Threat Detection Using Machine Learning with Oracle CASB Cloud Service

A recent announcement from the United States – Computer Emergency Readiness Team (US CERT)[i], published on April 16, 2018 warned of attacks from Russia-based IP addresses that were actively attempting to penetrate US-based infrastructure, including devices attached to personal networks, such as home routers. Such state-sponsored threats are undoubtedly some of the most difficult to identify and defend against due to the resources available to a nation state. While most of us consider ourselves unlikely “targets of interest” in these kinds of attacks, there are frequently collateral effects from these threats. This optimism bias is a not a viable, usable, or sustainable approach to comprehensive Information Security (InfoSec) risk management. Unfortunately, this remains a key characteristic of how many organizations approach internet-based threats to their usage of cloud applications.

A common tactic in many types of attacks is to execute “low volume” (few transactions) and “low velocity” (few targets) transactions that can be difficult to detect in highly-active cloud services. When such attacks are propagated by nation states, they can be harder to identify and defend against. This is an area where machine learning, and artificial intelligence can help significantly. Oracle Cloud Access Security Broker (CASB) helped detect and notify customer teams about one such recent attack.

SOURCES AND BEHAVIORAL PATTERNS OF ATTACK

F5 Networks reported an increase in cyber-attacks on Singapore-based resources from June 11-12, 2018[ii] while the visiting US President met with the leader of North Korea. This insight motivated F5 Networks to focus on future travel by the US President for increases in cyber-attacks leading up to and during his state visits.

CONNECT WITH US

Call +1.800.ORACLE1
or visit oracle.com.
Outside North America,
find your local office at
oracle.com/contact.

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle

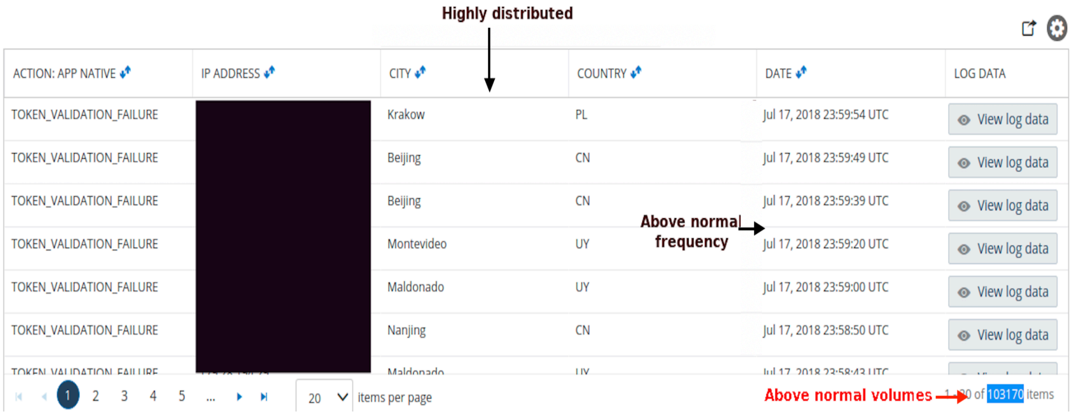
Disclaimer: This document is for informational purposes. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

On July 19, 2018, F5 Networks published an article[iii] regarding information security attacks on Finnish resources before and during the summit between the US and Russian Presidents. While the majority of the attacks reported by F5 Networks were “brute force” attacks targeting IoT devices, other unknown entities attempted to breach credentials and compromise resources across cloud environments used by Finland-based organizations.

If nation states employ low volume and low velocity attacks in highly active cloud services, these attacks can be very hard to detect given the resources at the disposal of the attacker. One such attack involving authentication tokens was detected by Oracle CASB and is described below.

AUTHENTICATION TOKEN THREAT DETECTION BY ORACLE CASB

Oracle’s CASB is actively engaged in monitoring cloud services employed by some Finland-based organizations and identified significant increases in anomalous activities over this period of time. One of our global CASB customers, with a Finland-based HQ, was alerted to threats to user accounts in one of their primary cloud services by attackers attempting to replay user authentication tokens. These low volume token replay attempts from suspicious IP addresses alerted us to perform further research that revealed similar attempts from locations without an associated IP reputation.



Highly distributed

ACTION: APP NATIVE	IP ADDRESS	CITY	COUNTRY	DATE	LOG DATA
TOKEN_VALIDATION_FAILURE	[redacted]	Krakow	PL	Jul 17, 2018 23:59:54 UTC	View log data
TOKEN_VALIDATION_FAILURE	[redacted]	Beijing	CN	Jul 17, 2018 23:59:49 UTC	View log data
TOKEN_VALIDATION_FAILURE	[redacted]	Beijing	CN	Jul 17, 2018 23:59:39 UTC	View log data
TOKEN_VALIDATION_FAILURE	[redacted]	Montevideo	UY	Jul 17, 2018 23:59:20 UTC	View log data
TOKEN_VALIDATION_FAILURE	[redacted]	Maldonado	UY	Jul 17, 2018 23:59:00 UTC	View log data
TOKEN_VALIDATION_FAILURE	[redacted]	Nanjing	CN	Jul 17, 2018 23:58:50 UTC	View log data
TOKEN_VALIDATION_FAILURE	[redacted]	Maldonado	UY	Jul 17, 2018 23:58:43 UTC	

Above normal frequency

Above normal volumes

1 - 20 of 103170 items

Figure 1:Detection of Abnormal Activity by Oracle CASB

Virtual tokens are used between entities for authentication and establishing a trust relationship. If a token is compromised, malicious transactions could be processed as valid ones. Some token validation errors occur as a part of normal operations; for example, when a token expires due to age, and subsequent attempts to use it would fail validation. A common tactic of many types of attacks are to execute “low volume” and “low velocity” transactions that can be difficult to detect in highly-active systems. In this sequence of events, the actor(s) accounted for potential discovery by threat detection systems. The token validation errors were discovered, but only one to three replay events were detected for each token in a 24-hour period.

Integrated Cloud Applications & Platform Services

Authored by Oracle CASB Threat Labs

Oracle's CASB consumed and analyzed over 650 GB of cloud security data over a period of 90 days before and during the Helsinki Summit. Slightly before and during the summit, there was a substantial rise in the attacks against the customer's monitored cloud services. Oracle CASB detected and alerted on a significant number of token validation errors; an increase of 700% from a single country as shown in Figure 2 below.

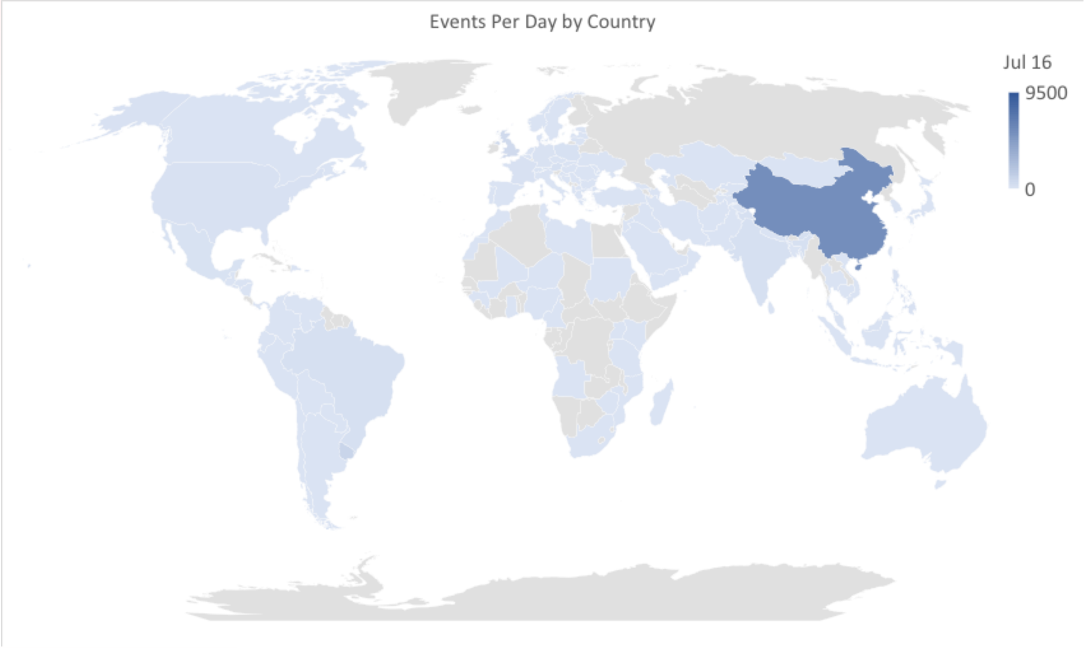


Figure 2: Events per day by Country, July 16th, Day of the Helsinki Summit

Subsequent review of the anomalous activity originating from China revealed many IP addresses had an unusually consistent number of events over the span of a single day with no additional activity before or after that day. Refer to Figure 3 below. Events that are highly normalized in approach methodology, consistency in scale, and focused on a specific event type are indicative of programmatic origins; human usage rarely generates this pattern of activity. Broad use of an application that rotates through hundreds of IP addresses in a token replay attack further implies greater sophistication on the part of the actor.

Integrated Cloud Applications & Platform Services

Authored by Oracle CASB Threat Labs

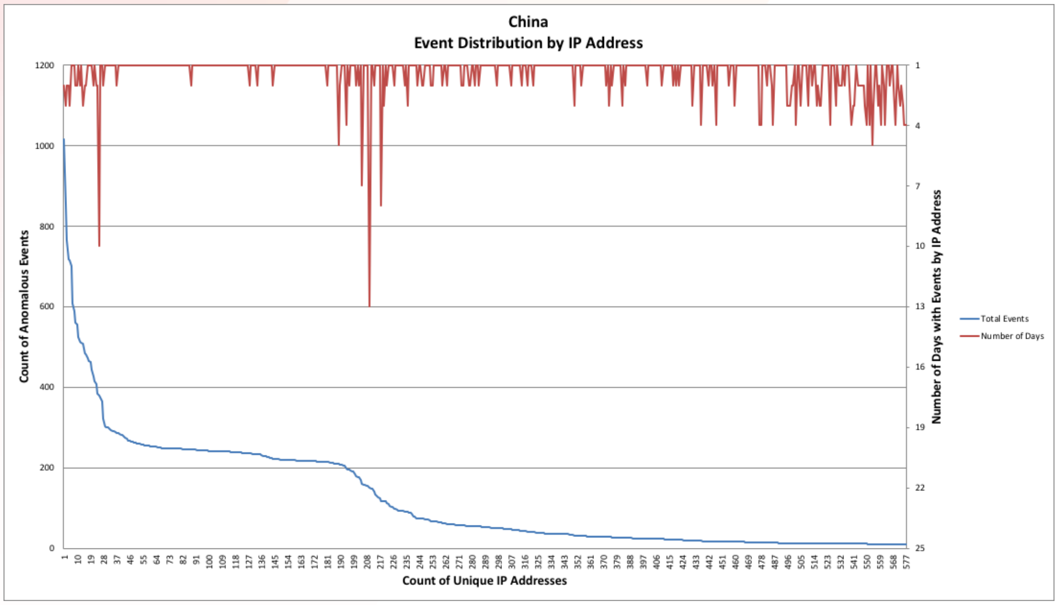


Figure 3: Event Distribution across IP Addresses in China

In contrast, the activity from Finland shows a varying number of events each day, over the same timeframe, across a similar number of unique IP addresses with a drastically different distribution as seen in Figure 4 below.

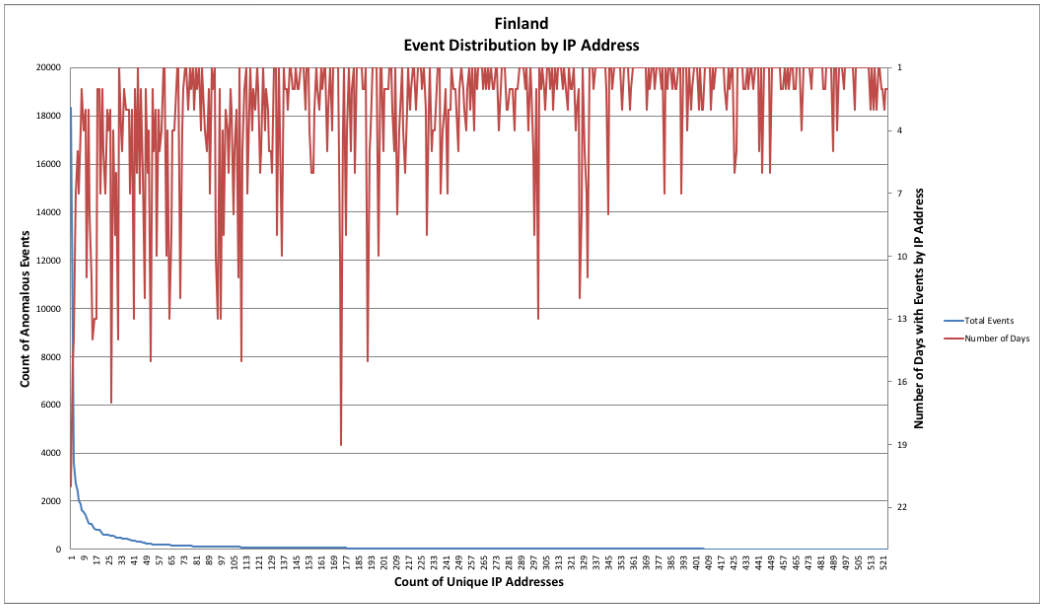


Figure 4: Event Distribution across IP Addresses in Finland

Integrated Cloud Applications & Platform Services

Authored by Oracle CASB Threat Labs

Substantial activity from a small number of IP addresses indicates that these transactions originate from within the organization's IP range. The uniformity of the activity from a single country (China in this case) is readily discernible in comparison with Figure 3: Event Distribution across IP Addresses.

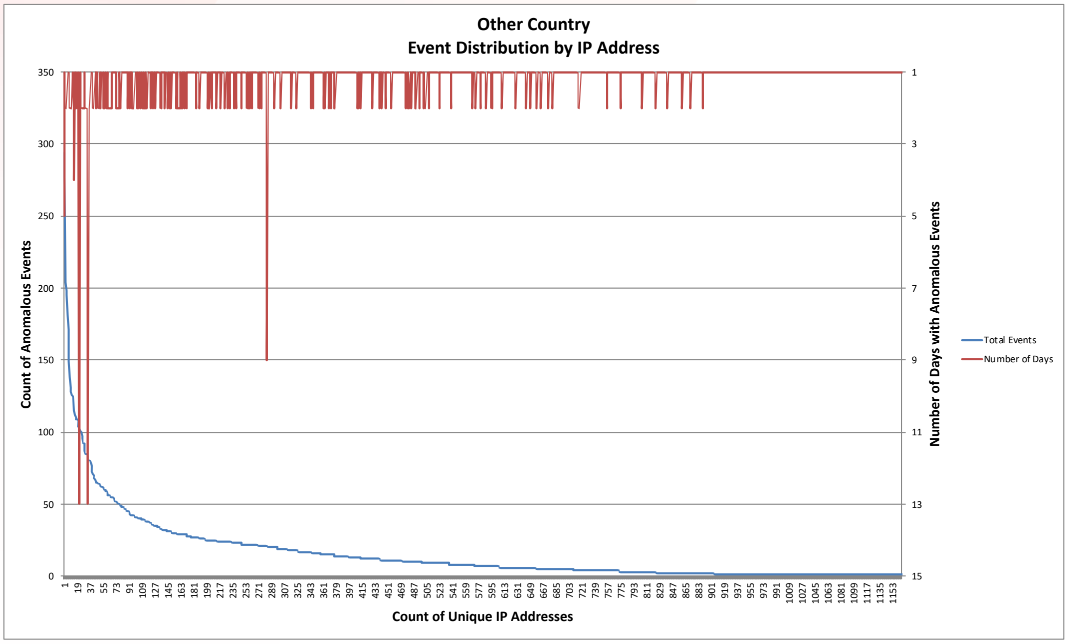


Figure 5: Uniformity of Events

Further research revealed additional "low volume", "low velocity" probing efforts from a third country as seen in Figure 5 above. In this instance, the artificially consistent nature of the activities mirrored by multiple IP addresses indicate an active probe of the cloud applications which were unlikely to cross the threshold of standard threat detection systems.

SUMMARY

It is important to develop a comprehensive information security program and train your team to monitor and research anomalous activities. Given the sheer volume of data and transactions that cloud applications generate, automated tools with machine learning, such as Oracle's CASB Cloud Service, are designed to perform much of the analysis in identifying and alerting the team to suspicious activities from external actors and from valid, authorized users. Machine learning provides the fastest mechanism to detect insider threats and anomalous user behavior.

[i] https://www.us-cert.gov/ncas/alerts/TA18-106A
[ii] https://www.f5.com/labs/articles/threat-intelligence/russian-attacks-against-singapore-spike-during-trump-kim-summit
[iii] https://www.f5.com/labs/articles/threat-intelligence/cyber-attacks-spike-in-finland-before-trump-putin-meeting

Integrated Cloud Applications & Platform Services

Authored by Oracle CASB Threat Labs