

# 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:
  - 218.92.0.186 – China – 896 attempts
  - 218.92.0.187 – China – 616 attempts
  - 218.92.0.187 – China – 346 attempts
  - 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)

The screenshot displays the Microsoft Sentinel interface. At the top, the IP address **5.178.87.180** is highlighted in a red box. Below the navigation tabs, a message states: "The incident queue now displays incidents according to the latest automatic or manual updates made on incidents. For more information, see incident queue details." Below this, there are links for "Report" and "Copy list link". A filter bar shows "1 Week" and "3 incidents". A search bar contains "Search for name or ID". A table lists incidents, with the first three rows highlighted in red:

Incident name	Incident ID	Severity	Investigation state	Categories	Impacted assets	Active alerts
Password Spray	5441	High		Credential access	finallabscott, guest	1/1
Password Spray	5754	High		Credential access	vm-finallab-scott, guest	1/1
Password Spray	4940	High		Credential access	vm-finallab-scott, guest	1/1

Below the table, the "Password Spray" incident details are shown. The status is "High", and it is "Active" and "Unassigned". The "Attack story" tab is selected, showing a timeline of events. The "Incident graph" tab is also visible, showing a network diagram with nodes for "guest", "finallabscott", and "5.178.87.180".

## 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
```

Export Show empty columns 1827 items

Filters: Add filter

ActionType	RemoteIP	DeviceName	Country	City	Attempts
> LogonFailed	(id) 218.92.0.186	linux-target-1.p2zfs...	China		896
> LogonFailed	(id) 218.92.0.187	bigfeelinix.p2zfs0...	China		616
> LogonFailed	(id) 218.92.0.187	dt-linux-test.p2zfs...	China		346
> LogonFailed	(id) 58.33.67.164	fredlc-windows1	China	Shanghai	299
> LogonFailed	(id) 134.199.144.100	linux-vm-test-ac.p2zf...	Australia	Sydney	151
> LogonFailed	(id) 31.184.215.139	dan-win-10	Russia	St Petersburg	151
> LogonFailed	(id) 31.184.215.185	kashuser	Russia	St Petersburg	149
> LogonFailed	(id) 31.184.218.81	severance-2025	Russia	St Petersburg	149
> LogonFailed	(id) 209.38.95.188	dt-linux-test.p2zfs...	Australia	Sydney	146
> LogonFailed	(id) 115.239.62.6	vm1	China		145
> LogonFailed	(id) 77.90.185.229	mm-edr-test	Germany		139
> LogonFailed	(id) 170.64.233.183	gonsalvrlinx.p2zfs0...	Australia	Sydney	138
> LogonFailed	(id) 31.184.215.139	ir-sentinel-moa	Russia	St Petersburg	137
> LogonFailed	(id) 31.184.218.81	dan-win-10	Russia	St Petersburg	130
> LogonFailed	(id) 158.69.165.242	britt-windows10	Canada	Montreal	129
> LogonFailed	(id) 115.187.35.6	win-vm-mde	India	Kolkata	124
> LogonFailed	(id) 170.64.229.4	linux-vm-vulnerabilit...	Australia	Sydney	122
> LogonFailed	(id) 218.92.0.187	linux-target-1.p2zfs...	China		119
> LogonFailed	(id) 143.110.188.143	brian-linux-vm-scan...	India	Bengaluru	111
> LogonFailed	(id) 31.184.215.139	sa-mde-test-2	Russia	St Petersburg	111
> LogonFailed	(id) 95.143.190.228	win-vm-mde	Russia	Moscow	111
> LogonFailed	(id) 185.7.214.14	vm1	Russia		110

ActionType	RemoteIP	DeviceName	Country	City	Attempt
> LogonFailed	(ip) 190.181.24.50	whibbert-edr-md	Bolivia	Santa Cruz	100
> LogonFailed	(ip) 77.223.118.28	whibbert-edr-md	Russia	Moscow	83
> LogonFailed	(ip) 91.238.181.8	whibbert-edr-md	France		80
> LogonFailed	(ip) 45.227.254.3	whibbert-edr-md	Panama		44
> LogonFailed	(ip) 182.160.114.213	whibbert-edr-md	Bangladesh	Dhaka	34
> LogonFailed	(ip) 188.124.36.148	whibbert-edr-md	Russia	St Petersburg	30
> LogonFailed	(ip) 5.182.5.119	whibbert-edr-md	Russia	St Petersburg	29
> LogonFailed	(ip) 5.182.4.154	whibbert-edr-md	Russia	St Petersburg	16
> LogonFailed	(ip) 31.184.218.81	whibbert-edr-md	Russia	St Petersburg	16
> LogonFailed	(ip) 45.92.177.109	whibbert-edr-md	Russia	St Petersburg	16
> LogonFailed	(ip) 185.137.233.87	whibbert-edr-md	Russia	St Petersburg	16
> LogonFailed	(ip) 95.143.190.228	whibbert-edr-md	Russia	Moscow	15
> LogonFailed	(ip) 95.143.191.159	whibbert-edr-md	Russia	Moscow	15
> LogonFailed	(ip) 5.178.87.180	whibbert-edr-md	Russia	St Petersburg	13
> LogonFailed	(ip) 92.42.15.193	whibbert-edr-md	Russia	Moscow	13
> LogonFailed	(ip) 31.184.215.139	whibbert-edr-md	Russia	St Petersburg	12
> LogonFailed	(ip) 31.184.215.185	whibbert-edr-md	Russia	St Petersburg	11
> LogonFailed	(ip) 31.184.215.241	whibbert-edr-md	Russia	St Petersburg	11
> LogonFailed	(ip) 41.219.184.18	whibbert-edr-md	Nigeria	Lagos	8
> LogonFailed	(ip) 185.42.12.5	whibbert-edr-md	United Arab Emirates		4
> LogonFailed	(ip) 85.185.33.244	whibbert-edr-md	Iran		3
> LogonFailed	(ip) 10.0.8.5	whibbert-edr-md			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
```

>	Mar 29, 2025 7:30:...	 finallabscott	(∞) 5.178.87.180	guest
>	Mar 29, 2025 7:30:...	 finallabscott	(∞) 5.178.87.180	guest
>	Mar 29, 2025 4:44:...	 vm-enterprise-s	(∞) 5.178.87.180	guest
>	Mar 29, 2025 4:44:...	 vm-enterprise-s	(∞) 5.178.87.180	guest
>	Mar 29, 2025 2:10:...	 vm-final-lab-ke	(∞) 5.178.87.180	guest
>	Mar 29, 2025 2:10:...	 vm-final-lab-ke	(∞) 5.178.87.180	guest
>	Mar 28, 2025 9:33:...	 winserver-final	(∞) 5.178.87.180	guest
>	Mar 28, 2025 9:33:...	 winserver-final	(∞) 5.178.87.180	guest
>	Mar 27, 2025 12:5:...	 vm-finallab-sam	(∞) 5.178.87.180	guest
>	Mar 27, 2025 12:5:...	 vm-finallab-sam	(∞) 5.178.87.180	guest
>	Mar 26, 2025 2:02:...	 sb-wins-vul	(∞) 5.178.87.180	guest
>	Mar 26, 2025 2:02:...	 sb-wins-vul	(∞) 5.178.87.180	guest
>	Mar 25, 2025 9:00:...	 vm-finallab-ste	(∞) 5.178.87.180	guest
>	Mar 25, 2025 9:00:...	 vm-finallab-ste	(∞) 5.178.87.180	guest
>	Mar 24, 2025 9:49:...	 vm-abel	(∞) 5.178.87.180	guest
>	Mar 24, 2025 9:49:...	 vm-abel	(∞) 5.178.87.180	guest
>	Mar 24, 2025 5:41:...	 vm-final-lab-dr	(∞) 5.178.87.180	guest
>	Mar 24, 2025 5:41:...	 vm-final-lab-dr	(∞) 5.178.87.180	guest

## IOC Confirmation - VirusTotal

The image displays two screenshots of the VirusTotal web interface, showing the analysis results for two different IP addresses. Both screenshots are in dark mode.

**Top Screenshot:**

- Community Score:** 3 / 94
- IP Address:** 77.223.118.26 (77.223.116.0/22)
- AS:** AS 50340 (JSC Selectel)
- Country:** RU (Russia)
- Last Analysis Date:** 3 days ago
- Security vendors' analysis:** 3/94 security vendors flagged this IP address as malicious.
- Detections:**
  - Criminal IP: Malicious
  - SOCradar: Malicious
  - Fortinet: Malware
  - Abusix: Clean

**Bottom Screenshot:**

- Community Score:** 1 / 94
- IP Address:** 5.178.87.180 (5.178.86.0/23)
- AS:** AS 49505 (JSC Selectel)
- Country:** RU (Russia)
- Last Analysis Date:** 2 hours ago
- Security vendors' analysis:** 1/94 security vendor flagged this IP address as malicious.
- Detections:**
  - Fortinet: Malware
  - Criminal IP: Suspicious

Report Compiled By:

Mohammed A

Cyber Security Support Engineer (Intern)

LOG(N) Pacific | Cyber Range

Date: 30/03/2025