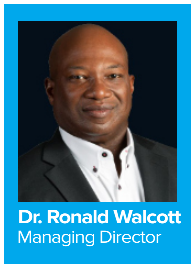
precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 24 AUGUST 2023

In this issue of our newsletter, we will discuss the impacts of Attacks against Cloud Services on businesses and users



Dr. Ronald Walcott
Managing Director

In an era driven by digital transformation, the landscape of information technology has undergone a profound shift, with cloud services emerging as a pivotal enabler of scalable, flexible, and cost-effective solutions for individuals and businesses alike. Cloud services provide a virtualized environment that hosts an array of resources such as computing power, storage, and networking, offering unprecedented levels of accessibility and convenience. However, this technological advancement has also given rise to a new frontier of threats and challenges, prominently exemplified by the escalating specter of attacks against cloud services.

HOW DO CYBER-ATTACKS IMPACT CLOUD SERVICES FOR BUSINESSES AND USERS?

In recent years, as organizations have embraced cloud solutions to optimize their operations, streamline processes, and enhance collaboration, the allure of this virtualized realm has not gone unnoticed by malicious actors. Cybercriminals, state-sponsored groups, and hacktivists have all recognized the potential value of targeting cloud environments, thereby creating a multifaceted threat landscape that demands vigilant attention and comprehensive defense strategies. These attacks against cloud services can have far-reaching implications, impacting not only the confidentiality, integrity, and availability of sensitive data but also the overall trust in the digital infrastructure that underpins modern society.

Cyberattacks have a profound impact on cloud services, affecting both the providers of cloud services and the customers who rely on them. These attacks can disrupt operations, compromise data, erode trust, and lead to financial losses. Here are some of the key ways in which cyberattacks impact cloud services:

1) **Service Availability and Reliability:** One of the primary impacts of cyberattacks on cloud services is the disruption of service availability and reliability. Attacks such as Distributed Denial of Service (DDoS) can overwhelm cloud infrastructure, causing services to become slow or completely inaccessible. This can lead to downtime for businesses and users, resulting in lost revenue and decreased productivity.

2) **Data Breaches and Privacy Violations:** Cyberattacks can lead to unauthorized access to sensitive data stored in the cloud. If attack-

In this Issue:

ers successfully breach a cloud service, they may gain access to confidential information such as customer data, financial records, intellectual property, and more. This not only compromises privacy but can also have legal and regulatory consequences.

3) **Resource Exploitation:** Malicious actors can exploit cloud resources for their own purposes, such as cryptocurrency mining or launching further attacks. This can lead to unexpected resource consumption, increased costs for cloud customers, and degraded performance for legitimate users.

4) **Reputational Damage:** High-profile cyberattacks against cloud services can damage the reputation and trust of both the cloud service provider and its customers. This loss of confidence can lead to customers seeking alternative providers, impacting the provider's business and revenue.

5) **Financial Loss:** Cyberattacks can result in financial losses due to business disruption, costs associated with mitigating the attack, potential legal fines, and compensation to affected customers. Organizations may also incur expenses related to strengthening security measures and recovering from the attack.

WHAT ARE DIFFERENT TYPES OF ATTACKS THAT HAVE IMPACT CLOUD SERVICES?

Several types of cyberattacks can have a significant impact on cloud services. These attacks exploit vulnerabilities and weaknesses in cloud infrastructure, applications, and user behaviors. Here are some of the different types of attacks that can affect cloud services:

1) **Distributed Denial of Service (DDoS) Attacks:** DDoS attacks flood a cloud service with a massive volume of traffic, overwhelming its resources and causing it to become unavailable to legitimate users. These attacks can disrupt business operations, leading to service outages and financial losses.

2) **Data Breaches:** Data breaches involve unauthorized access to sensitive information stored in the cloud. Attackers can steal customer data, financial records, intellectual property, and other confidential data, compromising privacy and potentially violating regulatory requirements.

3) **Man-in-the-Middle (MitM) Attacks:** MitM attacks occur when attackers intercept communications between users and the cloud service. This can enable them to eavesdrop on sensitive data, modify messages, or impersonate legitimate users.

4) **Account Hijacking:** In account hijacking attacks, attackers gain unauthorized access to cloud accounts by exploiting weak passwords, stolen credentials, or vulnerabilities in authentication mechanisms. Once in control, attackers can misuse the accounts for malicious purposes.

5) **Zero-Day Exploits:** Zero-day exploits target unknown vulnerabilities in software or systems. If such vulnerabilities exist in cloud infrastructure or applications, attackers can exploit them for unauthorized access or data theft.

Here are some ways in which these attacks can be defended against:

Defending against attacks on cloud services requires a comprehensive and layered approach to security. Here are some strategies and best practices to help mitigate the risks and protect cloud environments from various types of attacks:

1) **Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security to user accounts. This helps prevent unauthorized access even if credentials are compromised.

2) **Strong Password Policies:** Enforce strong password policies that require complex passwords and regular password changes to reduce the risk of credential-based attacks.

3) **Data Encryption:** Encrypt data both at rest and in transit. This helps protect sensitive information from unauthorized access even if attackers gain access to the data.

4) **Access Controls and Role-Based Permissions:** Implement granular access controls and role-based permissions to ensure that users only have access to the resources and data they need to perform their tasks.

5) **Intrusion Detection and Prevention Systems (IDS/IPS):** Deploy IDS and IPS solutions to monitor network traffic and detect and prevent unauthorized activities and attacks.

6) **Employee Training and Awareness:** Educate employees about common attack vectors like phishing and social engineering to reduce the risk of successful attacks through user interactions.

Upcoming Events

LONDON CYBERSECURITY SUMMIT
September 19th, 2023
London

AMCHAM HSSE CONFERENCE
October 31st, 2023
Trinidad & Tobago

Frequently Asked Questions:

WHAT TYPES OF ATTACKS COMMONLY TARGET CLOUD SERVICES?

Common attacks include DDoS attacks, data breaches, account hijacking, phishing, malware injection, and supply chain attacks.

HOW DO ATTACKS IMPACT CLOUD SERVICE AVAILABILITY?

Attacks like DDoS overload cloud resources, causing service downtime or degradation for legitimate users.

CAN CLOUD SERVICES BE PROTECTED FROM DDOS ATTACKS?

Yes, cloud providers and customers can use DDoS protection solutions and strategies to mitigate the impact of DDoS attacks.

WHAT IS MULTI-FACTOR AUTHENTICATION (MFA), AND WHY IS IT IMPORTANT FOR CLOUD SECURITY?

MFA requires users to provide multiple forms of verification to access accounts. It's crucial for preventing unauthorized access to cloud services, even if passwords are compromised.

Headline News

Warning: Attackers Abusing Legitimate Internet Services

Microsoft's OneDrive and Google Cloud increasingly hide malicious activities as hackers count on network defenders to classify traffic with those services as inherently legitimate. The solution, said threat intelligence firm Recorded Future, is to flag or block the unapproved use of any cloud service.

Researchers with the firm's Insikt team found mounting abuse of commercial cloud offerings perpetrated most often by advanced persistent threat groups aligned with nation-states and to a lesser extent by cybercriminals.

Insikt security researchers analyzed more than 400 current malware families and found that 25% of them - most often information-stealing malware - abuse legitimate cloud services in some capacity, and two-thirds of those abuse more than one such service.

Attackers' proclivity for "living off trusted sites" is easy to explain: It makes their attempts to exfiltrate data, remotely relay command-and-control instructions or push downloads of malicious payloads to compromised endpoints tougher to spot. Using someone else's infrastructure is also less expensive for criminals than having to hire their own "bulletproof" hosting services - and oftentimes much easier and quicker to set up.

Cloud storage platforms, and Google Cloud in particular, are the most exploited, followed by messaging services - most often Telegram, including via its API - as well as email services and social media, the researchers found. Examples of other services being abused by attackers include OneDrive, Discord, Gmail SMTP, Mastodon profiles, GitHub, bitcoin blockchain data, the project management tool Notion, malware analysis site VirusTotal, YouTube comments and even Rotten Tomatoes movie review site profiles.

"It is important to note that ransomware campaigns use legitimate cloud storage tools such as mega.io or MegaSync for exfiltration purposes as well," although the cryptolocking malware itself may not be coded to work directly with legitimate tools, the report says.

Criminals' choice of service depends on desired functionality. Anyone using an info stealer such as Vidar needs a place to store large amounts of exfiltrated data. The researchers said cloud services' easy setup for less technically sophisticated users makes them a natural fit for such use cases.

Messaging services such as Telegram and Discord also are frequently used, at least for downloading payloads. Take the WhisperGate wiper malware attributed to Russia's GRU military intelligence agency and deployed in the days and weeks leading up to the all-out invasion of Ukraine ordered by Mo-

scow last February. In the second stage of a WhisperGate attack, malware on a victim's system downloaded the final stage of the malware, which was stored on Discord's content delivery network as a JPEG file, Recorded Future reported last year.

Criminals are also tapping messaging services. Last September, researchers reported that the widely used, pay-per-install malware service PrivateLoader had been downloading payload code as Discord attachments.

Abusing legitimate services isn't foolproof. Major providers' threat-hunting teams work overtime to detect malicious use. Researchers regularly track IP addresses being used to resolve malicious links or for data dead drops, and they share this intelligence so illicit use can be blocked.

To blunt the use of legitimate internet services by hackers - whether APT groups or criminals - Recorded Future recommends flagging or at least blocking outright the unapproved use of legitimate internet service as a short-term approach. A long-term strategy involves adding fine-grained defenses that facilitate the legitimate use of these services while blocking attempts to employ them maliciously. In particular, the researchers recommend TLS network interception tools for gaining visibility into encrypted network data, although they caution that such tools need to be backed by policies and procedures to minimize the "privacy and compliance concerns" that accompany decrypting data in transit.

The researchers also recommend regularly running simulated attacks to see if defenses are up to the task of spotting and blocking LIS abuse inside an enterprise.