

# How to do Incident Response – Fast!

Jasper Bongertz

Head of CSIRT

G Data Advanced Analytics

Leonard Rapp

Security Engineer


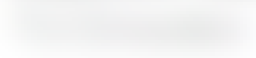


























































G Data Advanced Analytics



Tagelang  
Fesplatten  
kopieren

Schnell  
Ergebnisse  
erzielen

## Case Bootstrapper

<div>ADAN- </div> <div><div> Remove</div></div>	<div>ADAN- </div> <div><div> Remove</div></div>	<div>ADAN-123456 Irap FOR500 playground</div> <div><div> Remove</div></div>
<div>ADAN-99999 Irap FOR500 final challenge</div> <div><div> Remove</div></div>	<div>ADAN- </div> <div><div> Remove</div></div>	<div>ADAN-31337 Security Dumpsterfire GmbH</div> <div><div> Remove</div></div>



# Velociraptor

## Triage

```
autoexec:
  argv: ["artifacts", "collect", "-v", "AcquireAndUploadToNextCloud"]
  artifact_definitions:
    - name: AcquireAndUploadToNextCloud
      parameters:
        - name: webdav_url
          default: "https://[REDACTED]webdav/"
        - name: share_key
          default: CHANGE_ME

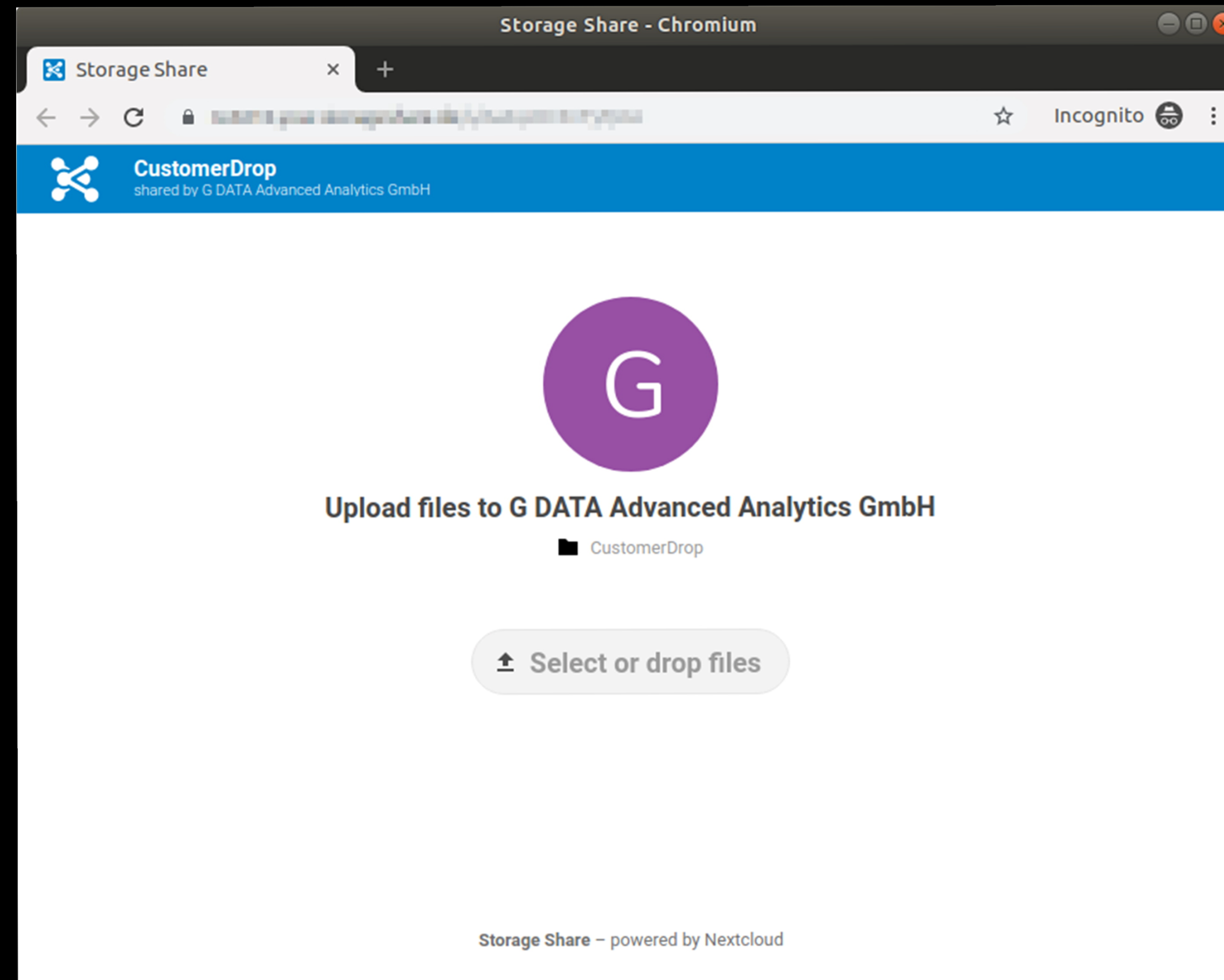
  sources:
    - queries:
      - LET hostname <= SELECT Hostname FROM info()
      - LET filename <= format(format="Collection_%s_%d.zip", args=[get(item=hostname, member="0.Hostname"), now()])
      - SELECT upload_webdav(
          file=Container,
          url=webdav_url,
          basic_auth_user=share_key,
          name=filename
        ) AS Uploaded
      FROM collect(
        artifacts=["Windows.KapeFiles.Targets"],
        args=dict(`Windows.KapeFiles.Targets`=dict(
          Amcache="Y",
          Antivirus="Y",
          EventLogs="Y",
          FileSystem="Y",
          LnkFilesAndJumpLists="Y",
          PowerShellConsole="Y",
          Prefetch="Y",
          RemoteAdmin="Y",
          RecentFileCache="Y",
          RegistryHives="Y",
          ScheduledTasks="Y",
          VSSAnalysis="Y",
          SRUM="Y",
          WindowsTimeline="Y"
        )),
        output=filename,
        level=5)
```



Velociraptor

Triage

Nextcloud  
& TFT





Case Panel schnuppertag

Artifacts

machine:schnuppertag\_Collection\_DESKTOP-AD4P8K4\_1651432171 x string::iso x data\_type:UsnJernl x Data.reason:FILE\_CREATE x

Raw Query: ▾

Build query

all

Total 3

yyyy-mm-dd HH:ii:ss,yyyy-mm-dd HH:ii:ss

Op.	Time Stamp	Data Type	Machine	Details
	2022-05-01 18:22:05	UsnJernl	Collection_DESKTOP-AD4P8K4_1651432171	File report[1].iso  Action FILE_CREATE
	2022-05-01 18:22:06	UsnJernl	Collection_DESKTOP-AD4P8K4_1651432171	File report.iso.e955fok.partial  Action FILE_CREATE
	2022-05-01 18:22:07	UsnJernl	Collection_DESKTOP-AD4P8K4_1651432171	File report.iso.npc6e80.partial  Action FILE_CREATE

Number of pages 1

1

Tag events & filter by tag



### Sync assets to IRIS

Kuiper case name:

Confirm assets before sync: ☒

[Sync now](#)

### Document Login/Logoff events

Kuiper case name:

Jira ticket ID:

Username:

Kuiper machine:

IRIS asset name:

Source IP:

Time range:   
e.g. Data.@timestamp:[2023-02-02T09:51:50 TO 2023-02-02T09:53:50]

[Sync now](#)





The screenshot displays the DFIR IRIS web interface. The top navigation bar includes tabs for Summary, Notes, Assets, IOC, Timeline (selected), Graph, Tasks, and Evidences. The left sidebar contains a menu with options like Dashboard, Overview, Case (highlighted), Alerts, Search, Activities, DIM Tasks, Manage cases, Advanced, and Help. The main content area shows a timeline for case #4 - ADAN-4444\_Timeline Service Test (FIN). The timeline is filtered by user 'Rapp, Leonard' and shows events from 2023-04-19 to 2023-04-20. The events include:

- Nachladen von Schadsoftware über PowerShell** (2023-04-19T10:13:37.000000): Ausführung von obfuskiertem PowerShell im Kontext des Nutzers **Peter Opfer**, welches Schadsoftware unter dem Pfad **C:\User\foobar\tmp\malware.exe** ablegt. (Category: Persistence)
- Ausführung von CobaltStrike** (2023-04-19T10:13:42.000000): Ausführung von CobaltStrike unter dem Pfad **C:\User\foobar\tmp\malware.exe**. (Category: Execution)
- Lateral movement** (2023-04-19T11:35:00.000000): RDP-Logon ausgehend von **admin-ws-123** auf **dc01** mit dem kompromittierten Konto **dom-admin**. (Category: Lateral Movement)
- Ausführen von PsExec** (2023-04-20T00:00:00.000000): Erstmalige Ausführung von "Ransomware.exe" & PsExec aus dem Pfad **c:\s\$\psexec.exe** von der Quell-IP-Adresse **8.8.8.8** aus. (Category: Execution)

The interface also features a search bar, a filter dropdown, and a 'Filter timeline' input field. The bottom right corner shows the version 'IRIS v2.3.2'.





Active Cases:

#2 - ADAN-9898_Timeline IRIS Test Case	#24 - ADAN-4199	#32 - ADAN-4398	#35 - ADAN-4539	#34 - ADAN-4540
<div>Timeline</div> <div>IOCs</div> <div>Systems</div>	<div>Timeline</div> <div>IOCs</div> <div>Systems</div>	<div>Timeline</div> <div>IOCs</div> <div>Systems</div>	<div>Timeline</div> <div>IOCs</div> <div>Systems</div>	<div>Timeline</div> <div>IOCs</div> <div>Systems</div>



VERTRAULICH   TLP:AMBER	
23.07.2023 22:53:41	<b>Öffnen von PowerShell</b> Öffnen von powershell.exe mit dem Konto [REDACTED]
23.07.2023 22:54:54	<b>Ausführung eines PowerShell-Skripts</b> Das PowerShell-Skript unter dem Pfad C:\v.ps1 wird durch das Konto [REDACTED] ausgeführt; insgesamt fanden zwei Ausführungen statt zwischen denen der PowerShell-Befehl Set-ExecutionPolicy Bypass ausgeführt wurde; zum Zeitpunkt der Analyse war das Skript nicht mehr auf dem System vorhanden
23.07.2023 22:56:05	<b>Ausführung Mimikatz</b> Das Programm C:\Users\[REDACTED]\Desktop\mim.exe wird durch das Konto [REDACTED] ausgeführt; die Datei ist zum Zeitpunkt der Analyse nicht mehr vorhanden; auf einem anderen System wird eine Datei mit gleichem Namen detektiert, bei der es sich um das Angreiferwerkzeug Mimikatz zum Auslesen von Passwörtern handelt
23.07.2023 22:57:54	<b>Öffnen einer Textdatei</b> Öffnen der Datei C:\Users\[REDACTED]\Desktop\253523.txt mit dem Konto [REDACTED] mit Hilfe des Programms Notepad (64-bit); die Datei ist zum Zeitpunkt der Analyse nicht mehr vorhanden
23.07.2023 23:11:48	<b>Ausführung Mimikatz</b> Das Programm C:\Users\[REDACTED]\Desktop\mim.exe wird durch das Konto [REDACTED] ausgeführt; um 01:07:22 Uhr erkennt die Antivirensoftware Bitdefender dieses Programm als das Angreiferwerkzeug Mimikatz, das

# Fragen?