# SOC Report: Password Spray Attempt on finallabscott

### Date Range Investigated:

- Primary scope: Last 24 hours
- Extended scope: 7 days (for context and IOC verification)

### **Device Investigated:**

- finallabscott (Internet-facing, unmanaged, no MDE enrollment)
- Alert: High-severity Password Spray (Mar 29, 2025, 3:30 PM)

## Summary of Findings

- Repeated LogonFailed events via Network logon type detected.
- Targeted account: guest
- Top 5 brute force source IPs:
  - o 218.92.0.186 China 896 attempts
  - o 218.92.0.187 China 616 attempts
  - o 218.92.0.187 China 346 attempts
  - o 61.177.172.244 China 299 attempts
  - 5.178.87.180 Russia 88 attempts
- Device logs show no successful logon from any of the flagged IPs.
- Activity also observed on additional VMs, but only guest logons failed. No elevation or shell activity.

#### Confirmed

- Attack Type: Password Spray
- Result: No compromise
- Persistence Evidence: None
- Shell/Beaconing C2: None
- Risk Factors: Internet-facing, no MDE coverage, active guest account

#### **Defensive Recommendation**

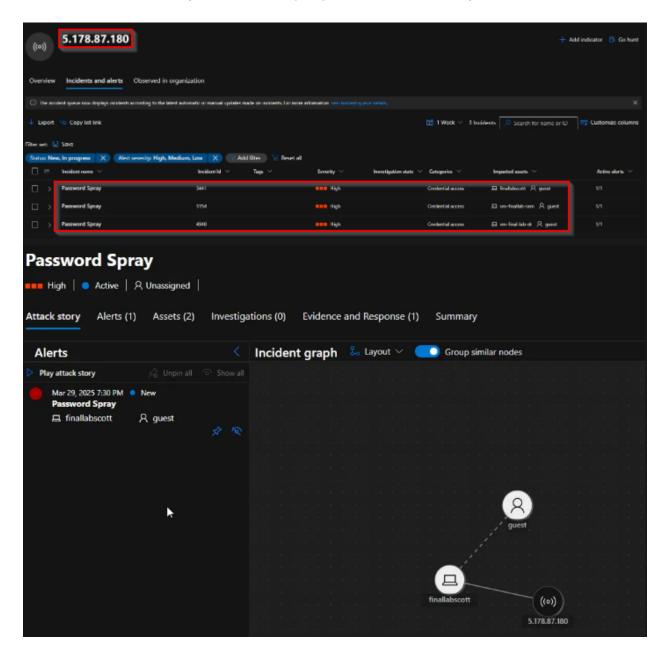
- Disable unused accounts (e.g., Guest).
- Enforce account lockout policies to mitigate spray attempts.



## **MITRE Mapping**

• T1110.003 - Brute Force: Password Spraying

# Alert Confirmation (Password Spray on finallabscott)



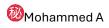
# Summary of Brute Force IPs – Lots of Activity

```
DeviceLogonEvents
| where LogonType == "Network"
| where ActionType == "LogonFailed"
| where isnotempty(RemoteIP)
| where RemoteIP != "10.0.0.8" //Attack Engine Noise Removed, Filter External IPS
| extend GeoInfo = geo_info_from_ip_address(RemoteIP)
| extend Country = tostring(GeoInfo.country), City = tostring(GeoInfo.city)
| summarize Attempts = count() by ActionType, RemoteIP, DeviceName, Country, City
| order by Attempts desC
```

							1827 items
Filters:	Filters:   Add filter						
	ActionType	RemotelP	DeviceName	Country	City	Attempts	
	> LogonFailed	(o) 218.92.0.186	☐ linux-target-1.p2zfvs	China		896	
	> LogonFailed	(w) 218.92.0.187	□ bigfeelinux.p2zfvso0	China		616	
	> LogonFailed	(°) 218.92.0.187	☐ dt-linux-test.p2zfvso ☐	China		346	
	> LogonFailed	(**) 58.33.67.164	☐ fredlc-windows1	China	Shanghai	299	
	> LogonFailed	(o) 134.199.144.100	☐ linux-vm-test-ac.p2zf	Australia	Sydney	151	
	> LogonFailed	(w) 31.184.215.139	🚨 dan-win-10	Russia	St Petersburg	151	
	> LogonFailed	(**) 31.184.215.185		Russia	St Petersburg	149	
	> LogonFailed	(**) 31.184.218.81	➡ severance-2025	Russia	St Petersburg	149	
	> LogonFailed	(**) 209.38.95.188	☐ dt-linux-test.p2zfvso	Australia	Sydney	146	
	> LogonFailed	( <b>o</b> ) 115.239.62.6	₽ vm1	China		145	
	> LogonFailed	(**) 77.90.185.229	□ mm-edr-test	Germany		139	
	> LogonFailed	(**) 170.64.233.183	☐ gonsalvrlinx.p2zfvso0	Australia	Sydney	138	
	> LogonFailed	(**) 31.184.215.139	☐ ir-sentinel-moa	Russia	St Petersburg	137	
	> LogonFailed	(**) 31.184.218.81	☐ dan-win-10	Russia	St Petersburg	130	
	> LogonFailed	(**) 158.69.165.242	□ britt-windows10	Canada	Montreal	129	
	> LogonFailed	(**) 115.187.35.6	<b>□</b> win-vm-mde	India	Kolkata	124	
	> LogonFailed	(**) 170.64.229.4	☐ linux-vm-vulnerabilit	Australia	Sydney	122	
	> LogonFailed	(o) 218.92.0.187	☐ linux-target-1.p2zfvs	China		119	
	> LogonFailed	(o) 143.110.188.143	☐ brian-linux-vm-scan	India	Bengaluru	111	
	> LogonFailed	(**) 31.184.215.139	➡ sa-mde-test-2	Russia	St Petersburg	111	
	> LogonFailed	(**) 95.143.190.228	🖴 win-vm-mde	Russia	Moscow	111	
	> LogonFailed	(°) 185.7.214.14	₽ vm1	Russia		110	



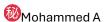
Actio	пТуре	RemotelP	DeviceName	Country	City	Attemp
>	LogonFailed	(•0) 190.181.24.50	□ whibbert-edr-md	Bolivia	Santa Cruz	100
>	LogonFailed	(×) 77.223.118.28	☐ whibbert-edr-md  ☐ and a second control of the second cont	Russia	Moscow	83
Þ	LogonFailed	(×) 91.238.181.8	□ whibbert-edr-md	France		80
>	LogonFailed	(w) 45.227.254.3		Panama		44
>	LogonFailed	№ 182.160.114.213	□ whibbert-edr-md	Bangladesh	Dhaka	34
>	LogonFailed	(w) 188.124.36.148	A whibbert-edr-md	Russia	St Petersburg	30
>	LogonFailed	( <b>→</b> ) 5.182.5.119	A whibbert-edr-md	Russia	St Petersburg	29
>	LogonFailed	(×) 5.182.4.154	■ whibbert-edr-md	Russia	St Petersburg	16
>	LogonFailed	<b>№</b> 31.184.218.81		Russia	St Petersburg	16
>	LogonFailed	(w) 45.92.177.109	□ whibbert-edr-md	Russia	St Petersburg	16
>	LogonFailed	(w) 185.137.233.87	A whibbert-edr-md	Russia	St Petersburg	16
>	LogonFailed	(w) 95.143.190.228	□ whibbert-edr-md	Russia	Moscow	15
>	LogonFailed	(≈) 95.143.191.159	□ whibbert-edr-md	Russia	Moscow	15
>	LogonFailed	(×) 5.178.87.180	☐ whibbert-edr-md	Russia	St Petersburg	13
>	LogonFailed	<b>№</b> 92.42.15.193		Russia	Moscow	13
>	LogonFailed	(×0) 31.184.215.139	□ whibbert-edr-md	Russia	St Petersburg	12
>	LogonFailed	(≈0 31.184.215.185	□ whibbert-edr-md	Russia	St Petersburg	11
>	LogonFailed	<b>№</b> 31.184.215.241	A whibbert-edr-md	Russia	St Petersburg	11
>	LogonFailed	(w) 41.219.184.18	■ whibbert-edr-md	Nigeria	Lagos	8
>	LogonFailed	<b>№)</b> 185.42.12.5		United Arab Emirates		4
>	LogonFailed	(w) 85.185.33.244	□ whibbert-edr-md	Iran		3
>	LogonFailed	(w) 10.0.8.5				2



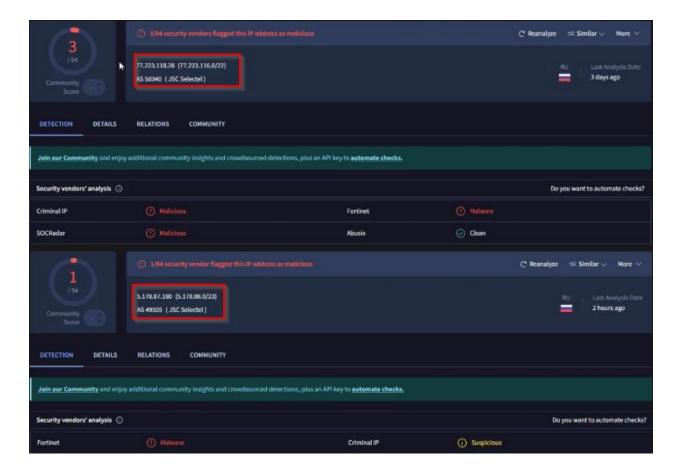
# No Successful Logons from Attackers

```
let RemoteIPsInQuestion = dynamic(["190.181.24.50", "5.178.87.180",
"77.223.118.28"]);
DeviceLogonEvents
| where ActionType == "LogonSuccess"
| where RemoteIP has_any(RemoteIPsInQuestion)
| project Timestamp, DeviceName, RemoteIP, AccountName
| order by Timestamp desc
```

A				
>	Mar 29, 2025 7:30:	☐ finallabscott	(•) 5.178.87.180	guest
>	Mar 29, 2025 7:30:	📮 finallabscott	( <b>••)</b> 5.178.87.180	guest
>	Mar 29, 2025 4:44:	□ vm-enterprise-s	( <b>o</b> ) 5.178.87.180	guest
>	Mar 29, 2025 4:44:		( <b>o</b> ) 5.178.87.180	guest
>	Mar 29, 2025 2:10:	🚨 vm-final-lab-ke	( <b>o</b> ) 5.178.87.180	guest
>	Mar 29, 2025 2:10:	🚨 vm-final-lab-ke	( <b>o</b> ) 5.178.87.180	guest
>	Mar 28, 2025 9:33:		( <b>o</b> ) 5.178.87.180	guest
>	Mar 28, 2025 9:33:	■ winserver-final	( <b>o</b> ) 5.178.87.180	guest
>	Mar 27, 2025 12:5	🚨 vm-finallab-sam	( <b>o</b> ) 5.178.87.180	guest
>	Mar 27, 2025 12:5	🚨 vm-finallab-sam	( <b>o</b> ) 5.178,87.180	guest
>	Mar 26, 2025 2:02:	🖴 sb-wins-vul	( <b>o</b> ) 5.178.87.180	guest
>	Mar 26, 2025 2:02:	🚨 sb-wins-vul	( <b>o</b> ) 5.178.87.180	guest
>	Mar 25, 2025 9:00:	□ vm-finallab-ste	( <b>o</b> ) 5.178.87.180	guest
>	Mar 25, 2025 9:00:	□ vm-finallab-ste	(w) 5.178.87.180	guest
>	Mar 24, 2025 9:49:	□ vm-abel	( <b>o</b> ) 5.178.87.180	guest
>	Mar 24, 2025 9:49:	₽ vm-abel	( <b>(*)</b> 5.178.87.180	guest
>	Mar 24, 2025 5:41:	□ vm-final-lab-dr	( <b>o</b> ) 5.178.87.180	guest
>	Mar 24, 2025 5:41:	☐ vm-final-lab-dr	(o) 5.178.87.180	guest



## IOC Confirmation - VirusTotal



Report Compiled By:
Mohammed A
Cyber Security Support Engineer (Intern)
LOG(N) Pacific | Cyber Range

Date: 30/03/2025