Microsoft Security

Multi-stage incident involving Execution & Lateral movement on one endpoint reported by multiple sources

PDF file generated on Jul 1, 2025 4:44 PM Timestamps are generated in UTC-5

🟥🟥🟥 High | ● Active | Unassigned | Attack Disruption

Contents

Overview

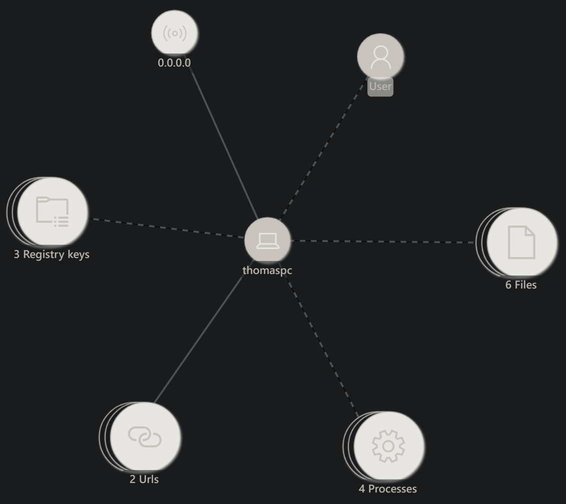
Incident details

Severity	High
Status	Active
Assigned to	-
Incident ID	68
Classification	Not set
Categories	Execution, Defense evasion, Credential access, Discovery, Lateral movement
Time created	Jun 27, 2025 3:29 PM
First activity	Jun 27, 2025 3:29 PM
Last activity	Jun 27, 2025 3:42 PM
Description	A contained user’s attempt to connect remotely to multiple devices was automatically blocked by attack disruption. An attacker might be trying to move laterally within your network by initiating remote sessions to various services.

Attack story

Attack story graph

MITRE categories	Number of alerts	Impacted assets	Evidence
5	17	2	5



Association
A relationship between two entities based on affiliation of one entity to another

Communication
Transmission of data between entities

Threat categories

5 threat categories

Alerts and categories

Active alerts
17/17

Tactics
5

Other categories
0

MITRE ATT&CK tactics

Execution, Defense evasion, Credential access, Discovery, Lateral movement

Other categories

No categories found

Execution 4 / 17

Defense evasion 2 / 17

Credential access 9 / 17

Discovery 1 / 17

Lateral movement 1 / 17

Scope

Impacted assets

2 impacted assets

Devices	Users
1	1

Devices

Device name	Device ID	Risk level↑	Exposure level	OS Platform	Tags	First activity	Last activity	Related alerts
thomaspc	a1f5210 94cf86a8 7614e4...	High	Medium	Windows 11		Jun 27, 2025 3:29 PM	Jun 27, 2025 3:42 PM	17/17

Users

User	Domain	Status	Priority↑	Email	Title	Department
user	thomaspc					

Evidence and response

Evidence

34 evidence

Files	IP Addresses	Processes	Registry Keys	URLs
6	1	22	3	2

Top evidence

First seen↓	Entity	Entity type	Verdict	Remediation status	Impacted assets	Detection origin
Jun 27, 2025 3:29 PM	0.0.0.0	IP Addresses	Suspicious		thomaspc,	Lateral movement using remo...
Jun 27, 2025 3:39 PM	sam	Files	Suspicious	Active	thomaspc,	Suspicious registry export,...
Jun 27, 2025 3:39 PM	reg.exe (PID: 8600)	Processes	Suspicious	Active	thomaspc,	Suspicious registry export,...
Jun 27, 2025 3:39 PM	sam	Registry Keys	Suspicious	Active	thomaspc,	Suspicious registry export
Jun 27, 2025 3:39 PM	reg.exe (PID: 7540)	Processes	Suspicious	Active	thomaspc,	Suspicious registry export,...
Jun 27, 2025 3:39 PM	system	Files	Suspicious	Active	thomaspc,	Suspicious registry export,...
Jun 27, 2025 3:39 PM	system	Registry Keys	Suspicious	Active	thomaspc,	Suspicious registry export
Jun 27, 2025 3:39 PM	cmd.exe (PID: 9848)	Processes	Suspicious	Active	thomaspc,	Suspicious PowerShell command...
Jun 27, 2025 3:39 PM	reg.exe (PID: 9840)	Processes	Suspicious	Active	thomaspc,	Suspicious PowerShell command...
Jun 27, 2025 3:39 PM	security	Files	Suspicious	Active	thomaspc,	Suspicious PowerShell command...
Jun 27, 2025 3:39 PM	security	Registry Keys	Suspicious	Active	thomaspc,	Suspicious registry export
Jun 27, 2025 3:40 PM	powershell.exe (PID: 10064)	Processes	Suspicious	Active	thomaspc,	Suspicious PowerShell command...

Top evidence

First seen↓	Entity	Entity type	Verdict	Remediation status	Impacted assets	Detection origin
Jun 27, 2025 3:40 PM	certutil.exe (PID: 6344)	Processes	Suspicious	Active	thomaspc,	Sensitive information theft activit...
Jun 27, 2025 3:40 PM	cmd.exe (PID: 3696)	Processes	Suspicious	Active	thomaspc,	Sensitive information theft activit...
Jun 27, 2025 3:40 PM	certutil.exe (PID: 9600)	Processes	Suspicious	Active	thomaspc,	Sensitive information theft activit...
Jun 27, 2025 3:40 PM	certutil.exe (PID: 10188)	Processes	Suspicious	Active	thomaspc,	Sensitive information theft activit...
Jun 27, 2025 3:40 PM	certutil.exe (PID: 7884)	Processes	Suspicious	Active	thomaspc,	Sensitive information theft activit...
Jun 27, 2025 3:40 PM	certutil.exe (PID: 9504)	Processes	Suspicious	Active	thomaspc,	Sensitive information theft activit...
Jun 27, 2025 3:40 PM	certutil.exe (PID: 7908)	Processes	Suspicious	Active	thomaspc,	Sensitive information theft activit...
Jun 27, 2025 3:40 PM	certutil.exe (PID: 9572)	Processes	Suspicious	Active	thomaspc,	Sensitive information theft activit...
Jun 27, 2025 3:40 PM	certutil.exe (PID: 6124)	Processes	Suspicious	Active	thomaspc,	Sensitive information theft activit...
Jun 27, 2025 3:40 PM	certutil.exe (PID: 6716)	Processes	Suspicious	Active	thomaspc,	Sensitive information theft activit...
Jun 27, 2025 3:40 PM	certutil.exe (PID: 9500)	Processes	Suspicious	Active	thomaspc,	Sensitive information theft activit...
Jun 27, 2025 3:40 PM	powershell.exe (PID: 7232)	Processes	Suspicious	Active	thomaspc,	Reading files from volume shadow...

Top evidence

First seen↓	Entity	Entity type	Verdict	Remediation status	Impacted assets	Detection origin
Jun 27, 2025 3:40 PM	SAM	Files	Suspicious	Active	thomaspc,	Reading files from volume shadow...
Jun 27, 2025 3:40 PM	SAM	Files	Suspicious	Active	thomaspc,	Reading files from volume shadow...
Jun 27, 2025 3:40 PM	SAM	Files	Suspicious	Active	thomaspc,	Reading files from volume shadow...
Jun 27, 2025 3:40 PM	https://raw.githubusercontent.com/S3cur3T...	URLs	Suspicious	Active	thomaspc,	Password spraying, A script with...
Jun 27, 2025 3:40 PM	powershell.exe (PID: 7660)	Processes	Suspicious	Active	thomaspc,	Password spraying, A script with...
Jun 27, 2025 3:40 PM	https://raw.githubusercontent.com/S3cur3T...	URLs	Suspicious	Active	thomaspc,	Password spraying, A script with...
Jun 27, 2025 3:40 PM	reg.exe (PID: 2408)	Processes	Suspicious	Active	thomaspc,	Suspicious export of SAM data...
Jun 27, 2025 3:42 PM	reg.exe (PID: 6980)	Processes	Suspicious	Active	thomaspc,	Suspicious registry export
Jun 27, 2025 3:42 PM	reg.exe (PID: 7908)	Processes	Suspicious	Active	thomaspc,	Suspicious registry export
Jun 27, 2025 3:42 PM	cmd.exe (PID: 8072)	Processes	Suspicious	Active	thomaspc,	Suspicious registry export,...

Supporting data

17 Active alerts

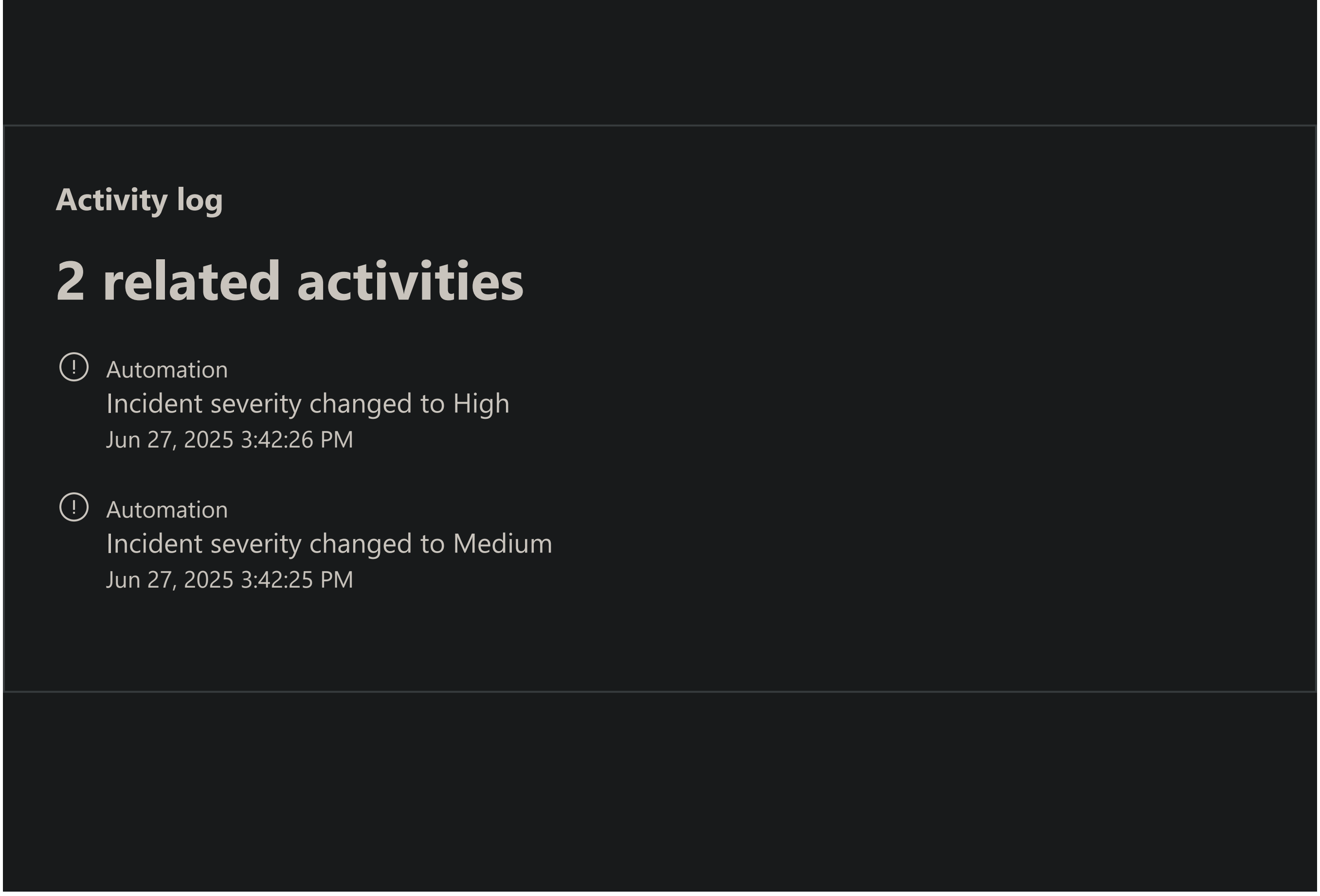
▮ Informational	▮ Low	▮ Medium	▮ High
1	2	12	2

All alerts

Alert name	Severity	Status	Detection	Impacted assets	First activity	Last activity↓
Lateral movement using remote logon by contained user...	Informational	New	MTP	thomaspc, user	Jun 27, 2025 3:29 PM	Jun 27, 2025 3:29 PM
Sensitive data was extracted from registry	Medium	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:39 PM	Jun 27, 2025 3:39 PM
Sensitive information lookup	Medium	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:39 PM	Jun 27, 2025 3:39 PM
Sensitive information theft activity via Securit...	Medium	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:40 PM	Jun 27, 2025 3:40 PM
Reading files from volume shadow copies	Medium	New	WindowsDefenderAtp	thomaspc, S-1-5-21-2078776141-3614560317-...	Jun 27, 2025 3:40 PM	Jun 27, 2025 3:40 PM
Suspicious PowerShell command line	Medium	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:39 PM	Jun 27, 2025 3:40 PM
Suspicious sequence of exploration...	Low	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:39 PM	Jun 27, 2025 3:40 PM
A script with suspicious content was observed	Medium	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:40 PM	Jun 27, 2025 3:40 PM
Suspicious PowerShell command line	Medium	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:40 PM	Jun 27, 2025 3:40 PM
Password spraying	Medium	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:40 PM	Jun 27, 2025 3:40 PM
Possible Antimalware Scan Interface (AMSI)...	High	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:40 PM	Jun 27, 2025 3:40 PM
Possible Antimalware Scan Interface (AMSI)...	High	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:40 PM	Jun 27, 2025 3:40 PM

All alerts

Alert name	Severity	Status	Detection	Impacted assets	First activity	Last activity↓
A malicious PowerShell Cmdlet was invoked on th...	Medium	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:40 PM	Jun 27, 2025 3:40 PM
Suspicious registry export	Medium	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:39 PM	Jun 27, 2025 3:40 PM
Suspicious export of SAM data from registry	Low	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:40 PM	Jun 27, 2025 3:40 PM
Suspicious registry export	Medium	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:39 PM	Jun 27, 2025 3:42 PM
Suspicious registry export	Medium	New	WindowsDefenderAtp	thomaspc, User	Jun 27, 2025 3:39 PM	Jun 27, 2025 3:42 PM



Activity log

2 related activities

Automation
Incident severity changed to High
Jun 27, 2025 3:42:26 PM

Automation
Incident severity changed to Medium
Jun 27, 2025 3:42:25 PM