eSENTIRE

INCIDENT REPORT:

esLOG+ Thwarts Amazon Web Services (AWS) Brute Force Attack

IT STARTED WITH PATIENT ZERO

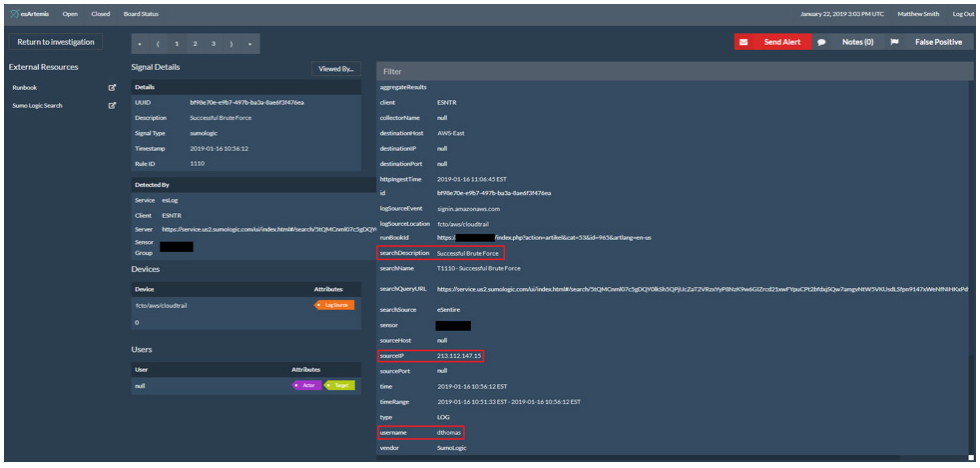
A cyberattacker obtained a legitimate username on a client's network and launched a dictionary attack against an eSentire customer's AWS instance. After numerous attempts, the attacker was able to determine the password and gain access to the AWS instance. The attacker attempted 31 passwords before successfully logging in. The threshold of five attempts was exceeded and an event was generated into the eSentire Security Operations Center (SOC).

T1110-AWS Brute Force Events

Last 24 Hours

#	time	username	total_failures_before_success
1	2019-01-16 10:56:12.000	dthomas	31

The SOC used the esArtemis dashboard to review the event. The SOC analyst extracted log information such as the type of attack (Successful Brute Force), the source IP address and the username the attacker had compromised. From the dashboard, the SOC analyst quickly reviewed the runbook and additional resources on the attack type and launched the investigation.



Attack Types:

AWS Brute Force

Brute force is one of the most commonly used methods adversaries use to gain access to an account or server. When passwords are unknown, an attacker attempts to gain access using different combinations of usernames and passwords until account lockout or a correct username and password are submitted. While incorrect logins frequently occur, the delineation between an intrusion attempt and a legitimate user requires a defined process to quickly filter noise from possible attack.

Due to the number of incorrect login attempts that are more prevalent in organizations with remote services, timely and scalable investigations are paramount to identifying, confirming and responding to potential attacks. In this case, eSentire's SOC leveraged esLOG+ to detect a threat actor's presence on a customer's AWS instance almost immediately and mitigated it in less than 17 minutes.

INVESTIGATION BEGINS

The SOC dove into the esLOG+ instance and focused on the username “dthomas.” Since that user is located in Cambridge, ON, the activity coming from the IP address in Canada is considered normal. The bigger concern was the 31 failed attempts coming from Sweden, which required additional investigation.

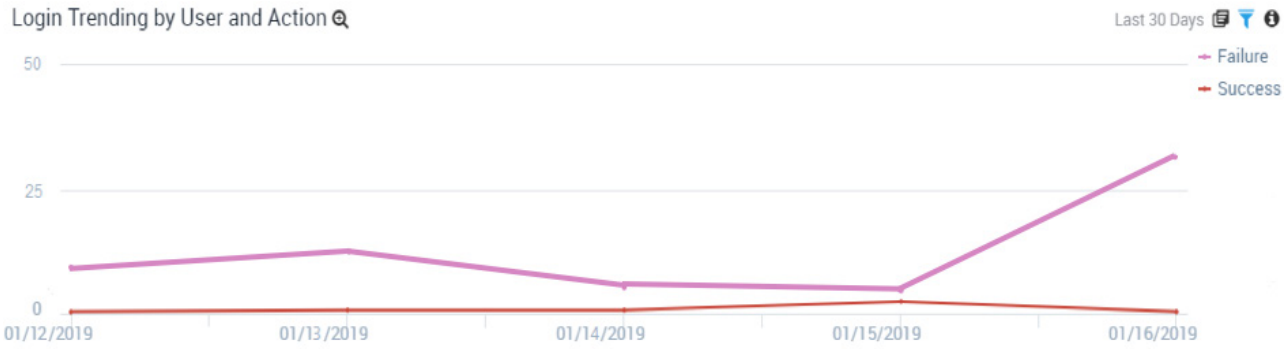
Login Action Count by User, Action, MFA Status, Source IP, Country, and City

Last 30 Days

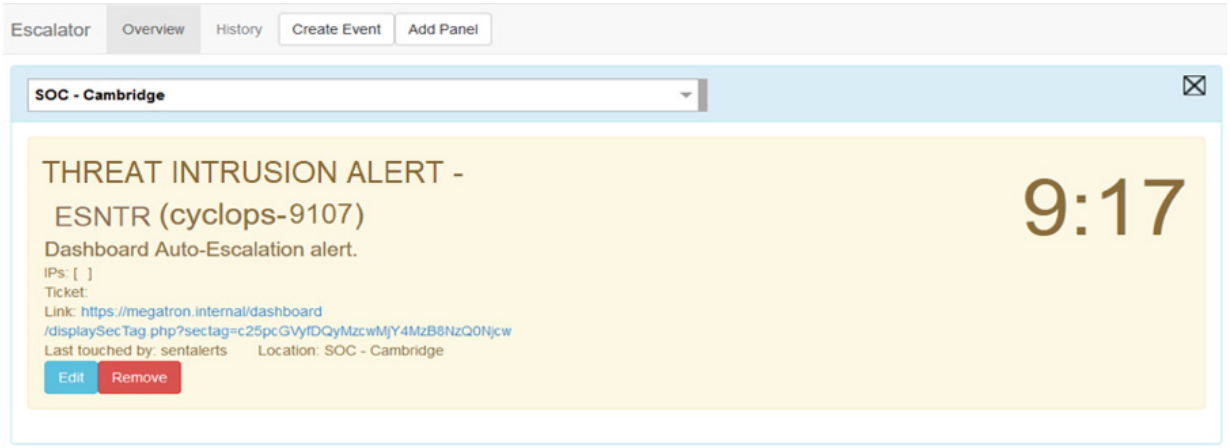
#	username	action	mfa_used	src_ip	country_name	city	_count
1	dthomas	Success	No	213.112.147.15	Sweden	Stockholm	1
2	dthomas	Success	No	52.129.34.145	Canada	Cambridge	12
3	dthomas	Failure	No	213.112.147.15	Sweden	Stockholm	31
4	dthomas	Failure	No	52.129.34.145	Canada	Cambridge	42

The SOC used the last 30 days of login logs for “dthomas” to determine the common login geolocations. An individual who travels often for business would have multiple login locations, therefore looking at historical data can help determine if this is common behavior for this user, or an anomaly.

Further investigation into the past 30 days of login logs for “dthomas” showed the user commonly failed to login, so a large spike in failed attempts coming out of Sweden on a single day was definitely inconsistent with historical behavior. At this point, the SOC generated an alert to our customer with details on where the logins were coming from, the IP address behind the attack, where they were logging in to, how eSentire detected it and some recommendations on how to proceed with eliminating the intrusion.



Due to the alert’s severity and the presence of a threat actor on the customer’s network, the SOC escalated the incident and placed a call to the client. The SOC informed our customer that the user password should be reset immediately, and the external IP should be blocked.



THREAT QUICKLY ELIMINATED

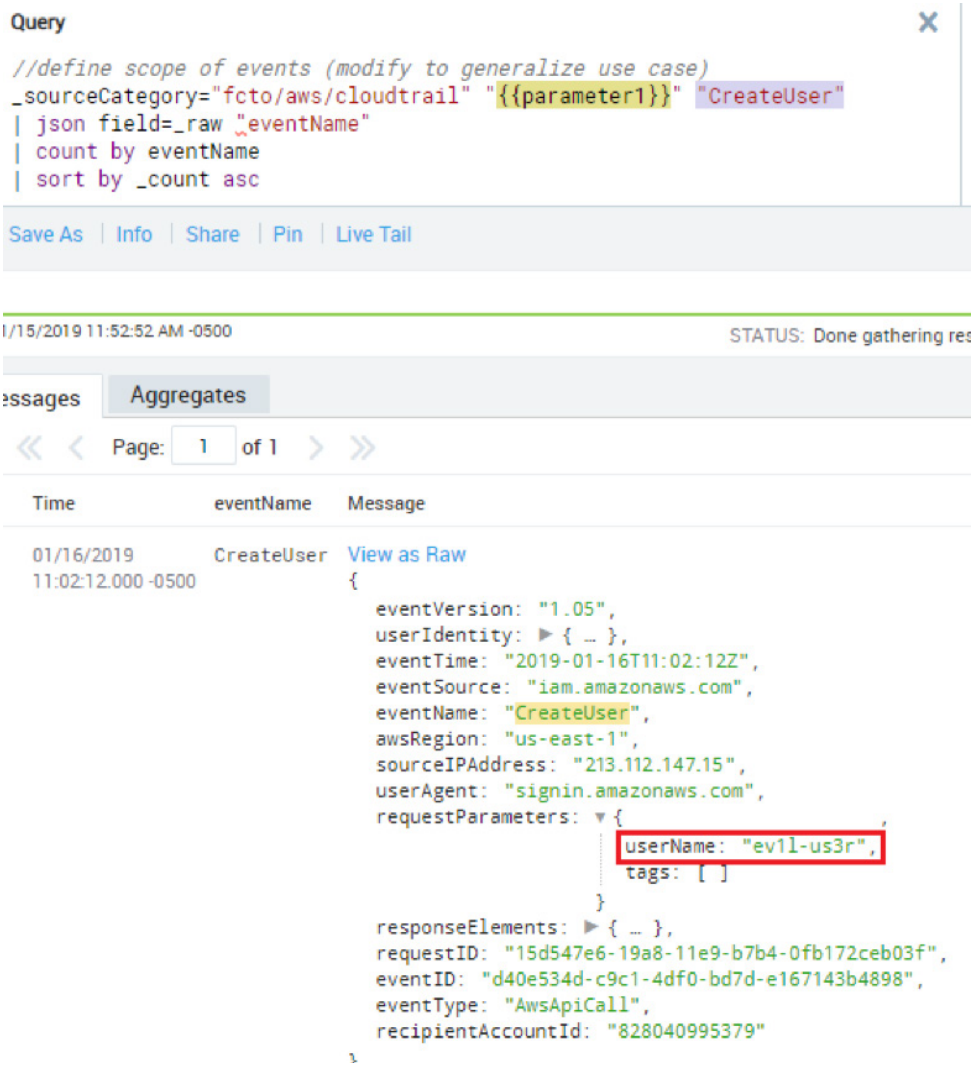
The customer followed the recommended actions of changing the user's password and blocking the malicious IP address, eliminating the attacker's access to their network. And then requested a deeper investigation into what activities the attacker performed after the successful login.

DIVING DEEPER

The SOC did a deep dive and checked all unique event types for this specific user for the last 24 hours and last 30 days. This allowed the SOC to see if any key events stood out … and one such event did. There was a "CreateUser" event that prompted further scrutiny. The SOC wanted to see if that account was created within the compromised time frame and did it look like "dthomas" did it or was it something malicious?

Upon further review of the raw log data for the "CreateUser" event, it was revealed that the attacker created a user called "ev1l-us3r." The eSentire SOC then checked activity for the "ev1l-us3r" account and confirmed that the account had not yet logged in to the AWS instance.

The customer was instructed to disable/delete the "ev1l-us3r" account to eliminate the attacker's ability to log in to the customer's AWS instance. Concurrently, the eSentire SOC enabled temporary detection for "ev1l-us3r" logging into the AWS instance while the customer remediated. The total time from detection to elimination was under 17 minutes.



ATTACK TIMELINE

eSentire

eSentire, Inc., the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $5.7 trillion AUM in the financial sector alone, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.esentire.com** and follow **@eSentire.**