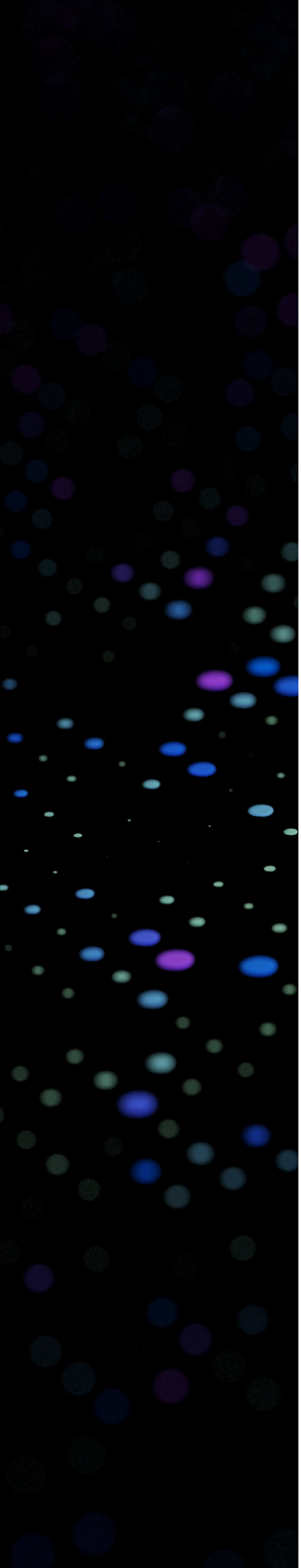


X-Force

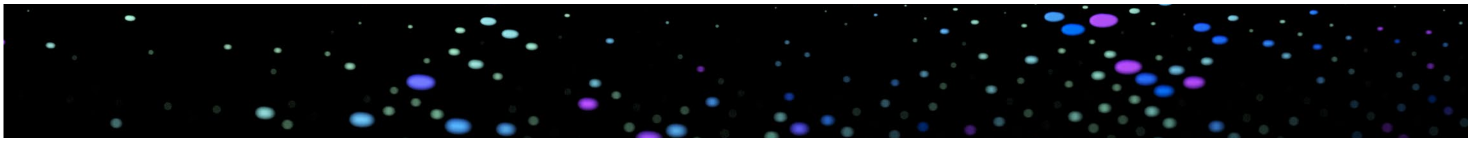
2021 IBM Security X-Force Cloud Threat Landscape Report

IBM Security X-Force Threat Intelligence

Special Intelligence Report

IBM

Table of contents



Introduction

In 2020, IBM Security X-Force produced a report containing exclusive research and data on ground-truth statistics surrounding threat actor targeting of cloud environments. Cloud adoption continues to thrive, providing convenience, cost savings, and near-permanent uptimes for organizations compared to on-premises infrastructure.

At the same time, threat actors continue to target cloud environments regardless of organization size, and shifting to a cloud model requires a specialized approach different from that of traditional deployments. A key factor to successful deployment—and management—of cloud environments is understanding how threat actors target them, what motivates them, and how to avoid common pitfalls that leave the cloud vulnerable.

This year, we have augmented our 2020 report with new and more robust data spanning Q2 2020 through Q2 2021. Data sets we used include dark web analysis, IBM Security X-Force Red penetration testing data, IBM Security Services metrics, X-Force Incident Response analysis and X-Force Threat Intelligence research. These multiple data sources help us better understand how threat actors are getting into cloud environments, what types of malicious activity are pursued once they're inside and how organizations can prepare and react to security incidents involving their cloud environments more effectively.

Key takeaways

Cloud environments need to be better secured

Cloud accounts/resources on the dark web: A thriving dark web market exists for public cloud access, with advertisements for tens of thousands of cloud accounts and resources for sale.

— In 71% of cases, threat actors offered Remote Desktop Protocol (RDP) access to cloud resources, enabling attackers to have direct access and conduct malicious activity.

— In some cases, account credentials to access cloud environments were being sold for a few dollars.

Passwords & Policies: 100% of X-Force Red penetration tests of cloud environments found issues with either passwords or policies.

Hardening systems: Based on X-Force research, two thirds of cloud breaches would likely have been prevented by more robust hardening of systems, such as properly implementing security policies and patching systems.

Cloud vulnerabilities surge: Almost half of the more than 2,500 disclosed cloud-related vulnerabilities recorded to date were disclosed in the last 18 months. While some of this growth can be attributed to better tracking (cloud vulnerabilities were added to MITRE's CVE standards in January 2020), this steep growth emphasizes the importance of closely managing this growing risk as more vulnerabilities are exposed.

Key takeaways

Threat actors target cracks in the armor

Public API policies represented a significant security gap. Two-thirds of the incidents analyzed involved improperly configured Application Programming Interface (APIs), based on analysis of X-Force Incident Response data of impacted clients.

One of the top attack vectors X-Force observed targeting cloud was threat actors **pivoting from on-premises environments into cloud environments**. This lateral movement was seen in almost a quarter of incidents X-Force responded to in 2020.

IBM estimates that over half of cloud breaches occurred due to “**shadow IT**”, emerging via unauthorized systems spun up against security policies which likely lacked vulnerability and risk assessments, as well as hardened security protocols.

Threat actors continue investing in cloud targeting

Cryptominers and ransomware remain the top dropped malware into cloud environments, accounting for over half of detected system compromises, based on the data analyzed.

Threat actors are continuing to pursue clouds in their malware development, with new variants of old malware focusing on Docker containers, as well as new malware being written in programming languages, like Golang, that run cross-platform.

A thriving dark web market for cloud access

IBM investigated dark and deep web sales of access to cloud accounts, and the results were sobering. Tens of thousands of accounts and resources were potentially offered for sale on multiple dark web markets. The vast majority of these sales were on markets automatically populated by different info-stealers and malware opportunistically compromising victims and offering credentials for sale. This bevy of compromised cloud resources highlights how readily available these platforms are for threat actors to use for a variety of malicious purposes.

The following analysis is based on IBM's dark web research, which, by its nature, is ever-changing. However, these data points are representative of IBM's insights from reviewing multiple dark web marketplaces from July 2020 through July 2021.

IBM research uncovered that some cloud accounts are more valuable than others, and the following data can help organizations better assess risk by understanding how valuable their cloud environments may be to cybercriminals and estimate the likelihood they could be attacked through them.

Many cloud accounts for sale, but not all created equal

Within the timeframe noted above, X-Force research found almost 30,000 cloud accounts potentially for sale on dark web marketplaces. Threat actors use a variety of commodity and open-source info-stealers and malware to populate the marketplaces listing the majority of these cloud accounts, making it difficult to assess how many actors support this activity.

Outside of the botnet-populated markets, cloud account advertisements in other dark web forums show prices that range from a few dollars to over $15,000 per account access credentials, based on a variety of factors. Those that appear to impact value of accounts for sale include amount of credit on the account, geography and level of account access to the organization that owns that account (root access versus less privileged users).

Looking for cloud credits

A number of cloud-related advertisements on the dark web involved selling cloud accounts that had access to account credits. Cloud account credits are monetary value associated with the account that can be used to buy additional computing resources from the cloud provider. For example, an organization may have a cloud account with a given provider and fund it with $1,000 worth of credits to have the flexibility to quickly scale resources as needed.

On average, the price tag for cloud access rose an extra $1 for every $15-30 in credit the account held. An account with $5000 in available credit would be worth about $250 (a ratio of 20:1). The scheme of account access pricing is similar to the sale of fraudulent access to bank accounts, whose value increases the more money a victim has in the account.

Threat actors may buy these compromised accounts for a fraction of the credit they hold and use them to host their own attacks. Their gain is twofold: they reduce costs, and they host malicious activity on otherwise legitimate resources which are less likely to have been blacklisted or blocked.

Low-cost access, potential for high impact

The low price of cloud accounts with high credit value could be the result of a few possibilities. There could be a large supply, or conversely a low demand, for cloud accounts in the dark web market ecosystem. Alternatively, the rate of monetization for credited accounts could be low, making the value of the accounts similarly depressed. Another reason could be the risk to the buyer should the cloud provider or victim discover the account is compromised and restrict access to the account. Finally, it is also easy to open some accounts with some monetary amount of credits, reducing the value of the labor put into acquiring these accounts. Interestingly, threat actors often offer warranties on sold access, promising a refund if the access is no longer available 7 or 14 days after sale, indicating access may not have a long lifespan.

Beyond using cloud environments to launch and scale attacks, stolen accounts can also help attackers gain the initial foothold in an organization's overall environment and plot lateral movement across other parts of their networks and more privileged users.

> Stolen accounts not only offer adversaries opportunity to launch attacks in the cloud, they also provide a way for attackers to gain a foothold in an organization's overall environment and access other parts of the network.

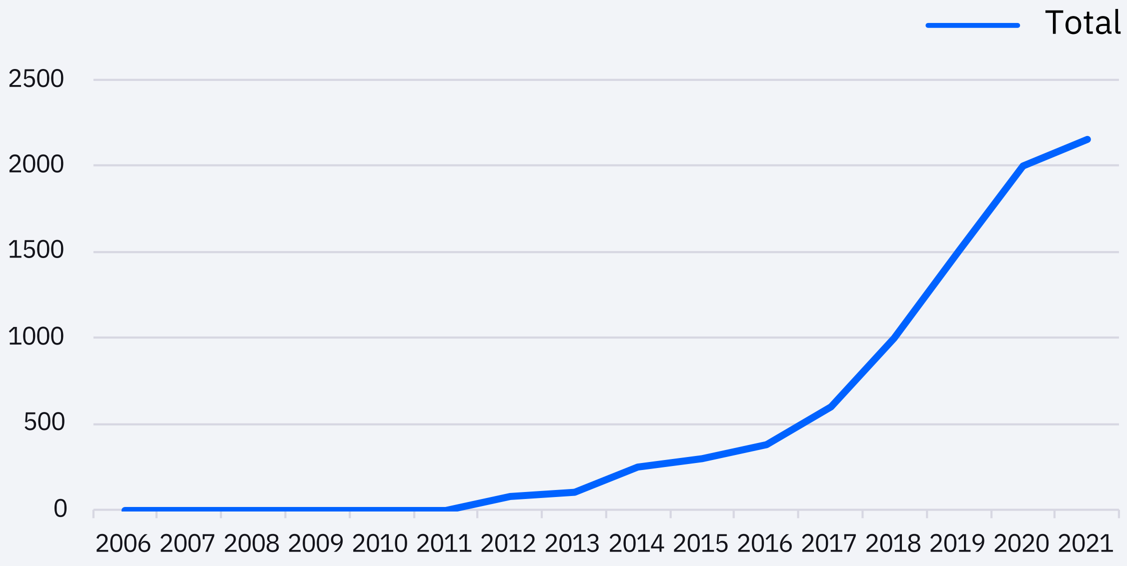
Assessing your value to threat actors

The dark web research shows that threat actors remain interested in accessing and taking advantage of cloud accounts, but IBM's research also highlights that not all accounts hold the same perceived value to an attacker and some elements may increase the value of an organization's account. For instance, an account based in western Europe with significant credits would be of very high value to threat actors and could increase an organization's threat profile. That sort of account is considered highly sought after and would sell quickly to cybercriminals.

Vulnerabilities in cloud environments grow in number and severity

Despite cloud environments' myriad of security benefits, researchers continue to discover new vulnerabilities that can help attackers break into the cloud. IBM research indicates that cloud vulnerabilities are growing in number, currently totaling over 2,500 vulnerabilities, a 150% increase in the last five years.

Number of cloud vulnerabilities tracked by X-Force



When it comes to vulnerabilities, IBM Security 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.

X-Force Red data shows that the severity of cloud-targeting vulnerabilities has grown significantly in recent years, likely due to threat actors’ realization that organizations are increasing their use of storing their critical data in multi-cloud environments. Cloud environments are heavily traveled data highways and are appetizing to threat actors due to the target-rich attack surface.

How threat actors are getting into cloud environments

Threat actors continue to access cloud data illicitly, and in this year's report IBM brings a host of new data points to refine our understanding of how they are targeting organizations' cloud assets.

150%

Cloud vulnerabilities are on the rise, increasing 150% over the last five years.

Password and policy violations, often from shadow IT, continue to plague cloud environments. X-Force Red found that 100% of their penetration tests into cloud environments in 2021 uncovered issues with at least one of these two components. These two elements trickled down to the most frequently observed initial infection vectors for organizations: improperly configured assets, password spraying and pivoting from on-premises infrastructure. In addition, API configuration and security issues, remote exploitation and accessing confidential data were common ways for threat actors to take advantage of lax security in cloud environments.

IBM Security X-Force Incident Response insights

The IBM Security X-Force Incident Response (IR) team analyzed cases over the last year involving cloud breaches and identified the most commonly exploited vulnerabilities and misconfigurations:

- Virtual machines and other resources with default security settings that were erroneously exposed to the Internet. This included misconfigured platforms and insufficiently enforced network controls that exposed internal services directly to the Internet, such as the Remote Desktop Protocol (RDP) on Microsoft platforms. Another example includes object data stores holding non-public data that were accessible publicly.
- Insufficient access control mechanisms, such as a lack of Multifactor Authentication (MFA) for SaaS solutions and federated services with landing pages accessible from the Internet. This means that with a stolen credential set, an attacker could authenticate themselves into an account without additional hurdles.
- Insufficiently segmented virtual networks and promiscuous trust relationships between on-premises and cloud computing environments. This means that a compromise in the cloud can enable further lateral movement across underlying systems.

X-Force IR also identified some organizational challenges that indirectly led to the compromises of cloud computing environments:

- Enterprises are still learning how to **monitor for and detect threats** in the cloud. This challenge is amplified by security policies that don't encompass the cloud, and a shortage of incident response skills that apply to cloud environments.
- Organizations do not have the same level of **confidence and expertise** when configuring security controls in cloud computing environments compared to on-premises environments.

Improperly configured resources

Insecure public APIs are a pervasive problem because they are very common and also allow external tools to interact with cloud functionalities, including access to data. Two thirds of cloud incidents in the data sample related to misconfigured API keys that allowed improper access. Similarly, the X-Force IR team found that over the last year, API credential exposure through public code repositories frequently accounted for threat actor access into cloud environments.

> Password spraying, exploited software vulnerabilities and cloud deployment misconfigurations are the most common methods threat actors use to access cloud environments.

When examining cloud-based cases, X-Force IR frequently identified unsecured resources unintentionally exposed to the Internet, such as misconfigured object storage services, as a major contributor to observed breaches. This data is further supported by the finding that almost two-thirds of breaches X-Force researchers observed were caused by insufficient hardening. IBM estimates that the use of shadow IT contributed to over half of the incidents analyzed.

The three most commonly observed methods for threat actors to compromise cloud environments in cases studied by X-Force IR were password spraying, software vulnerability, and pivoting from an on-premise compromise to the cloud.

Password spraying

This sort of attack is easily automated and can scale to target many organizations at once. X-Force IR often found that improper permissions further exacerbated compromises caused by successful password spraying attacks. Once an attacker managed to use a guessed/compromised password, their impact was greater in direct proportion to the user's privilege levels.

Software vulnerability

X-Force IR data found that vulnerabilities in software hosted on cloud environments often allow attackers to gain an initial foothold into an organization's environment. This challenge is exacerbated by the many types and brands of software that are cloud compatible, making securing each individual instance difficult for cybersecurity teams.

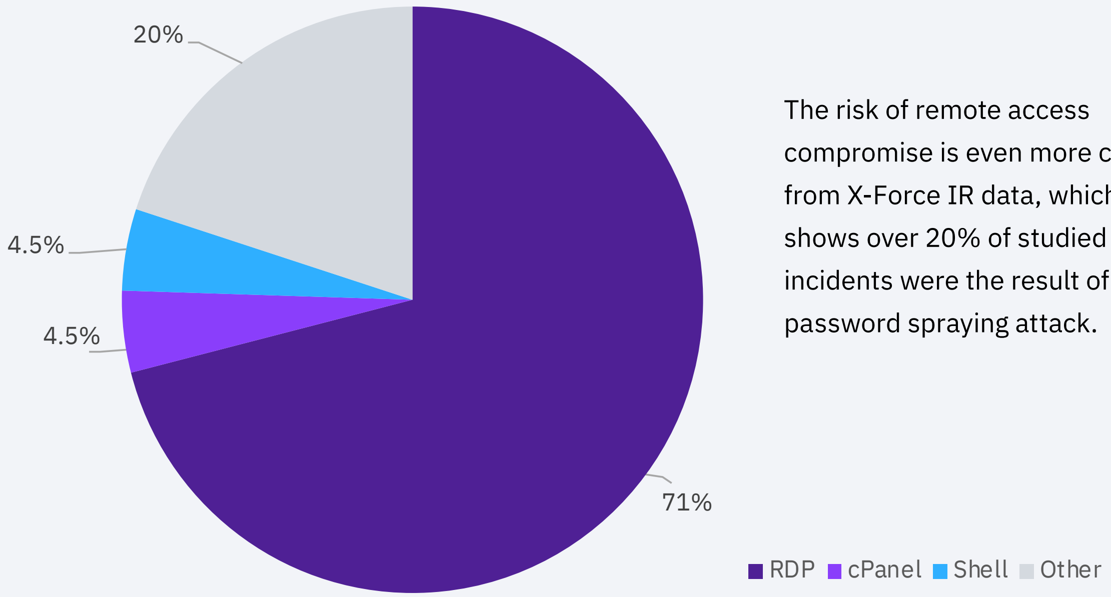
On-premises to cloud pivot

Another top three infection vector identified by X-Force IR is threat actors compromising end-users or systems hosted on-premises and pivoting to a cloud environment. This type of compromise, which occurred in over 23% of incident responses, can allow threat actors to deepen their hold on organizations and compromise even more organizational resources.

Remote exploitation favors RDP

Dark web data further reinforces the effectiveness of remote access compromise. IBM's analysis of dark web markets found that RDP accounted for the access vector in over 70% of cloud resources offered for sale on the dark web. cPanel and Shell access each took about 4.5% of the market share, suggesting that RDP access greatly exceeds the frequency of other access methods.

Dark web cloud accounts by access type



The risk of remote access compromise is even more clear from X-Force IR data, which shows over 20% of studied incidents were the result of a password spraying attack.

Threat actors using cloud environments for miners, ransomware and botnets

X-Force analyzed data from our IR teams to find how threat actors are using cloud environments once they're inside. Based on our analysis of incidents, cryptominers and ransomware were used extensively, accounting for over half of system compromises. Cloud environments are an attractive target for resource-intensive cryptominers as they can provide scalable resources and processing power. Also, cloud environments may not receive the same level of oversight as on-premises servers, which is appealing for threat actors and makes it easier for 'noisy' malware like DDoS bots and cryptominers to remain undetected for longer periods.

Clouds allow attackers to scale attacks and wipe traces; compromised clouds allow them to do it for free.

Malware focus on Docker

Analyzing malware trends impacting cloud environments, X-Force IR observed multiple malware families shifting their sights from targeting generic Linux systems to focusing on Docker containers. Attacks on Docker tend to fall into three categories: registry, host and running container attacks.

Some malware families illustrating this shift include XoRDDOS, Groundhog and Tsunami. This Docker-focused push expands beyond just bots, also highlighting the malicious activity of IoT malware (Kaiji), cryptominers (Xanthe, Kinsing) and other malware strains.

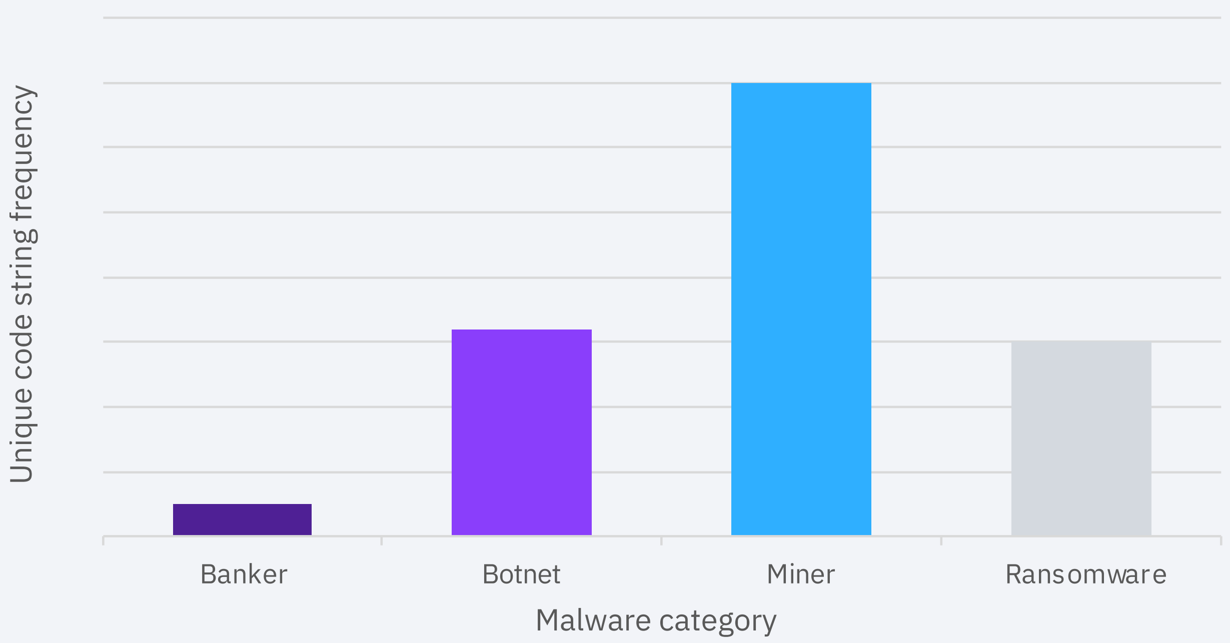
Botnet malware also saw increased popularity in targeting cloud environments this year. Specifically, exposed Docker servers seem to remain a prominent target for botnet malware. Threat actors have also been observed targeting other container platforms in addition to Docker. For example, the Siloscape malware was found compromising vulnerable Windows containers, and the container management platform, Kubernetes, is also increasingly targeted by actors such as TeamTNT.

Cloud-centric malware development on the rise

Research by Intezer highlights threat actors' continued investment in evolving the code in cryptominers, botnets and ransomware. Conversely, threat actors have shown little interest in updating banking trojan code so far in 2021. These conclusions align with IBM data indicating that cloud environments are targeted more heavily by cryptomining malware, with ransomware and botnets continuing to be popular options as well.

The following chart shows Intezer's research on the level of investment made in updating and altering malware over the last year by category. Miners show a high percentage of change, nearly 7% of code used being different year over year, indicating significant investment by actors. Comparatively, banking Trojans have a low percent of changed code, less than 1 percent.

Frequency of unique code strings



Cryptominers

Cryptominer infection, highlighted as a key malware used in compromised cloud environments in the 2020 Cloud Security Threat Landscape Report, remains a top threat actor goal. Based on Intezer research, one of the ways cryptominers infect cloud environments is via malicious Docker images. Threat actors, like TeamTNT, create images that contain malware and, once the threat actor gets access to a Docker daemon, they use the image to spin a new container with the malicious image.

Command and control shifts

Threat actors continue to use cloud infrastructure to host malicious payloads and maintain Command and Control (C2) backend for their operations. While we reported on this activity in last year's report, the trend has expanded, with 2021 seeing more cloud-based and web services being leveraged in new ways to avoid detection. Some illustrative examples include:

- A cloud-leveraging backdoor dubbed "PowerSlack" using popular chat software Slack for C2 communications.
- A malware family known as Astaroth stored C2 information in YouTube video descriptions, potentially hiding suspicious network traffic as legitimate activity.

Fileless malware

Evasive, fileless malware lurking in memory can elude standard detection tools leaving security teams blind to its presence. Besides using scripts to launch fileless malware, threat actors are now using Ezuri, an opensource crypter and memory loader written in Golang, which makes it even easier to launch undetected malware. Golang is a popular language that's rapidly becoming the language of choice for many cloud native operations and attack frameworks.

> Cloud platforms allow attackers to scale attacks and wipe traces. Compromised clouds allow them to do it for free.

Recommendations and best practices for preparing for and responding to cloud breaches

IBM Security X-Force suggests cloud users should consider implementing a multi-phased security approach in preparation and response to cloud security incidents.

Preparation

- 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 Cloud Pak for Security.

- Consider implementing a zero trust philosophy, including implementing virtual network segmentation to restrict access to resources and reduce the risk of lateral movement in the case of a compromise.

- Evaluate trust relationships between on-premises and cloud environments as a critical part of the security strategy. This is especially important for private clouds that may interact with other on-premises assets on a regular basis.

- Extend monitoring and detection capabilities to cloud environments. Determine and enable audit logging requirements in cloud environments and leverage cloud-native tools and technologies to monitor for malicious activity and evidence of compromise.

- Deploy a bastion host to isolate private cloud network zones from external, less trusted or untrusted networks, including the Internet, to reduce the cloud attack surface and minimize 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.
    - Modernize Identity and Access Management (IAM) 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.

- Scope penetration testing projects to identify vulnerabilities in cloud-hosted applications and environments.

- Engage in adversary simulation exercises using cloud-based scenarios to train and practice effective cloud-based incident response.

Responding

- Implement AI and automate incident response and malware analysis when feasible, as this 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 will allow for subsequent investigation into how the breach occurred and what, if anything, else the threat actors may have done while in the organization's environment.

- Leverage threat intelligence during incident response to use knowledge of the threat actor to hasten response times and enable more thorough response activities.

- Ensure your organization has the right tools and personnel for responding to a cloud breach, and that your incident response playbooks are specifically designed for cloud-based breaches.

- Have surge assistance on speed dial. Even large security teams often need assistance early in the incident response (IR) cycle and during remediation efforts. Having an X-Force Incident Response Retainer in place can help minimize delays getting the assistance you need during an attack.

About IBM Security X-Force

The X-Force team is comprised of industry-leading, highly skilled incident response professionals experienced in investigating compromises of on-prem, cloud and hybrid cloud environments. X-Force also provides proactive cloud service offerings for cloud such as maturity assessments, development of IR plans/playbooks, and training and simulation exercises. All of this is underpinned with industry-leading X-Force Threat Intelligence based on insights from IBM telemetry. This approach helps organizations prepare for, detect, and respond to security incidents more efficiently and effectively. It also helps minimize revenue loss and recovery costs associated with a security incident. If you would like to learn more about any of the X-Force report findings or would like to learn about any X-Force services schedule a consult here.

Contributors

Charles DeBeck

Richard Emerson

Andrew Gorecki

Charlotte Hammond

Intezer

Scott Lohr

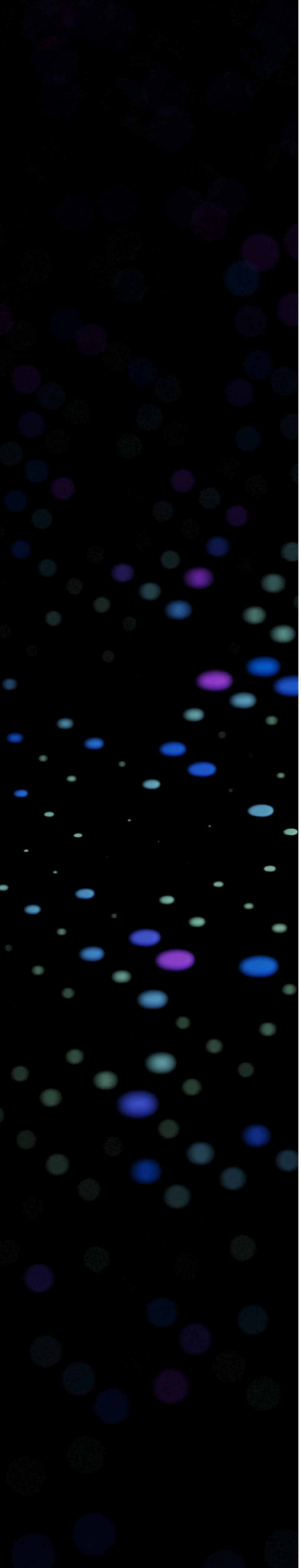
Mitch Mayne

Scott Moore

Jason Riggs

Oscar Sanchez

Johnny Shaieb



IBM Security
New Orchard Rd
Armonk, NY 10504
U.S.A.

Produced in the United States of America