34 Cloud Security Terms You Should Know

AVANAN
The Cloud Security Platform

Account Takeover

A type of cyber attack in which the hacker spends extended periods of time dormant in a compromised account, spreading silently within the organization through internal messages until they have access to information that is valuable to them. They may use the account to attack other organizations.

Advanced Persistent Threat (APT)

This an attack in which an the attacker gains access to an account or network and remains undetected after the initial breach. The “advanced” describes the initial breach technique (phishing or malware) that was able to evade the victim's security. The attack is "persistent" because the attacker continues to carry out the attack through reconnaissance and internal spread long after the initial breach.

Advanced Threat Protection (Microsoft ATP)

Microsoft offers its Advanced Threat Protection for an additional $24 per user per year. It includes capabilities not available in the default Office 365/Outlook.com account:

- **Safe Links:** replaces each URL, checking the site before redirecting the users.
- **Safe Attachments:** scanning attachments for malware
- **Spoof Intelligence:** analyzes external emails that match your domain.
- **Anti-phishing Filters:** looks for signs of incoming phishing attacks.

Anomaly

A type of behavior or action that seems abnormal when observed in the context of an organization and a user's historical activity. It is typically analyzed using some sort of machine-learning algorithm that builds a profile based upon historical event information including login locations and times, data-transfer behavior and email message patterns. Anomalies are often a sign that an account is compromised.

API Attack

An API (Application Programming Interface) allows two cloud applications to talk to one other directly, allowing a third party to read or make changes directly within a cloud application. Creating an API connection requires a user's approval, but once created, runs silently in the background, often with little or no monitoring. An API-based attack typically involves fooling the user into approving an API connection with a phishing attack. Once granted the API token, the attacker has almost complete access and control, even if the user changes the account password. To break the connection, the user must manually revoke the API token.

Behavioral Analysis

A security measure in which a file's behavior is monitored and analyzed in an isolated environment in order to see if it contains hidden malicious functions or is communicating with an unknown third-party.

Brand Impersonation

A method of phishing attack in which the perpetrator spoofs the branding of a well-known company to fool the recipient into entering credentials, sharing confidential information, transferring money or clicking on a malicious link. An example might be a forged email that looks like it is from a social media company asking to verify a password.

Breach Response

A form of security that remedies the damage caused by a breach. For example, changing passwords, revoking API tokens, resetting permissions for shared documents, enabling multi-factor-authentication, restoring lost or edited documents, documenting and classifying leaked information, identifying potential pathways to collateral compromise.

CASB

An acronym for Cloud Access Security Broker. This is a type of security that monitors and controls the cloud applications that an organization's employees might use. Typically, the control is enforced by routing web traffic through a forward- or reverse-proxy. CASBs are good for managing Shadow IT and limiting employee's use of certain SaaS or the activity within those SaaS but do not monitor third-party activity in the cloud–i.e. shared documents or email.

Cloud Access Trojan

Also known as a CAT, a Cloud Access Trojan describes any method of accessing a cloud account without the use of a username and password, for example, a malicious user syncing a desktop app, forwarding all email to an external account, connecting a malicious script or simply authorizing a backup service for which they have full access. In each case, the attacker needs only momentary access, often gained through a phishing attack.

Cloud Messaging Apps

Cloud-based communication services that include email but are used by companies for internal communication but also might include trusted partners. Often employees imbue more trust in these apps even though they are just as capable of distributing malware or phishing messages.

Cloudify

Taking a software that was created for on-premise or datacenter usage, wrapping it with an API container and converting it to a cloud service. For example, taking the malware analysis blade from a perimeter appliance and adapting it so that it can be configured and scaled without the need for direct management. This also includes the automation of software licensing and version control.

Compromised Account

An account which has been accessed and is possibly controlled by an outside party for malicious reasons. This can be done either via API connection or by gaining credentials to the account from a leak or phishing email. Typically, the goal of the attacker is to remain undetected, in order to use it as a base for further attacks.

Data Classification

A security and compliance measure in which all of an organization's documents are scanned and categorized based on their sensitivity and then are automatically encrypted or adjusted to the correct sharing level permissions. For example documents containing customer information or employee social security numbers would be classified as highly sensitive and encrypted where as an external facing white paper would be classified as non-sensitive and likely not encrypted.

DLP (Data Leak Prevention or Data Loss Prevention)

A type of security that prevents sensitive data, usually files, from being shared outside the organization or to unauthorized individuals within the organization. This is done usually through policies that encrypt data or control sharing settings.

DRM

Digital Rights Management: a set of access control technologies for restricting the use of confidential information, proprietary hardware and copyrighted works, typically using encryption and key management.

Gateway

A gateway is any device or is another word for an MTA, please see the definition for MTA.

IRM

Information Rights Management is a subset of Digital Rights Management that protects corporate information from being viewed or edited by unwanted parties typically using encryption and permission management.

Latency

The added time it takes for an email to be delivered to its intended recipient. Security measures sometimes add latency as they perform scans on the email prior to allowing the email to reach the user's inbox.

Malconfiguration

A deliberate configuration change within a system by a malicious actor, typically to create back-door access or exfiltrate information. While the original change in configuration might involve a compromised account or other vulnerability, a malconfiguration has the benefit of offering long term access using legitimate tools, without further need of a password or after a vulnerability is closed.

Misconfiguration

A dangerous or unapproved configuration of an account that could potentially lead to a compromise typically done by a well-intentioned user attempting to solve an immediate business problem. While there is no malicious intent, misconfiguration is actually the leading cause of data loss or compromise.

Misconfiguration

A dangerous or unapproved configuration of an account that could potentially lead to a compromise typically done by a well-intentioned user attempting to solve an immediate business problem. While there is no malicious intent, misconfiguration is actually the leading cause of data loss or compromise.

MTA

An acronym for Message Transfer Agent. An MTA is an appliance or service that acts as the authorized server-of-record for electronic messages, eventually passing them on to the final mail server.

Phishing

A type of attack in which a message (often email, but could be any messaging system) is sent from a malicious party disguised as a trusted source with the intention of fooling the recipient into giving up credentials, money, or confidential data. It often includes a malicious link or file, but could be a simple as a single sentence that causes some sort of insecure response.

Proxy

A proxy can include any gateway, service or appliance that causes a rerouting of traffic through an appliance or cloud service. For example, a web proxy or CASB will redirect a user's web browsing in order to decrypt the traffic and block particular applications or data. Mail proxy gateways (see MTA) reroute incoming email in order to scan and block spam, phishing or other malicious email. A proxy is limited in its visibility as it cannot monitor or control traffic it cannot see, i.e. remote and non-employee web usage or internal email traffic.

Quarantine

The act of encrypting, moving or changing the share permissions of a file so that it is unreachable by a user until it can be deemed safe or authorized by the intended recipient.

Ransomware

A type of malware that encrypts the files on an endpoint device using a mechanism for which only the attacker has the keys. While the attacker will offer the key in exchange for payment, fewer than half of victims that do pay actually recover their files.

Sandboxing

A type of security measure that involves testing a file or link in a controlled environment to see what effect it has on the emulated operating system, typically the first line of defense against zero-day attacks for which there is no signature or pre-knowledge of the code.

Shadow IT

Any unapproved cloud-based account or solution implemented by an employee for business use. It might also include the use of an unknown account with an approved provider, but administered by the user rather than corporate IT.

Shadow SaaS

An unapproved cloud application that is connected in some way (typically by API) to that organization's SaaS or IaaS with access to corporate data but without permission from the organization.

Spearphishing

A type of phishing attack that is designed to target a small number of users, sometimes only one user such as a CEO. Spear-phishing attacks usually involve intensive research by the hacker to increase the chances that the intended target will fall for it.

Tokens

A unique authorization key used for API interactions. Each token is granted a certain level of access and control and often continues to provide access until the token is manually revoked.

URL Analysis

A security measure that reviews a link to assess if it is genuine and will direct to a safe and expected destination with no unintended side effects.

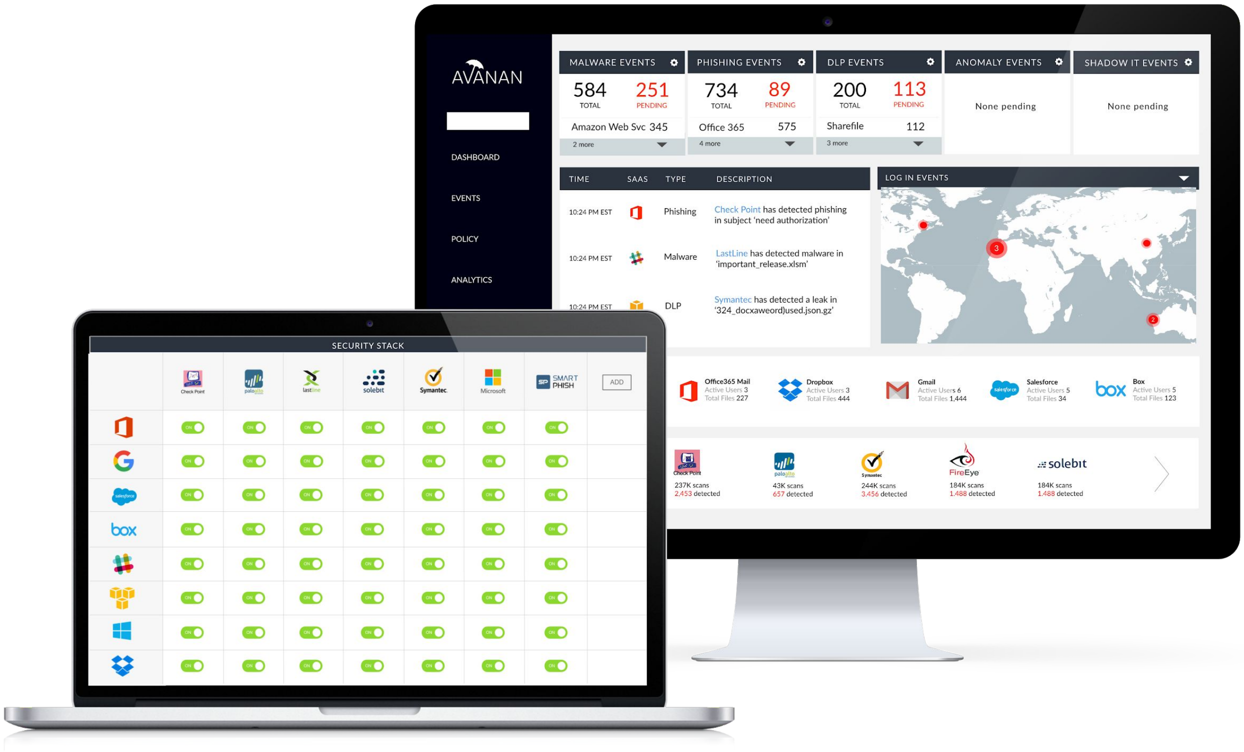
URL Impersonation

A technique used in phishing attacks in which the hacker creates a URL that looks like a link to a trusted website to the untrained eye. These techniques can be thwarted using URL analysis.

User Impersonation

A technique used in phishing attacks in which the hacker makes their email look like it is coming from a trusted sender, either a corporation or another employee. This can be done by editing their nickname or using an email address that looks like it is from a trusted organization.

Start a free trial of Avanan Cloud Security



MALWARE EVENTS		PHISHING EVENTS		DLP EVENTS		ANOMALY EVENTS	SHADOW IT EVENTS
584 TOTAL	251 PENDING	734 TOTAL	89 PENDING	200 TOTAL	113 PENDING	None pending	None pending
Amazon Web Svc	345	Office 365	575	Sharefile	112		
2 more		4 more		3 more			

TIME	SAAS	TYPE	DESCRIPTION
10:24 PM EST		Phishing	Check Point has detected phishing in subject 'need authorization'
10:24 PM EST		Malware	LastLine has detected malware in 'important_release.xlsm'
10:24 PM EST		DLP	Symantec has detected a leak in '324_docxaweord)used.json.gz'

Office365 Mail
Active Users 3
Total Files 227

Dropbox
Active Users 3
Total Files 444

Gmail
Active Users 6
Total Files 1,444

Salesforce
Active Users 5
Total Files 34

Box
Active Users 5
Total Files 123

Check Point
237K scans
2,453 detected

paloalto
43K scans
657 detected

Symantec
244K scans
3.456 detected

FireEye
184K scans
1.488 detected

solebit
184K scans
1.488 detected

SECURITY STACK

	Check Point	paloalto	lastline	solebit	Symantec	Microsoft	SP SMART PHISH	ADD
	ON	ON	ON	ON	ON	ON	ON	
	ON	ON	ON	ON	ON	ON	ON	
salesforce	ON	ON	ON	ON	ON	ON	ON	
box	ON	ON	ON	ON	ON	ON	ON	
	ON	ON	ON	ON	ON	ON	ON	
	ON	ON	ON	ON	ON	ON	ON	
	ON	ON	ON	ON	ON	ON	ON	
	ON	ON	ON	ON	ON	ON	ON	