Cloud Credential Compromise Campaign Originating from Russian-Affiliated Infrastructure

proofpoint.com/us/blog/cloud-security/cloud-credential-compromise-campaign-originating-russian-affiliated

March 3, 2022

Blog
Cloud Security
Cloud Credential Compromise Campaign Originating from Russian-Affiliated Infrastructure

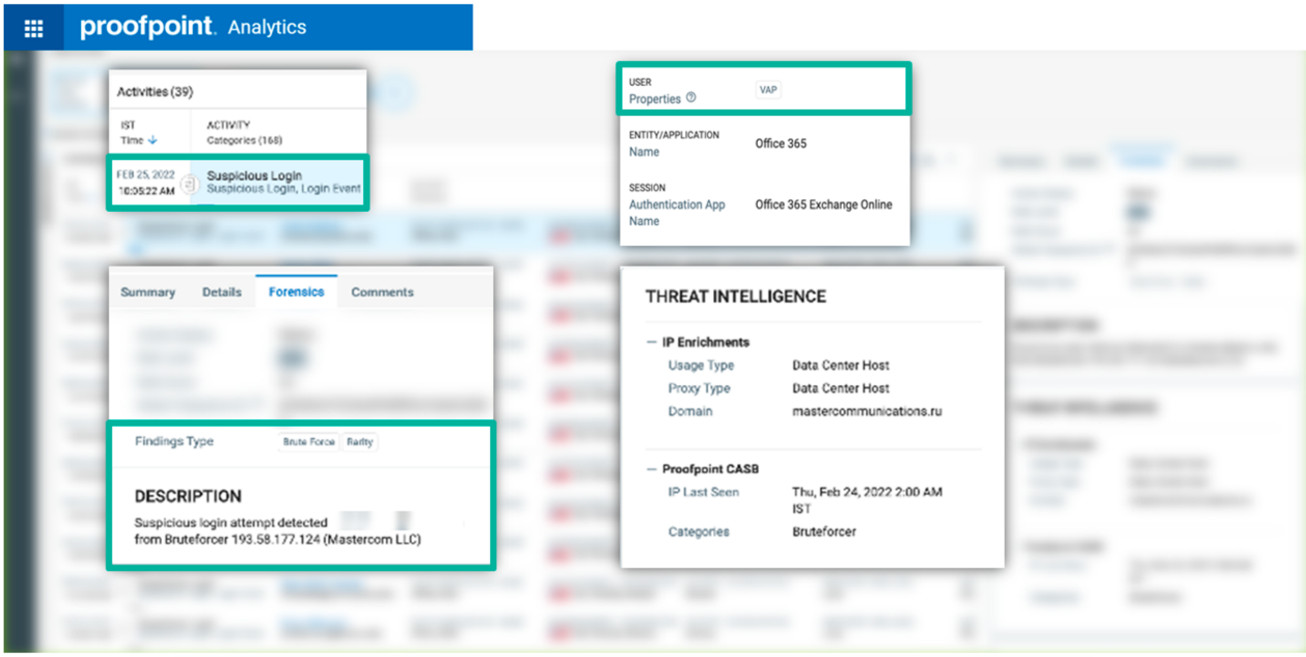
March 03, 2022 Proofpoint Cloud Security Research

Proofpoint Cloud Security group researchers have found widespread cloud credential variance attacks on organizations since February 22, 2022, originating from Russian-affiliated infrastructure. This blog post will explain the very active threat campaign targeting our customers' cloud apps and how to secure your cloud risks.

Attack profile and example attack

As of February 28, 2022, we've observed approximately 78,000 credential variance attacks (i.e. brute force or password spray attempts), targeting 4,340 user accounts across 728 monitored cloud environments. Over 85% of the targeted organizations are US-based, with the remainder operating in other Western countries. The vast majority of attacks either originated from identified Russian sources (IP addresses and DCH services located in Russia) or from servers associated with Russian hosting services, chiefly in the US. In our assessment, unauthorized access could open the door to account takeover, privilege escalation, lateral movement, and data exfiltration.

The screenshot below showcases one of the many attacks we've seen. We detected this threat to the user based on identifying the credential variance attack type, user behavior analytics ,and the user being heavily targeted in the past (the user is a Very Attacked Person , or VAP). In this case, the user has never attempted to log in to their organization's Office 365 account using the hostname “mastercommunications.ru” and a data hosting center (DCH) proxy. In fact, our threat intelligence has identified that as typical for this threat actor.



Activities (39)

IST Time ↓ | ACTIVITY Categories (168)

FEB 25, 2022 10:05:22 AM — Suspicious Login
Suspicious Login, Login Event

USER Properties: VAP

ENTITY/APPLICATION Name: Office 365

SESSION Authentication App Name: Office 365 Exchange Online

Findings Type: Brute Force, Rarity

DESCRIPTION

Suspicious login attempt detected
from Bruteforcer 193.58.177.124 (Mastercom LLC)

THREAT INTELLIGENCE

— IP Enrichments

Usage Type	Data Center Host
Proxy Type	Data Center Host
Domain	mastercommunications.ru

— Proofpoint CASB

IP Last Seen	Thu, Feb 24, 2022 2:00 AM IST
Categories	Bruteforcer

Screenshot: Suspicious login attempts from credential variance attacks detected by Proofpoint CASB viewed on the Information and Cloud Security platform

Targeted industries and other technical analysis

The primary targets have been varied, with no industry accounting for more than 11% of all attacks. The top five most targeted industries account for 44% of all the attacks, including manufacturing, financial services, healthcare, business services, and construction.

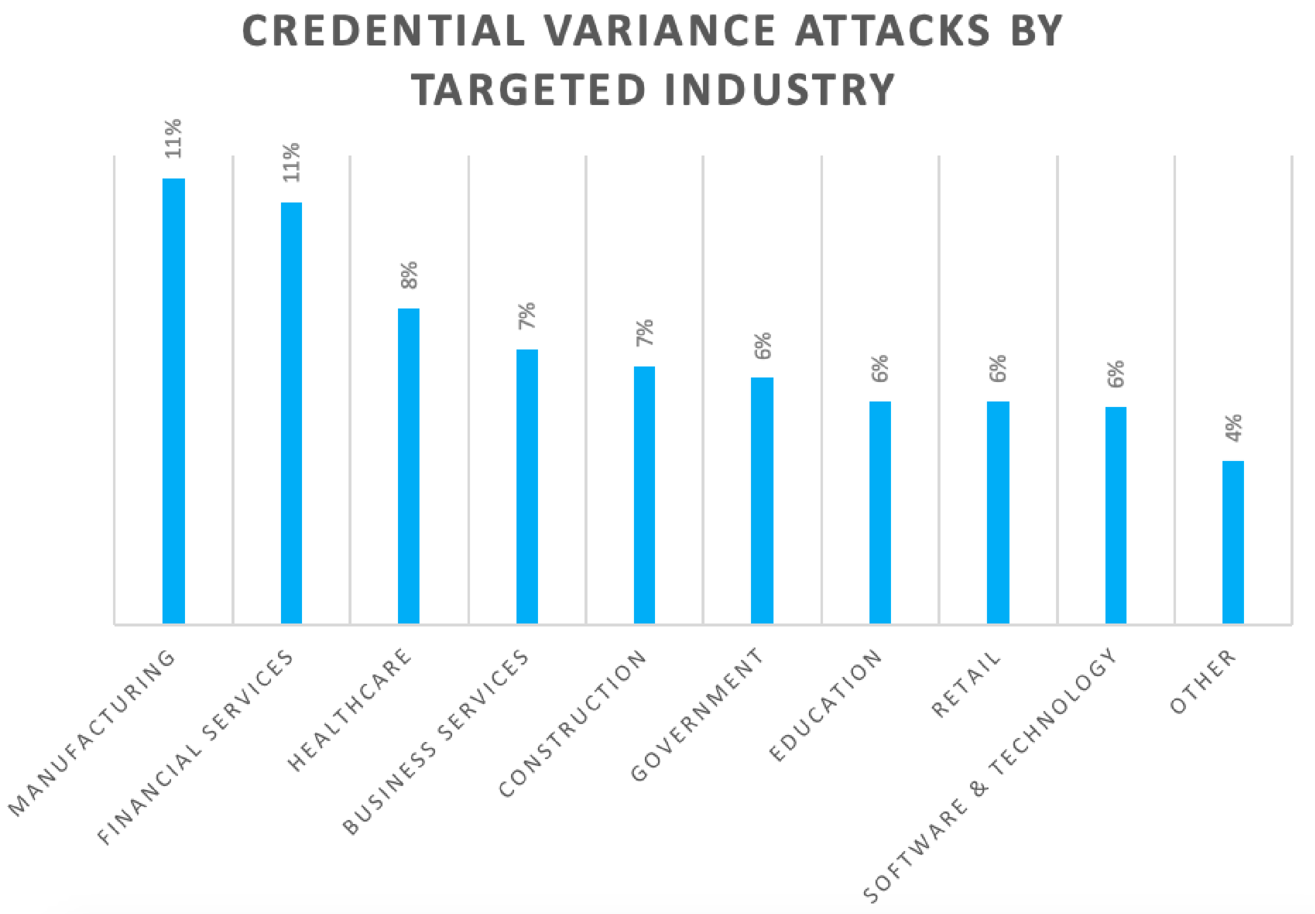


Chart: Proofpoint security research analysis on credential variance attacked by the targeted industry for February 22 – February 28, 2022

A few interesting artifacts of the campaign:

1. An unusual user agent (UA) string – "*14 Windows Mobile - Tablet Very common*" – amongst the many we've seen. We have seen either as a standalone string or appended to the end of a longer UA string. This UA string is unique to this campaign and may be unintentional.
2. The attacks are conducted against users in alphabetic order by username, which may be a trait of the credential variance tool kit used.
3. The malicious targeting attempts are decentralized, with multiple hosting services and operational assets trying to compromise user accounts simultaneously.

Protect your cloud accounts with cloud security best practices

- Treat any traffic from the IOCs listed below as potentially suspicious while this campaign is active.

- Monitor all cloud accounts of your organization for suspicious logins and remediate highly suspicious logins immediately.

- Limit cloud traffic from locations of interest to trusted web infrastructure (IP addresses, ISP hosts).

- Use multi-factor authentication on your cloud services, especially web, customer, or partner-facing applications.

- Set up DLP policies to identify sensitive data exfiltration to unmanaged devices.

- Monitor for suspicious configuration changes to 3rd party OAuth apps, cloud email and cloud servers.

Summarized Indicators of Compromise (IOCs):

ISP / Proxy Service	**Associated Domain**	**IP Address**
Address Management Inc.	clouvider.co.uk	103.151.103.243
Admin LLC	cadmin.ru	213.139.193.38
Auction LLC	dauction.ru	45.87.124.155
B2 Net Solutions Inc.	servermania.com	23.229.53.52
23.229.53.63		
23.229.67.247		
23.229.67.248		
23.229.79.18		
23.229.79.24		
23.229.79.25		
23.229.79.28		
LIR LLC	lir.am	103.152.17.248

Mastercom LLC	mastercommunications.ru	109.94.218.192
193.58.177.124		
OVH US LLC	ovh.com	51.81.45.12
51.81.45.128		
Proline IT Ltd	selectel.ru	176.53.133.249
193.160.216.60		
193.160.217.66		
77.83.4.102		
77.83.5.161		
Qwarta LLC	qwarta.ru	193.232.144.116
194.190.112.167		
194.190.179.10		
194.190.190.64		
194.190.90.41		
194.190.91.222		
194.226.185.120		
195.19.209.226		
212.193.136.39		

212.193.137.253
212.193.140.208
212.193.143.60
62.76.147.174
62.76.153.235

This post will be updated with additional details on observed user agents.

Is your organization protected from cloud credentialing attacks? Learn about Cloud Account Defense.

Subscribe to the Proofpoint Blog