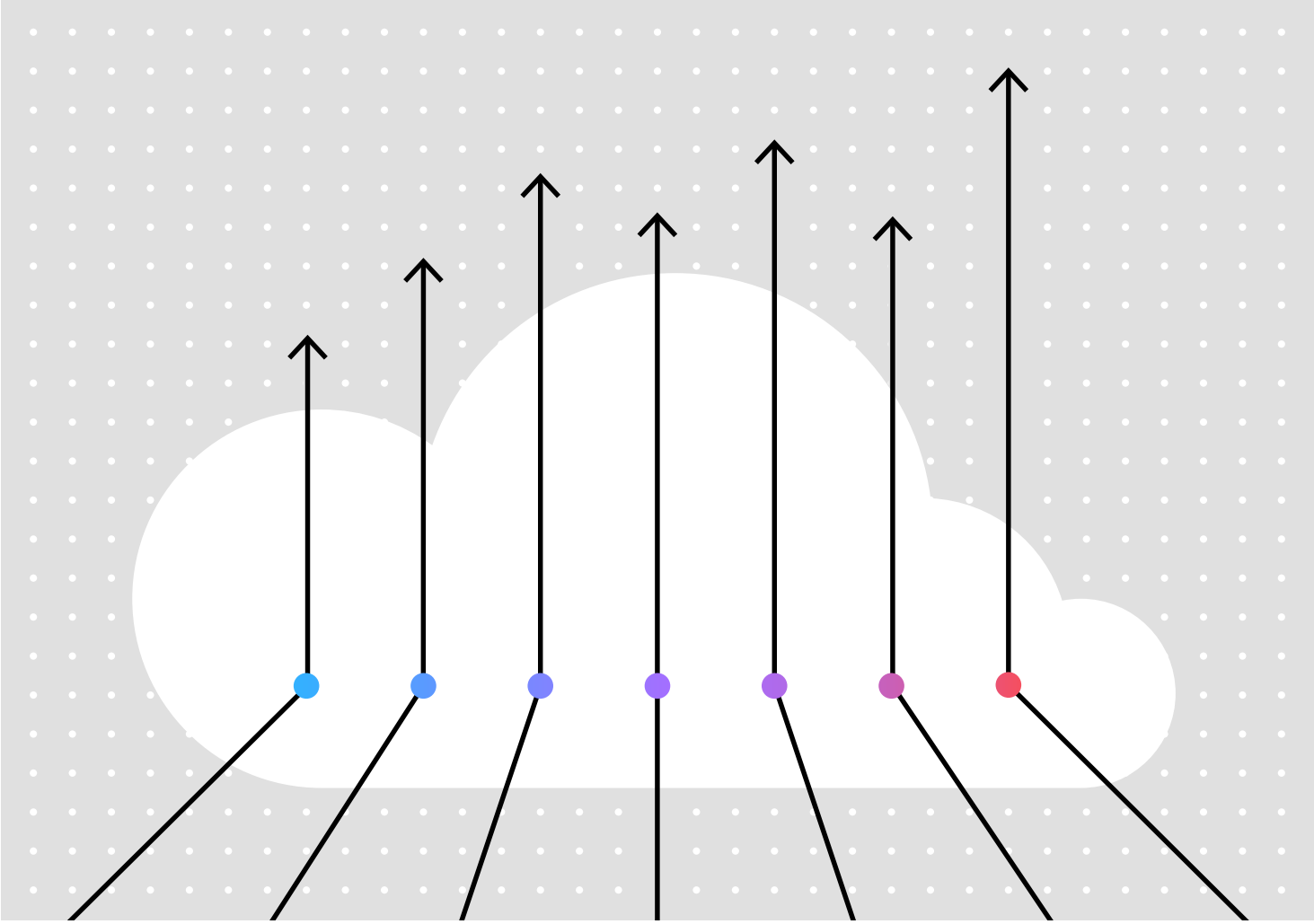
IBM **Security**

2022 IBM Security X-Force Cloud Threat Landscape Report



IBM

Table of contents

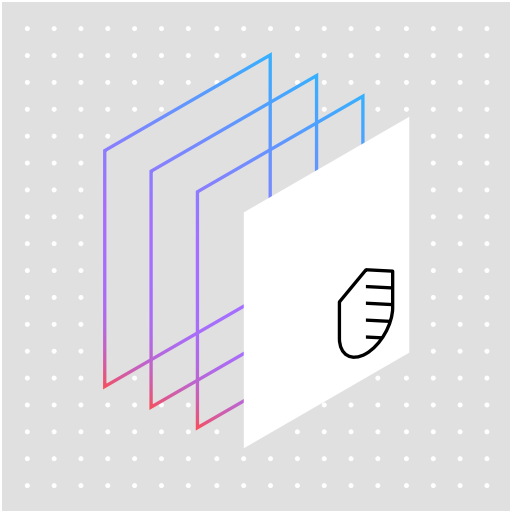
Introduction

As organizations continue to migrate to or manage their private, public, hybrid cloud or multicloud environments, security should be an integral part of the process. Unfortunately, embedding security in every step of your organization's cloud journey can be challenging. For this reason, IBM Security® X-Force® produces the Cloud Threat Landscape Report, now in its third 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, X-Force reviewed data compiled between July 2021 through June 2022 and gleaned from the following sources:

- IBM Security X-Force Threat Intelligence
- IBM Security X-Force Red penetration tests
- X-Force incident response (IR) engagements
- Dark web insights from X-Force analysis
- Intelligence provided by report contributor Intezer

Our findings reveal the various ways we've observed threat actors compromising cloud environments and what types of malicious activity are pursued once they're inside. Additionally, organizations learn how they can prepare and react to security incidents involving their cloud environments more effectively.



99%

of the cases analyzed, cloud identities have been found to be excessively privileged

↑28%

increase in new vulnerabilities compared to last year

↑200%

increase in cloud accounts being advertised on the dark web

Key takeaways

Excess privilege is a concerning problem in the cloud

– Data from the X-Force Red penetration testing indicates that in 99% of the cases analyzed, cloud identities have been found to be excessively privileged. This setup allows any attacker who gains a foothold in the environment to pivot and move laterally to exploit additional cloud components or assets.

Vulnerability exploitation leads the way

– 26% of X-Force IR engagements involving successful cloud compromises were a direct result of an exploited vulnerable application.
– Cloud vulnerabilities continue to surge. As of this publication, X-Force has tracked over 3,200 cloud-related vulnerabilities, which represents a 540% increase in the last six years, and a 28% increase in new vulnerabilities compared to last year.

The average severity of cloud vulnerabilities has been steadily increasing

– In addition to more vulnerabilities to track and fix, X-Force Red data indicates that overall, these threats are also increasing in severity.
– Threat severity has increased from an average score of 15 in 2012 to an average IBM risk score of 18 over the past 12 months.

X-Force observed over 100,000 cloud accounts being advertised on the dark web

– That amount is more than a 200% increase over what was found in the 2021 analysis.

Threat actors are selling access through Remote Desktop Protocol (RDP) and credentials

– X-Force analysis of dark web markets shows that 76% of cloud account sales are in the form of RDP access. Another 19% comes in the form of compromised credentials to cloud accounts.
– The average sale price in a cloud-related transaction is USD 10.27.
– Stolen or compromised credentials demand a 47% higher selling price than RDP access.

Threat actors continue investing in cloud targeting

– Cryptominers and ransomware remain the top dropped malware into cloud environments.
– Based on X-Force data, Monero cryptominers appear to be the most widely deployed, namely XMRig.

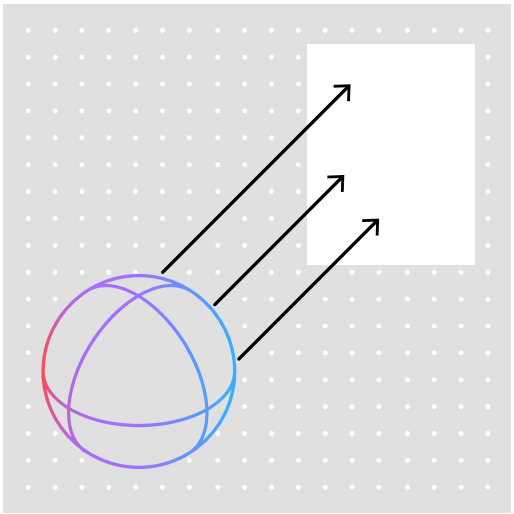
IBM Security X-Force incident response insights

The IBM Security X-Force IR team reviewed engagements involving cloud-related incidents over the past year and identified the following most common attack vectors and industry trends impacting cloud infrastructure:

Scanning for and exploiting vulnerable infrastructure was the most commonly observed initial access vector in cloud environments, based on X-Force responding to related cases. This vector represented the initial infection vector for 26% of cloud incidents. Stolen credential use was the second most observed at 9%.

Manufacturing led all industries with 21% of all cloud-related incidents that X-Force responded to in the past year. This trend matches what we see in other areas of the cyberthreat landscape such as ransomware targeting.

Every geographic region of the world experienced cloud attacks. Our IR experience reflects that threat actors have significant and growing cloud expertise. With few exceptions, these threat actors operate unconstrained by a client's cloud hosting preferences, rules of law or any physical geographic boundaries.



Initial access vectors

Exploitation of public-facing applications
Vulnerable public-facing applications running in a cloud environment are common targets for threat actors. Organizations face the difficult task of cataloging all applications running in an environment and helping to ensure all remain patched and appropriately monitored. X-Force routinely observed threat actors making use of bulk vulnerability scanning for exploitation in cloud environments. The Log4j vulnerability and a vulnerability in VMware Cloud Director were two of the more commonly leveraged vulnerabilities in IR engagements.

Log4j: The Log4j vulnerability had a significant impact across all sectors due to the Apache Log4j library being widely deployed among cloud services and within the infrastructure of major cloud providers. Additionally, the Log4j vulnerability, disclosed in December 2021, was quickly used by malicious actors.

- Linux® malware families were early exploiters of Log4j, including B1txor20, Elknot, Kinsing, Mirai, Muhstik and Monero cryptominers.
- Ransomware groups such as Conti and NightSky also exploited the Log4j vulnerability.

VMware: VMware Cloud Director allows providers to operate and manage their cloud infrastructure to gain visibility into data centers across sites and geographies. A vulnerability in Cloud Director (CVE-2022-22966) allows an attacker to perform remote code execution to gain access to servers. This vulnerability can potentially expose sensitive data and lead to a loss of control of private clouds within an infrastructure. Interestingly, many of the major vulnerabilities that were heavily exploited in the past year primarily affected the on-premises version of applications, sparing the cloud instances. Examples include the Microsoft Exchange ProxyShell/ProxyLogon vulnerabilities as well as the Atlassian Confluence vulnerability (CVE-2021-26084).

Misconfiguration missteps lead to brute force
According to Intezer, another common access vector into cloud environments is misconfiguration. Research points to the risks behind misconfigured workflow management platforms, including Apache Airflow and Argo Workflows. Each platform has its own security challenges, and Intezer discovered thousands of exposed credentials, sensitive data and cryptojacking campaigns.

The danger of leaked credentials is that threat actors can use them to gain unauthorized access to cloud environments. The attackers then have the permissions of the exposed credentials, essentially allowing them to infiltrate the organization while staying undetected. X-Force IR data revealed that many cloud intrusions were the result of some form of brute force attack. Some examples include credential stuffing and password spraying.

Attacker objectives: Cryptomining and sometimes extortion

X-Force data analysis allowed us to determine common actions that threat actors took upon successful compromise of cloud environments. These observations generally mirror the trends observed and reported in the 2021 X-Force Cloud Threat Landscape Report. While cloud environments have been targeted for attempted data extortion, much of the threat activity appeared to be concentrated on using compromised access to cloud resources for cryptomining.

Why threat actors choose the cloud to mine
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 leveraging compromised infrastructure, threat actors can transfer the cost onto the victim.
2. Actors may count on cloud resources receiving less thorough and 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.

Based on X-Force data, threat actors showed a preference for Monero cryptominers. The top cryptominer observed was XMRig, which was delivered through a variety of methods, including malicious shell scripts and Kinsing malware.

Notable threat actors targeting cloud for cryptomining
A few notable groups have been observed within the past year that emphasize cryptominer distribution. X-Force observed activity involving the Rocke Group, a threat group that deploys Monero miners to compromised cloud environments.

X-Force also observed multiple compromises of cloud infrastructures by the Outlaw Group. This group was first observed in 2020 and appeared to go dark, but reemerged in 2022. Outlaw has several tools in its arsenal, including IRC shellbots, XHide and the XorDDoS Linux rootkit, and has been deploying XMRig cryptomining malware on compromised cloud infrastructures.

Other notable groups targeting cloud environments include publicly reported campaigns of the following threat actors:

- TeamTNT, which targets cloud infrastructure
- LemonDuck, which targets Docker cloud instances
- Denonia cryptominer, which targets AWS Lambda
- CoinStomp, which as of this publication primarily targets cloud service providers in Asia

Exfiltration, extortion and data destruction
X-Force also observed cases in which threat actors targeted cloud environments after compromising enterprise networks. In some cases, this targeting takes place in parallel to a ransomware infection or as a standalone effort to gain access to data that's being stored using cloud solutions. Threat actors with this access may threaten or choose to exfiltrate, leak or destroy the data.

Excessive privilege aiding lateral movement

X-Force Red found that in 99% of cloud penetration tests conducted in 2021, cloud identities, meaning human users and service accounts, were excessively privileged. This setup enabled attackers who managed to get a foothold in the environment to pivot and move laterally to exploit additional cloud components or assets. Excessively privileged users can be defined as ones who have more permissions than they need to do their job or task.

Excessive permissions was part of the most common misconfiguration X-Force Red observed in cloud penetration tests conducted in the last year. Joining excessive permissions was poor cloud account application programming interfaces (API) access policies, which lack multifactor authentication (MFA) or password policies or both. Insufficiently protected public assets, such as public storage buckets, internet-facing databases with poor authentication controls and overly permissive network access rules or unpatched systems also showed up in this year's penetration tests.

An expanding attack surface: Cloud vulnerabilities

X-Force Red Vulnerability Management Services (VMS) provides insights on known vulnerabilities in cloud environments. X-Force is currently tracking over 3,200 cloud-related vulnerabilities, a 540% increase in the last six years. Year-over-year shows a roughly 28% increase in new vulnerabilities compared to our 2021 report, as shown in Figure 1.

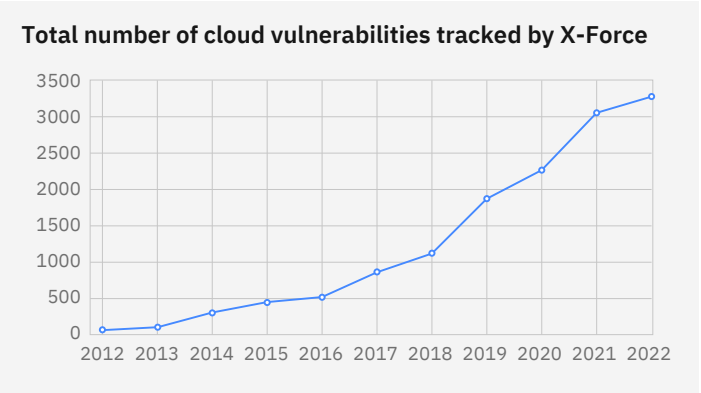


Figure 1. The number of tracked cloud vulnerabilities has grown exponentially in the last decade.

It stands to reason that as the number of available cloud-based applications rises, more cloud-related vulnerabilities will be disclosed, which increases the overall attack surface for cloud environments. Not all vulnerabilities are created equal, however.

When it comes to prioritizing vulnerabilities, X-Force Red uses a multifaceted ranking algorithm to score the severity of vulnerabilities with a "risk score." The risk score uses a variety of factors, such as ease of use, level of access granted and impact on the affected system, to accurately measure vulnerabilities.

This information is inserted into a risk formula that scores the threat based on the Common Vulnerability Scoring System (CVSS) score, the potential damage possible, difficulty and utility to an attacker.

X-Force Red data shows that the average threat score over the past decade has steadily been increasing. A huge uptick has occurred in the total number of cloud-related Common Vulnerabilities and Exposures (CVEs) being tracked. The average threat score for the past one year is 18, compared to 15 in 2012.

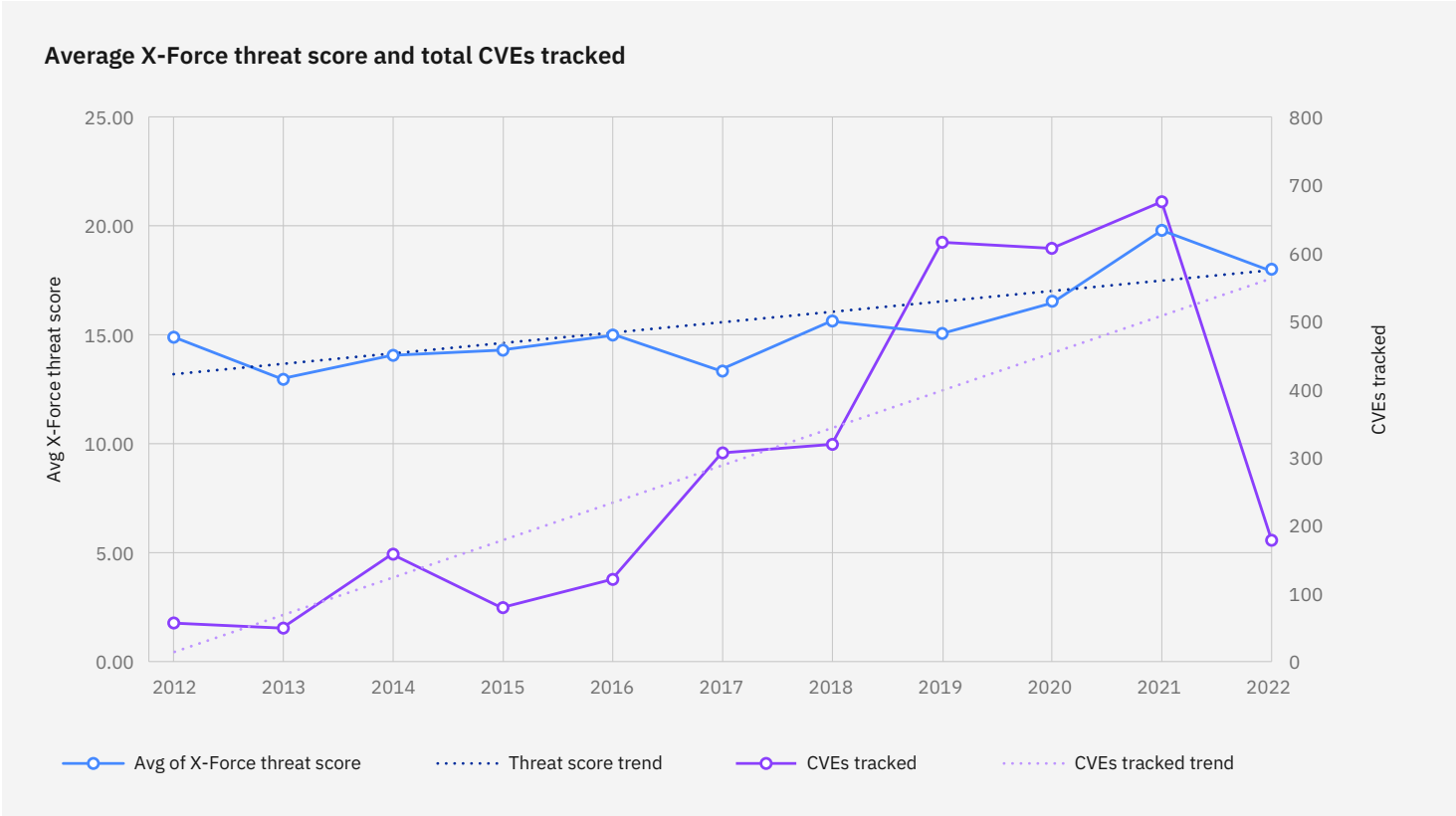


Figure 2. The total number of CVEs tracked and the average severity have increased steadily in the last decade.

Dark web and cloud

X-Force researchers regularly gather intelligence from the dark web to better understand the environment where threat actors typically trade. Various forums and marketplaces exist where access to cloud accounts are requested, traded and sold to the highest bidder.

The following analysis is based on X-Force dark web research from June 2021 to June 2022. During this timeframe, X-Force observed over 100,000 cloud accounts being advertised on the dark web—a more than threefold increase of 200% over what we observed during the previous year. Cloud accounts are advertised for nearly all cloud service providers, with AWS and Azure Cloud together representing 90% of observed compromised cloud accounts for sale.

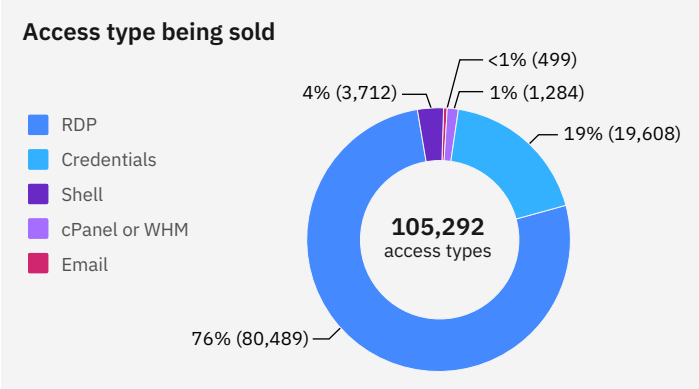


Figure 3. RDP makes up more than three-fourths of cloud access sold over a 12-month period.

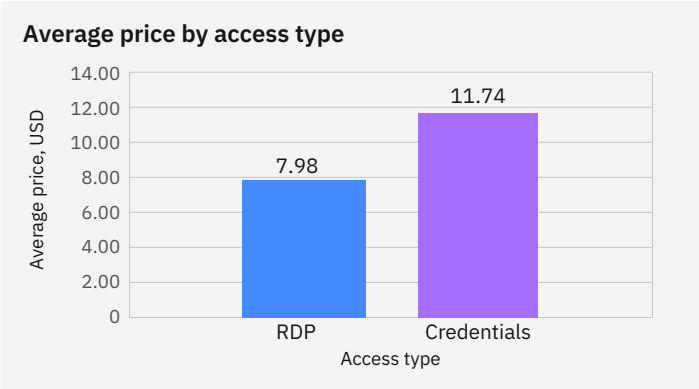


Figure 4. A notable difference exists between demands of pricing for RDP compared to credentials.

Understanding what type of cloud access that threat actors are selling can help us understand how they managed to compromise accounts. Figure 3 shows the most common types of cloud access sold, according to our analysis.

RDP: RDP represents credentials for 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 when compared to one with lesser resources.

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.

Shell: Shell access likely indicates the ability to initiate a reverse shell connection on the targeted resource.

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

cPanel, also known as WebHost Manager: WebHost Manager (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 an end user to manage the server.

Pricing of compromised cloud accounts

Threat actors use multiple marketplaces and forums to advertise items for sale on the dark web. Our analysis of postings from June 2021 to June 2022 allowed us to extract pricing information from various dark web marketplaces, as shown in Figure 4.

The average prices as described in this graphic came from analysis of over 52,000 forum postings across multiple dark web marketplaces. This review allowed us to compare prices between two of the most common access types: credentials and RDP. We observed that login credentials demand a higher price than RDP access by approximately 47%. One reason for this difference is likely because postings that advertise credentials often include multiple sets of login data, potentially from other services that were stolen along with the cloud credentials.

Recommendations for preparation and response to cloud breaches

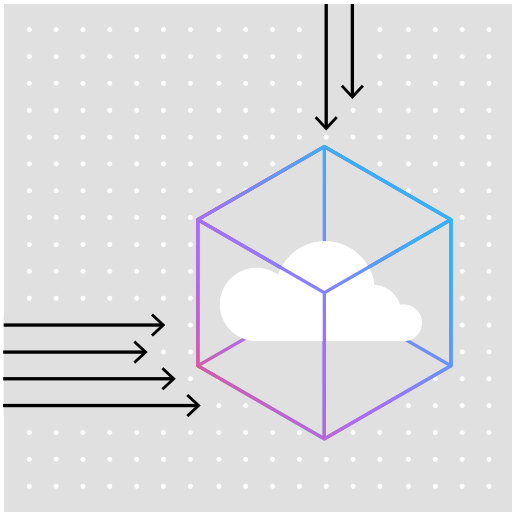
Whether you've already implemented a cloud solution or are in the beginning stages of cloud migration, engaging a trusted advisor to guide your cloud security initiatives is essential. IBM Cloud Security Strategy Services can aid in identifying cybersecurity gaps and help implement and manage the following recommendations:

Preparation

- Extend monitoring and detection capabilities to cloud environments with IBM Security QRadar XDR Connect. Determine and enable audit logging requirements in cloud environments. Use cloud-native tools and technologies to monitor malicious activity and evidence of compromise with products like IBM Cloud Security and Compliance Center.

- Utilize an IBM zero trust security strategy to include implementation of 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.

- Consult X-Force Red Cloud Penetration Testing Services 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 X-Force Red Adversary Simulations Services to perform exercises using cloud-based scenarios to train and practice effective cloud-based incident response.

- Establish device or service activation, or both, and deactivation best practices that incorporate vulnerability and policy compliance scanning and remediation through the system's lifecycle.

- Where possible, use an open and integrated security approach, which can 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, such as IBM Cloud Pak® for Security.

- Implement virtual network segmentation to restrict access to resources and reduce the risk of lateral movement in the case of a compromise.

- Use solutions enabling strong data protection, such as IBM Cloud Hyper Protect Crypto Services and IBM Security Guardium Data Protection especially for all forms of sensitive data, to provide a deeper level of protection against unauthorized access and theft.

- 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.

- Implement cloud web application defenses, including controls, such as a web application firewall and vulnerability management for applications and unmanaged cloud resources.

- 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.

  - 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.

  - Modernize identity and access management (IAM) with IBM Security IAM solutions to reduce reliance on username and password combinations and combat threat actor credential theft.

- Implement provisioning policies and enforce rules to govern the lifecycle of deployed resources, including who can provision resources and their types, duration and the placement of those resources.

  - This control is necessary to reduce the risk of exposing a cloud environment to external threats.

  - Use automation extensively to remove human error as possible.

- Review if 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 IBM Security X-Force Incident Response Retainer. If your team is smaller or missing the required skill, retain third-party services that can respond as needed.

Reacting

- Implement IBM Security QRadar SOAR to help your organization with AI and automate incident response and malware analysis when feasible. This process can help reduce response time and 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 IBM Security Threat Intelligence during an incident response to use knowledge of the threat actor to speed up response times and enable more thorough response activities.

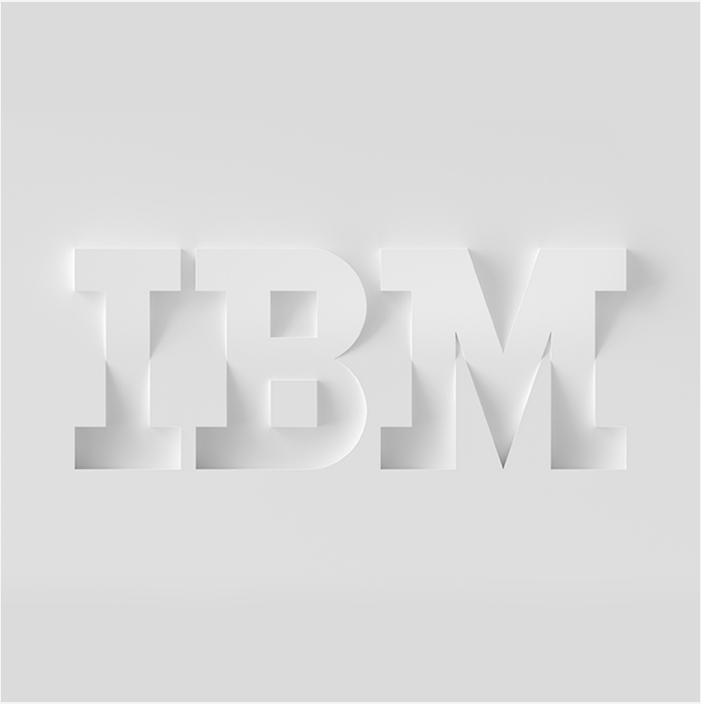
About IBM Security X-Force

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. X-Force believes the threat 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 analysts with X-Force 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 in strengthening your cloud security posture, schedule a one-on-one consultation with an IBM Security X-Force expert.



Contributors

Chris Caridi

Richard Emerson

Charlotte Hammond

Kat Weinberger

Agnes Ramos-Beauchamp

Dimitris Vassilopoulos

Yannick Bedard

Scott Lohr

Scott Moore

Mark Robinson

Jason Deyalsingh

Chris Bedell

Johnny Shaieb

Intezer

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
September 2022