRig cryptominer being deployed on Linux machines and cloud instances. XMRig is used as the main payload to mine the Monero cryptocurrency.

Why threat actors choose to mine the cloud

The threat actors behind cryptomining activity are likely attracted to cloud platforms for the following reasons:

1. Cryptomining activity is highly resource intensive and therefore costly. By taking advantage of a compromised infrastructure, threat actors can transfer the cost onto the victim.
2. Actors may count on cloud resources receiving less thorough and less vigilant monitoring compared to on-premises resources, allowing mining malware to operate longer before being detected and removed.
3. High-profile vulnerabilities in internet-facing infrastructure—such as the Log4j vulnerability—have enabled threat actors to attempt to scan, exploit and deploy cryptominers opportunistically and at scale.

Chaos RAT

The X-Force team has also observed the Chaos Remote Administrative Tool (Trojan.Linux.CHAOSRAT) being deployed as a remote access tool (RAT). Chaos RAT functions include reverse shell file download, upload and delete; screenshots; operating system information gathering; shutting down and restarting the host; and opening URLs. This RAT shows the sophistication and evolution of cloud-based threat actors.

KeyBot

X-Force researchers observed and analyzed KeyBot, a scanner written in Python that is used to scan a list of domains for keys associated with various services, including cloud-based applications. This particular strain of malware has been seen targeting Amazon Web Services (AWS) servers. The actions performed on the system included dropped files, persistence mechanisms, process execution details and network communications.

Cloud vulnerabilities: An upward trajectory

IBM X-Force Red Vulnerability Management Services provides insights on known vulnerabilities in cloud environments. The X-Force team is tracking nearly 3,900 cloud-related vulnerabilities, a number that has doubled since 2019.

Number of total cloud vulnerabilities tracked by X-Force Red Vulnerability Management Services

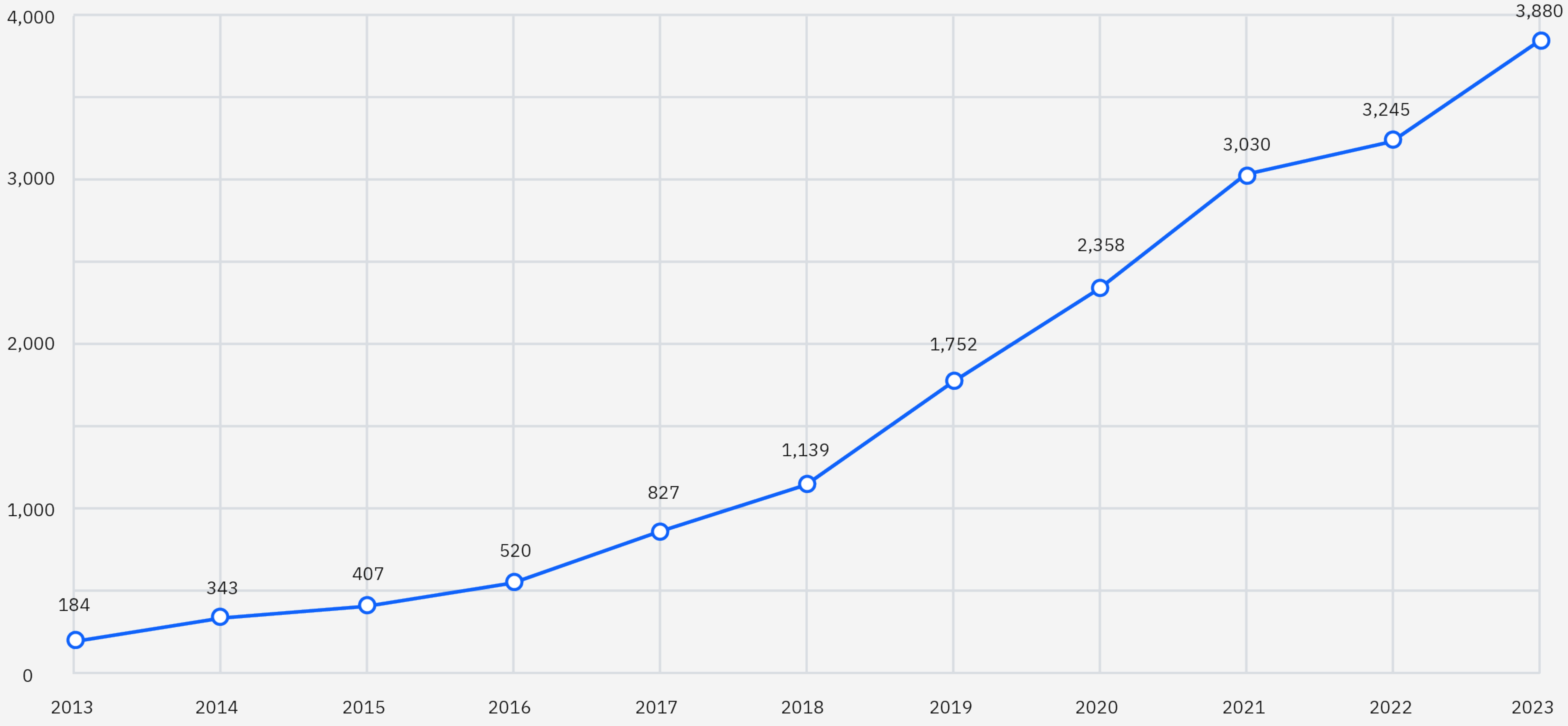


Figure 1. The number of tracked cloud vulnerabilities has grown exponentially in the last decade.

X-Force data shows that both the average X-Force threat score and new CVEs tracked over the past decade have been trending upward.[9] Despite a dip in 2022, this year, we've observed 632 new CVEs.

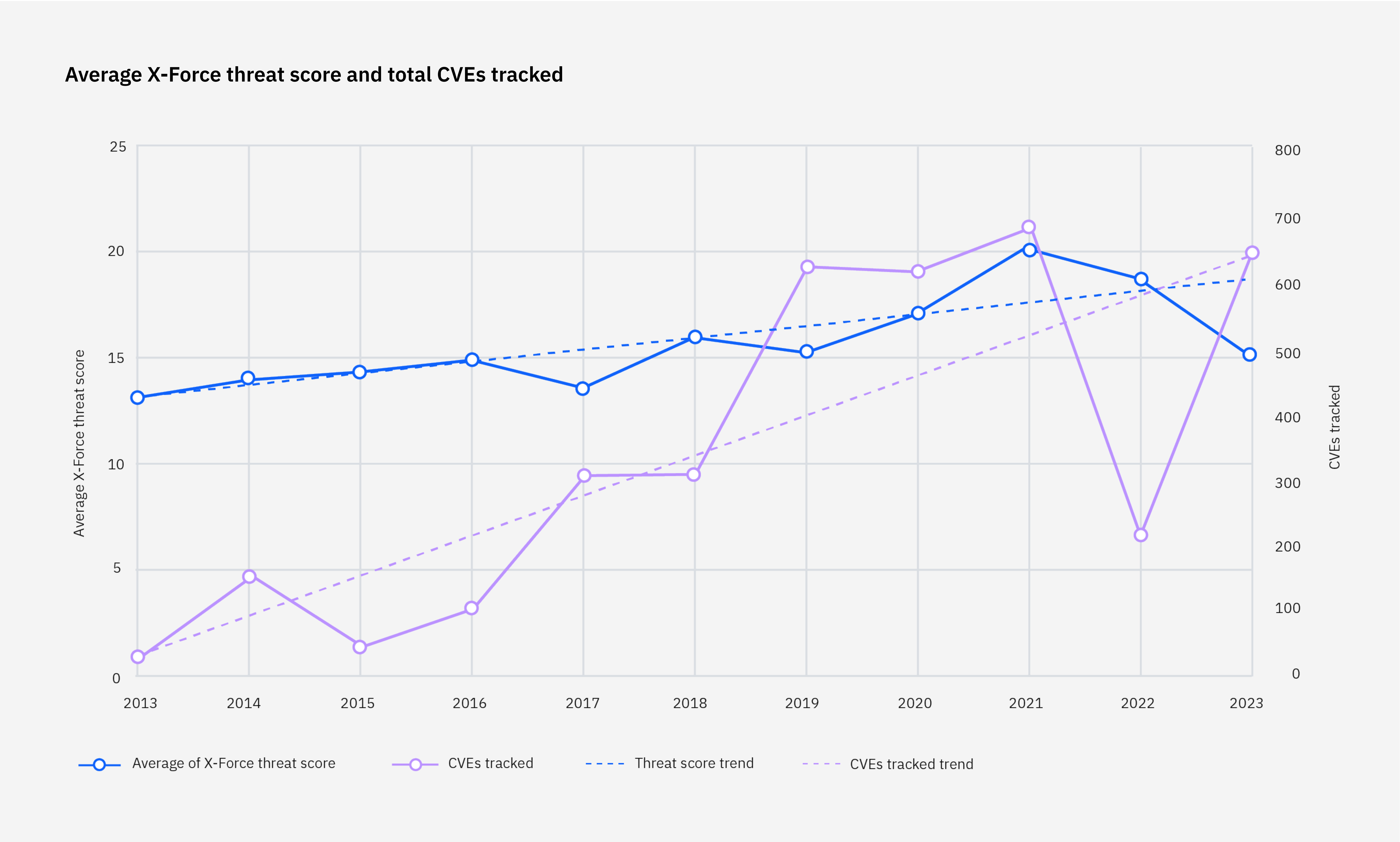
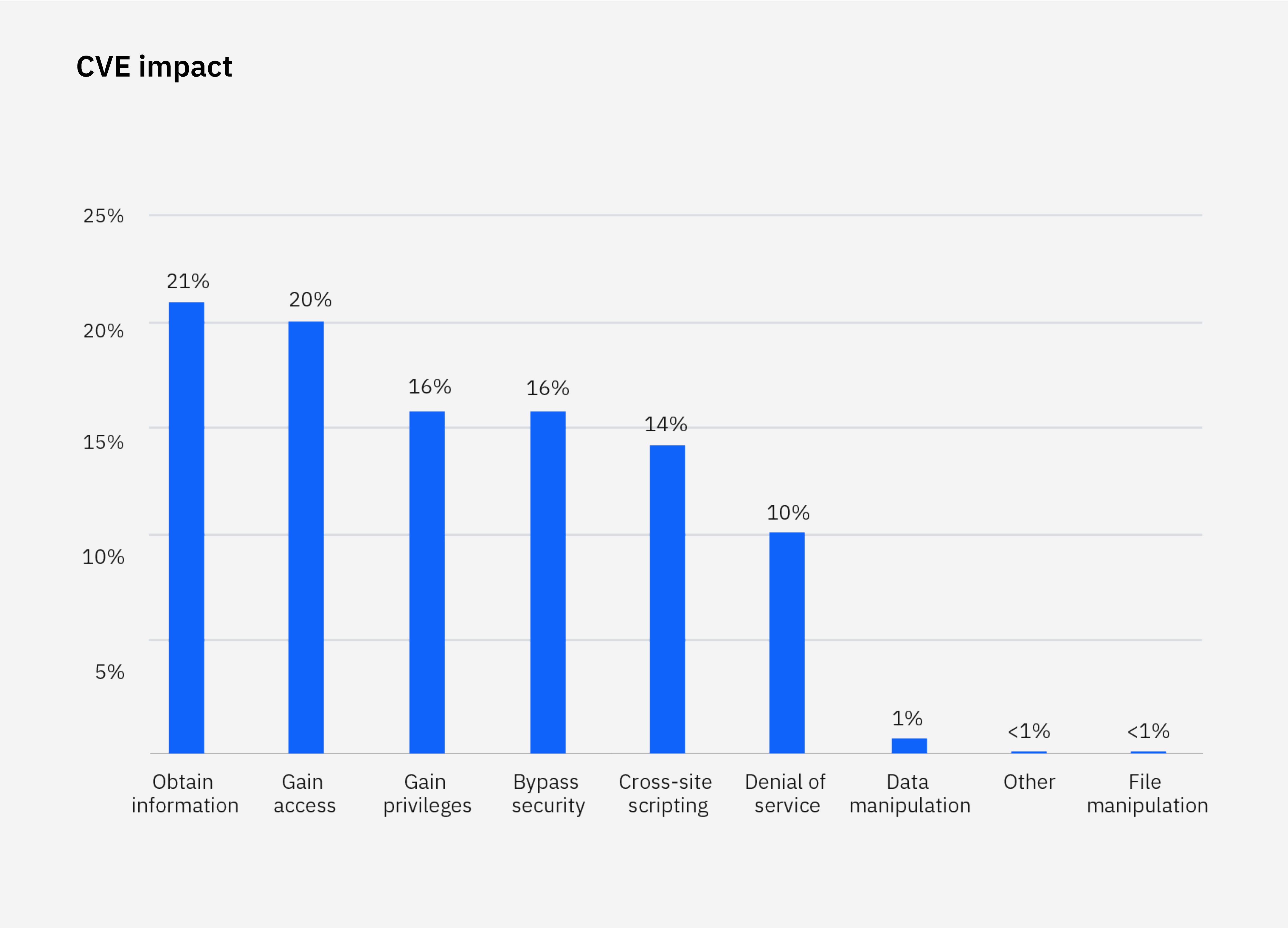


Figure 2. The total number of tracked CVEs and their average severity has increased steadily in the last decade.

As part of our analysis this year, the X-Force team categorized these new CVEs according to their potential impact if they’re successfully exploited. What we’ve observed is that obtaining information, gaining access and gaining privileges are the top three impacts of the CVEs discovered during the reporting period. Attackers often use the exploitation of a CVE as an initial access vector. Once successful, they can take advantage of this access to facilitate their ultimate objective, which can involve deploying cryptominers, ransomware and other types of malware.



CVE impact

Figure 3. Obtaining information is the number one CVE impact.

Number of cloud-related vulnerabilities the X-Force team is tracking, a number that has doubled since 2019

3,900

Percentage of new CVEs that allows an attacker to obtain information, gain access or gain privileges

57%

Cloud and the dark web

For the 2023 report, X-Force researchers analyzed data in collaboration with Cybersixgill to get insight into how cloud infrastructure is exploited on dark web marketplaces. To do this analysis, we gathered data from various dark forums and pulled some of the key insights and takeaways from our observations. The following analysis is based on X-Force dark web research from June 2022 to June 2023.

Threat actors often sell to or request compromised credentials from some of the most popular cloud-based software-as-a-service (SaaS) solutions. Doing so allows them the broadest level of access with a given set of usernames and passwords. Our research indicates that Microsoft Outlook was far and away the most mentioned SaaS solution on dark web marketplace discussions, followed by WordPress and Zoom.

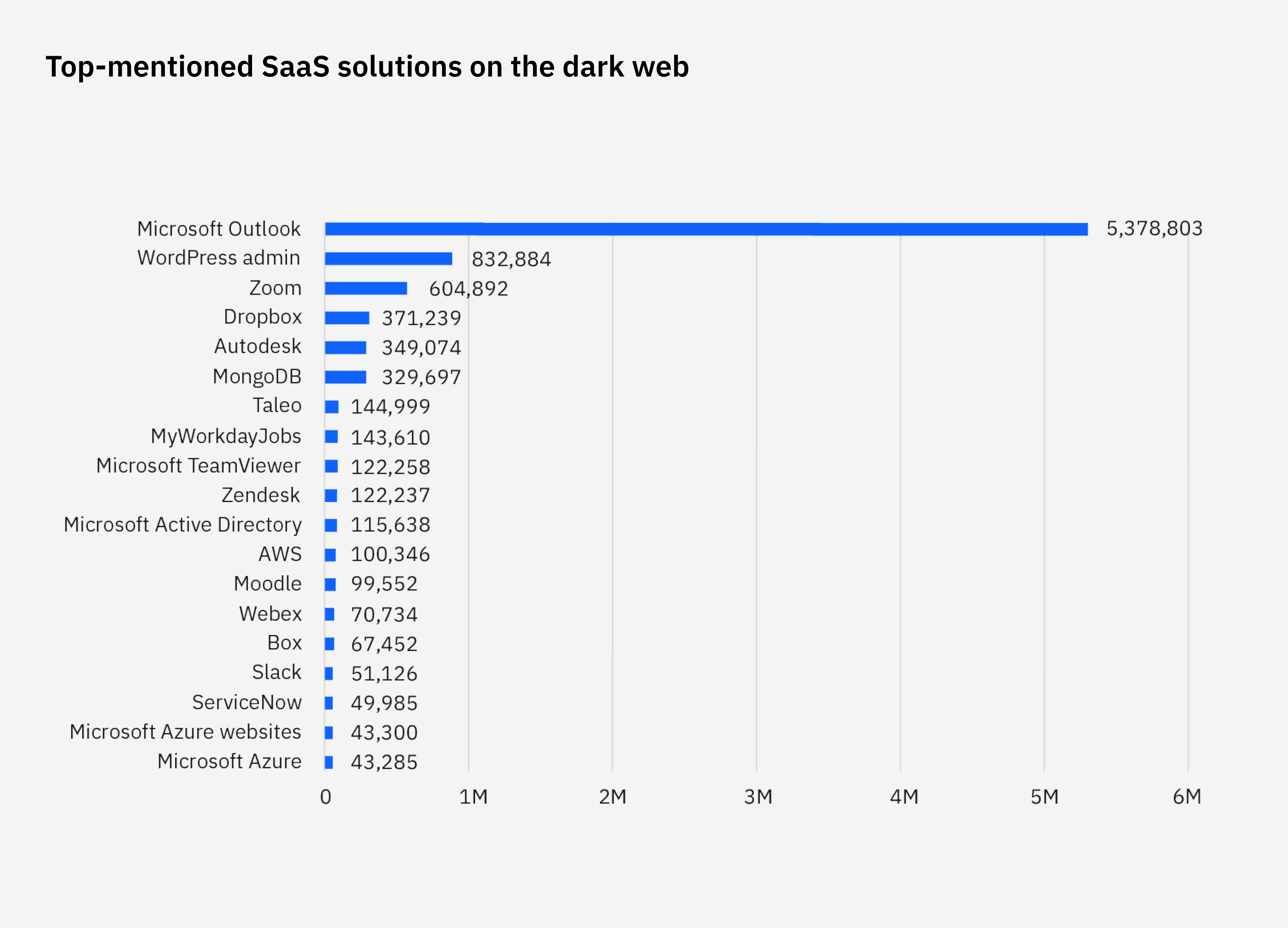

Top-mentioned SaaS solutions on the dark web

Figure 4. Top-mentioned SaaS solutions are based on dark web marketplace discussions.

Understanding what type of cloud access that threat actors are selling can help us understand how they managed to compromise accounts. Figure 5 shows the most common types of cloud access sold, according to our analysis.

Credentials: This cloud access includes login username and password combinations for cloud accounts. Credentials can also encompass a variety of additional host information pertaining to the infected system. In most cases, this cloud access includes the operating system version, IP address and other data captured by various information-stealing malware, such as additional credentials for other services. In 2023, we observed a slight decrease in pricing for credentials, from USD 11.74 in 2022 to USD 10.68 in this year's report.

Email: In the form of Simple Mail Transfer Protocol (SMTP), email accounts allow threat actors to send spam and phishing emails. Account-specific settings, such as how many daily email messages can be sent, have the potential to impact the selling price.

Shell or SSH: SSH is a protocol that allows authorized users to open remote shells on other computers. Shell access likely indicates the ability to initiate a reverse shell connection on the targeted resource.

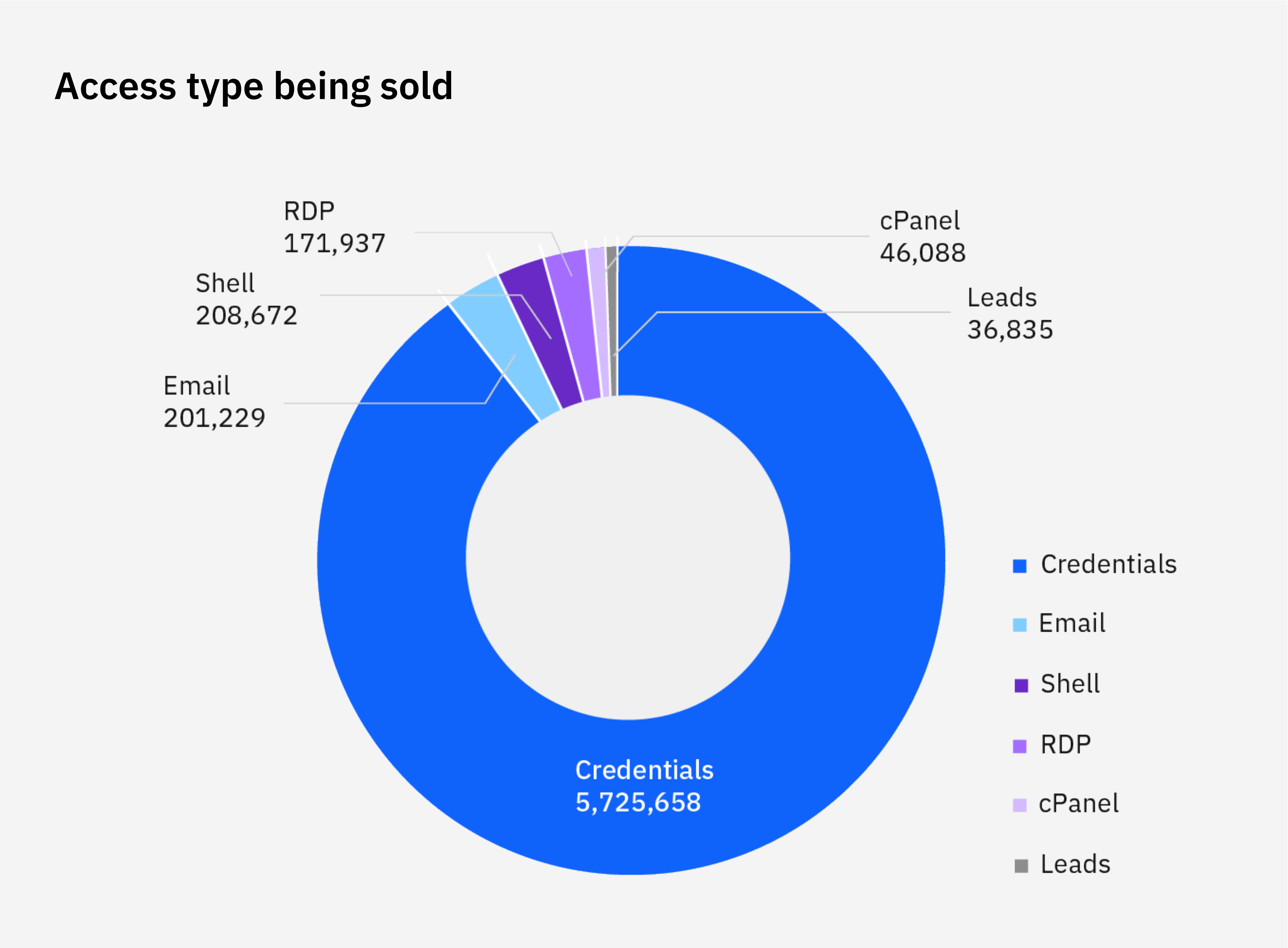


Figure 5. Credentials comprise 90% of cloud access types sold during the reporting period.

Pricing of compromised cloud accounts

Remote Desktop Protocol (RDP): RDP represents credentials for Microsoft Windows-based systems running on a cloud resource. Certain factors, such as available resources, can influence the perceived value of the account. For example, a system with more RAM and processing capability will usually demand a higher price than one with fewer resources. We observed a jump in pricing for RDP access from USD 7.98 per access in 2022 to USD 10.67 in 2023.

cPanel, also known as WebHost Manager (WHM): WHM is an administrative access tool that allows users to manage the back end of cPanel accounts. cPanel is a Linux-based graphical interface that allows a user to manage the server.

Leads: Leads represent lists of emails that attackers can use for spamming and phishing campaigns and are usually sold as is.

Threat actors use multiple marketplaces and forums to advertise items for sale on the dark web. Our analysis of postings from June 2022 to June 2023 allowed us to extract pricing information from various dark web marketplaces, as shown in Figure 6.

Average price by access type

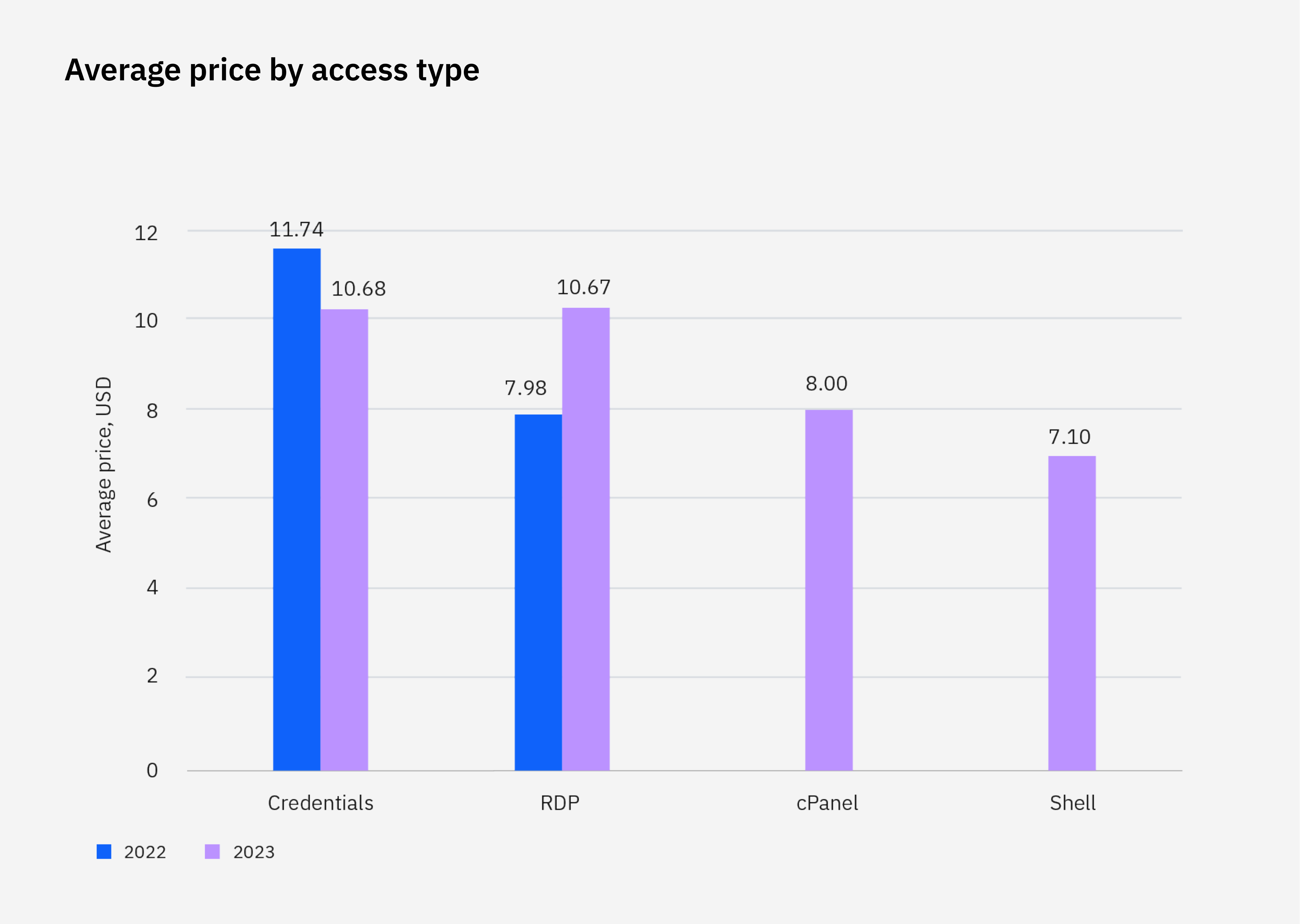


Figure 6. A jump in pricing for RDP access and a slight decrease in credential pricing were observed. Pricing data for shell and cPanel access is being reported for the first time this year.

Industry and geography significance

Although organizations across all industries and geographies are subject to the same cloud vulnerabilities and risks, we believe it's valuable to report on where we see the most incidents. Since last year, the X-Force team has seen the most cloud-related incidents occur in the media and entertainment sector, accounting for 21% of cases.

According to Nutanix's Third Annual Enterprise Cloud Index, the media and entertainment industry "leads in the exclusive use of multiple public cloud services and is ahead in deployments of hyperconverged infrastructure (HCI)."[10] This aggressive cloud adoption strategy could contribute to the high ranking of incidents, given more targets are available for attacks.

Further, Europe accounted for 64% of the incidents we responded to, which may also be a result of the high usage of cloud in this region. Per Forrester's The State of European Cloud, 2022, 87% of European enterprises use multiple public cloud platforms.[11] This percentage equates to a plethora of potential targets.

64%

Number of incidents the X-Force team responded to in Europe, among clients worldwide

Recommendations and best practices

Whether you’ve already implemented a cloud solution or are in the beginning stages of cloud migration, engaging a trusted advisor to guide your cloud security initiatives is essential. Cloud security strategy services can help you identify cybersecurity gaps and implement and manage the following recommendations.

Preparation

Testing and exercises

- Review whether your organization has the right tools and personnel for responding to a cloud breach and that your IR playbooks are specifically designed for cloud-based breaches with proactive services included in an IR retainer. If your team is smaller or missing the required skills, retain third-party services that can respond as needed.
- Perform cloud penetration testing to find and fix flaws that may expose your cloud and container environment to attackers. Manual testing can help uncover flaws that tools alone can’t find, such as misconfigurations and excessive privileges.
- Engage in adversary simulation exercises using cloud-based scenarios to train and practice effective cloud-based IR.

Monitoring

- Understand your exposure on the dark web with a brand monitoring service.
- Extend monitoring and detection capabilities to cloud environments. Determine and enable audit logging requirements in cloud environments. Use cloud-native tools and technologies to monitor malicious activity and evidence of compromise.
- Implement a solution that integrates daily automatic compliance checks into your development lifecycle to help protect customer and application data.
- Implement cloud application defenses, including controls, such as a web application firewall and vulnerability management for applications and unmanaged cloud resources.
- Know your attack surface through a solution capable of uncovering the full scope of your network and locating shadow IT infrastructure.

Data protection

- Use solutions enabling strong data protection, especially for all forms of sensitive data, to provide a deeper level of protection against unauthorized access and theft.
- Manage your secrets centrally in a single-tenant, dedicated instance using a secret management tool, such as API keys to keep and rotate secrets.

Segmentation

- Implement virtual network segmentation to restrict access to resources and reduce the risk of lateral movement in case of a compromise.
- Deploy a bastion host to isolate private cloud network zones from external, less trusted or untrusted networks, including the internet. This activity reduces the cloud attack surface and minimizes the risk of unauthorized access to cloud resources. Firewalls and load balancers can be helpful in filtering traffic in relevant gates to the cloud environment.

Reacting

- Implement a security orchestration, automation and response (SOAR) solution to help your organization with AI and automate IR and malware analysis when feasible. This process can help reduce response time and the overall average cost of breaches associated with cloud environments.
- Preserve forensic artifacts during an investigation by redeploying—not reimaging—affected machines. This approach allows for subsequent investigation into how the breach occurred and what else the threat actors may have done while in the organization's environment.
- Use security threat intelligence during an IR to take advantage of knowledge about the threat actor to speed up response times and enable more thorough response activities.

Strategies and best practices

- Use a zero trust security strategy approach to include implementation of multifactor authentication (MFA) and the principle of least privilege. This strategy is especially important for private clouds that may interact with other on-premises assets on a regular basis.
- Establish device or service activation or both along with deactivation best practices that incorporate vulnerability and policy compliance scanning and remediation through the system’s lifecycle.
- Use an open and integrated security approach when possible to help connect the dots between security data that resides across fragmented cloud environments. Consider security platforms that rely on open technologies and allow for tight integrations between tools to achieve a centralized control dashboard.
- Implement and enforce strong access control practices, including the principle of least privilege for cloud identities, MFA for privileged accounts, and accounts accessing cloud resources through federated services.
  - Modernize identity and access management (IAM) to reduce reliance on username and password combinations and combat threat actor credential theft.
  - Use AI capabilities to help scrutinize digital identities and behaviors, verify their legitimacy and deliver smarter authentication.
  - Ensure systems are regularly tested for policy compliance.
  - Automate security group privileges and new user creation to least privilege by default.
  - Remove users promptly when decommissioning and automate blocking after an idle period to minimize the risk of ghost users that can be compromised by attackers.
  - Gain visibility into cloud identities to manage permissions, identify inactive or excessive permissions, and optimize access policies to simplify meeting IAM security needs with cloud infrastructure entitlement management (CIEM).
- Implement provisioning policies and enforce rules to govern the lifecycle of deployed resources, including who can provision resources and their types, duration and placement.
  - Reduce the risk of exposing a cloud environment to external threats by using this control.
  - Use automation extensively to remove as much human error as possible.

About the IBM X-Force team

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 the age of relentless cyberattacks, a connected everything and increasing regulatory mandates, organizations need a focused security approach. The X-Force team believes threats should be the focal point. Through penetration testing, vulnerability management and adversary simulation services, the 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 X-Force IR team knows where threats may hide and how to stop them. X-Force researchers create offensive techniques for detecting and preventing threats, while the X-Force team collects and translates threat data into actionable information for reducing risk.

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

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

Contributors

- Chris Caridi
- Austin Zeizel
- Richard Emerson
- Kat Metrick
- Jeremy Khalouian
- Mohit Goyal
- Johnny Shaieb
- Patrick Adam Fussell
- Agnes Ramos-Beauchamp
- Yannick Bedard
- Scott Lohr
- Michael Mitchell
- Chris Bedell

Appendix

Threat activity report summary 1

Overview
In late 2022, the X-Force team investigated a compromised cloud environment that had an unauthorized account. A malicious actor used a compromised cloud provider account to log in and create additional users. Though the activity wasn't tied to a previously known group, some evidence suggests the actor behind the campaign may have been an Indonesian threat actor group.

Impact
The X-Force investigation revealed that the threat actor had created additional accounts and cloud instances and uploaded multiple files to those instances, including a tool to scan for compromised accounts and a text file containing previously compromised credentials. The actor also sent spam email messages from known phishing domains to multiple personal email addresses.

- **Spam emails:** One of the additional accounts created was labeled “root.” The root account was observed modifying the privileges of other accounts. This account was used to send tens of thousands of phishing emails using the actor-created email accounts “n0.reply@suivis-chronopost[.]fr” and “n0.reply@suivis-chr0nopost[.]fr.”

- **Cloud instance creation:** The root account was observed creating multiple cloud instances, pairing different keys for each. One of the cloud instances was used to download compressed files, which the threat actor decompressed and installed and then ran binaries. One of the directories created was labeled “KeyBot,” which contained multiple files that could be used to compromise other environments through CVE-2021-3129 and indiscriminately mass scan domains for certain sensitive keys for AWS, Alibaba and other cloud providers.
- **Installation of Shodan for scanning compromised accounts:** The malicious actor installed Shodan in the cloud instance by using a publicly leaked API key. There were two hacker handles noted in tools used by this threat actor: “EcchiExploit” and “KangKlepfound.” Coincidentally, EcchiExploit has self-identified as an Indonesian black hat hacker, and some of the observed infrastructure belonged to Telkom Indonesia.

Resolution
Based on observations during remote analysis, the X-Force team provided these recommendations:

- **Remove compromised access keys, malicious key pairs and email addresses:** During the investigation, the X-Force team found one compromised cloud provider access key, three key pairs created by the malicious actor, and email addresses within the CloudTrail logs verified by a compromised account.
- **Reset passwords and implement MFA:** The X-Force team strongly recommended that the compromised accounts have their passwords reset, along with MFA enabled as priority, and then all accounts phased to have MFA enforced. Additionally, credentials should be audited and rotated periodically.
- **Implement principle of least privilege:** During the investigation of logs, the X-Force team noted that the root account was used to perform many tasks. It was also very easy for the malicious actor to gain a high level of privilege within the cloud environment. If higher privilege is needed for a task, it should be granted and removed once the task is complete. This process will mitigate the risk to the cloud environment by users not having unnecessary permissions.

Threat activity report summary 2

Overview
In 2Q 2023, the X-Force team responded to a Makop (Phobos) ransomware incident involving a Windows server running on a cloud instance with the RDP exposed. The threat actor was able to access the system over an RDP session, possibly by brute-force attempts, ultimately leading to the deployment of the Makop ransomware and a ransom note requesting contact to multiple email addresses.

Impact
In addition to Makop ransomware, the X-Force team found evidence of a Laplas Clipper infostealer and Phonk cryptocurrency miner installations on the server. Although the same compromised account was involved in all malicious activity, it's unclear if the same threat actor was responsible for deploying all aforementioned malware on the compromised system.

- **RDP and brute force:** The threat actor gained initial access to the environment through a successful RDP connection using a valid account. Throughout the duration of this malicious activity, the Windows server experienced tens of thousands of password brute-force attempts, including over a thousand attempts targeting the account that was compromised and used during the incident.
- **Ransomware deployment:** The threat actor linked to the incident has been assessed as "Phobos/Makop," an opportunistic ransomware group that typically attempts to extort money by offering a decryption key for compromised data. Threat actors encrypted victim files, and the MKP extension was affixed to impacted filenames. A ransom note was also provided that included the following threat actor contact email addresses: datastore@cyberfear[.]com and back2up@swismail[.]com. This threat actor doesn't maintain a data leak site, and the X-Force team didn't identify evidence of data exfiltration or attempts at lateral movement.

- **Additional files downloaded:** On the same day as the first connection, a threat actor executed multiple file downloads using Microsoft Background Intelligent Transfer Service (BITS). The compressed file in this instance contained the executable “settings.exe,” which was executed by the bat script, ultimately dropping “GQGYSQ.exe.” The file “GQGYSQ.exe” was identified as the Phonk cryptocurrency miner. Over 24 hours later, a threat actor used BITS to download two additional files. Once executed, these files dropped another file, “ntlhost.exe.exe,” a version of Laplas Clipper infostealer. Laplas attempts to redirect cryptocurrency payments to a threat actor-controlled wallet by switching cryptocurrency addresses identified in the clipboard.

Resolution
Based on observations during remote analysis, the X-Force team provided several recommendations, such as:

- **Block IP addresses, hashes and domains:** The investigation identified numerous file-based indicators of compromise (IOCs).
- **Reset passwords and rebuild impacted system:** Passwords of all users on the impacted machine should be reset and password reuse should be identified elsewhere in the environment. The impacted system should be rebuilt and restore only the data that has been scanned and verified to be clean and trusted.
- **Employ server security best practices:** Block internet access to all ports that aren’t required for the server’s core purpose. Allow server management only through a secure jump host on the internal network subnet. Install an endpoint detection and response along with antivirus on the newly deployed system and verify that it’s monitored by your security team and properly integrated with your security information and event management (SIEM) solution.

1. Cost of a Data Breach Report 2023, Ponemon Institute and IBM Security®, July 2023.
2. Valid Accounts: Cloud Accounts, MITRE ATT&CK, 21 March 2023.
3. Exploit Public-Facing Application, MITRE ATT&CK, 14 April 2023.
4. Phishing: Spearphishing Link, MITRE ATT&CK, 11 April 2023.
5. Log4j - Initial Access to the Cloud, Palo Alto Networks, Inc., 21 March 2022.
6. Proxyjacking has Entered the Chat, Sysdig, Inc., 4 April 2023.
7. CVE-2021-21974, The MITRE Corporation, 4 January 2021.
8. Generic malware includes loaders and downloaders that aren't explicitly tied to one specific malware family.
9. The X-Force team uses a multifaceted ranking algorithm to prioritize and score the severity of vulnerabilities with a risk score that uses factors such as ease of use, level of access granted and impact on the affected system. This information is inserted into a risk formula that scores the threat based on the Common Vulnerability Scoring System (CVSS), the potential damage possible, difficulty and utility to an attacker.
10. Cloud Migration a Top Priority for Media and Entertainment Industry, Spiceworks Inc., 9 November 2021.
11. Cloud Usage Is Alive And Well In The European Cloud Market, Forrester, 19 July 2022.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
September 2023

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.