Speed is key: Leveraging the Cloud for Forensic Artifact Collection & Processing

Lukas Klein (SAP, Germany)
Jason Ballard (SAP, Germany)
Christian Koepp (SAP, Germany)
About us

• SAP Global Security runs four Incident Response Hubs (US East, US West, Europe, Asia)
• Operates 24/7 IR services for internal stakeholders

Lukas Klein  @RantaSec
Jason Ballard  
Chris Koepp
Motivation

• Attackers move quickly (full domain compromise in hours)
• Insights like actionable IoCs as quickly as possible
• Triage artifacts sufficient to answer most questions
• Full forensic image slow and not needed for all cases
• Enterprise forensic tools struggle with complex environments
• Manual processes and (human) decencies delay response
Our Problem

Mail/Phone → Affected User → Processing Environment → DFIR Station
Our Solution

Mail/Phone ➔ Affected User ➔ Processing Environment ➔ Compromised Host ➔ EDR Console ➔ DFIR Station
Artifact Collection
Artifact Collection

EDR Console

Compromised Host

EDR Agent

Invoke-LRCollection.ps1
- Downloads second stage
- Validates integrity

Invoke-TriageCollection.ps1
- Collect memory
- Collect triage artifacts
- Encrypt & upload triage
- Encrypt & upload memory

Processing Environment
Artifact Collection: Dependencies

Surge-Collct: Memory Collection

KAPE: Triage Artifact Collection

7zip: Compression & Encryption

AWS PowerShell Tools: Upload
Artifact Collection: KAPE .tkape Config

Description: PowerShell Console Log File
Author: Mike Cary
Version: 1.0
Id: efa4332a-89eb-430c-ab61-006a9e6620d7
RecreateDirectories: true
Targets:

Name: PowerShell Console Log
Category: PowerShellConsoleLog
Path: C:\Users\%user%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ ConsoleHost_history.txt

# Documentation
# https://community.sophos.com/malware/b/blog/posts/powershell-command-history-forensics
# https://digital-forensics.sans.org/media/DFPS_FOR508_v4.4_1-19.pdf
Artifact Collection: Envelope Encryption
Artifact Collection: Envelope Encryption

Compromised Host

Random Symmetric Key
Artifact Collection: Envelope Encryption

- Compromised Host
  - Random Symmetric Key
- Cloud Processing Environment
  - Private Decryption Key
Artifact Processing

EDR Console → Compromised Host → Processing Environment → DFIR Station
Artifact Processing

Enc(Artifacts, Key) → Staging
Artifact Processing

Enc(Artifacts, Key) → Staging → Replicate-onUpload → Raw Long Term Storage
Artifact Processing

Scheduled Task:
- Invoke-ArtifactProcessing.ps1
  - Download & decrypt
  - Process raw artifacts
  - Encrypt & upload

Replicate on Upload

Raw Long Term Storage

Processor

Staging

Enc(Artifacts, Key)

Processed
Artifact Processing: Scaling

1. **Enc(artifacts, key)**
   - Staging

2. **Replicate-onUpload**

3. **Raw Long Term Storage**
   - DFIR Station

4. **Processed**
EDR API Trigger

- EDR Console
- Compromised Host
- Processing Environment
- DFIR Station
EDR API Trigger: Hands-On

```json
{
    "Commands": [
        {
            "type": "RunScript",
            "params": [
                {
                    "key": "ScriptName",
                    "value": "Invoke-LRCollection.ps1"
                },
                {
                    "key": "Args",
                    "value": "-casenum INCIDENT001337 -skipmem"
                }
            ]
        }
    ],
    "Comment": "Triggered by joe.doe@sap.com"
}
```

EDR Console API

https://api.securitycenter.microsoft.com/api/machines/<machine_uuid>/runliveresponse

- **SOAR-ready**
- **Audit-ready**
- **Response Timeout is 10 minutes**
  - Use sub-process to carry on executing long running tasks
EDR API Trigger: Hands-On

```json
{
  "Commands": [
    {
      "type": "GetFile",
      "params": [
        {
          "key": "Path",
          "value": "C:\Windows\System32\msrpc22.dll"
        }
      ]
    },
    "Comment": "Triggered by SOAR bot"
  }
}
```

Do it before RunScript
- Dedicated API call
- index=0 in Commands array

Results available at

https://api.securitycenter.microsoft.com/api/machineactions/<machineaction_uuid>/GetLiveResponseResultDownloadLink(index=0)
Demo
Summary

• Reference architecture
• Triggered via API
  • Manual execution as a backup
• DFIR artifacts in minutes
• Repeatable collection
• Free tools fitting each budget
• Automated cloud processing can be added at scale
Future Work

• Open sourcing in progress
• infrastructure as code
• Additional processing capabilities
• Automatic ingestion into time sketch
• LiveResponse Library API:
  Automated creation and upload of highly customized scripts per host