

Time ↗	Name ↑↓	Severity ↑↓	Status ↑↓	Verdict ↑↓	Assignee	Actions
Mar 21st 2025 at 13:58	Double-Extension File Creation	High	⌚ Closed	✓ True Positive	You (L1)	🔗 ⚡
Description:		This rule detects a creation of a double-extension file like '*.pdf.exe' or '*.gif.lnk', often used by hackers in phishing attacks to trick users into opening the malicious executable.				
Host:	LPT-HR-009					
Process Name:	chrome.exe					
Process User:	S.Conway					
Target File:	C:\Users\S.Conway\Downloads\cats2025.mp4.exe					
File MotW:	https://freecatvideoshd.monster/cats2025.mp4.exe					
File MD5:	14d8486f3f63875ef93cf240c5dc10b					
Comment:	<ul style="list-style-type: none"> <li>- Provide training to prod</li> <li>- Block email</li> </ul>					
Mar 21st 2025 at 13:30	Potential Data Exfiltration	Critical	⌚ Closed	✗ False Positive	You (L1)	🔗 ⚡
Description:		This rule detects 5 or more gigabytes of data sent from a single device to a single destination within a day, which may indicate data exfiltration to untrusted location.				
Destination:	*.zoom.us					
Source IP:	192.168.45.66					
Source Network:	UK04/MEETINGROOM					
Sent Data:	5.8 GB					
Received Data:	5.2 GB					
Comment:	<ul style="list-style-type: none"> <li>- Who: Clients and managers</li> <li>- When: March 21, 2025</li> <li>- Where: Meeting Room Facility</li> <li>- Why: The Data are from data consumed by online meeting bandwidth.</li> </ul>					
Mar 21st 2025 at 13:02	Download from GitHub Repository	Low	⌚ Closed	✗ False Positive	You (L1)	🔗 ⚡
Mar 21st 2025 at 12:40	Unusual VPN Login Location	Medium	⌚ Closed	✗ False Positive	T.Ross (L1)	🔗 ⚡
Mar 21st 2025 at 11:53	Bruteforce Attack from External	Medium	⌚ Closed	✓ True Positive	J.Adams (L2)	🔗 ⚡

## Alert Simulations – Triage, False Positive/True Positive Identification, and Resolving and Closing Tickets

Time	Name ↑↓	Severity	Status	Verdict	Assignee	Actions
1 Mar 21st 2025 at 11:53	2 Bruteforce Attack from External	3 Medium	4 ⌚ Closed	5 ✓ True Positive	6 J.Adams (L2)	🔗 ⚡
Mar 21st 2025 at 13:58	Double-Extension File Creation	High	⌚ Awaiting action	None	None	🔗 ⚡
Description:		7 This rule detects a creation of a double-extension file like '*.pdf.exe' or '*.gif.lnk', often used by hackers in phishing attacks to trick users into opening the malicious executable.				
Host:		8 LPT-HR-009				
Process Name:		chrome.exe				
Process User:		S.Conway				
Target File:		C:\Users\S.Conway\Downloads\cats2025.mp4.exe				
File MotW:		https://freecatvideoshd.monster/cats2025.mp4.exe				
File MD5:		14d8486f3f63875ef93cf240c5dc10b				

## Alert Structure