ZOLDER

applied security research

INTUNE | DUTCH MICROSOFT & SECURITY MEETUP

6-9-2022

WHOAMI

- Rik van Duijn
  - Ethical hacker
  - OSCP / OSCE
  - 8+ years of experience
  - Cybercrime / Malware analysis
  - Mede oprichter Zolder

WHAT ARE WE TALKING ABOUT

- Intro
- Code-exec voorbeelden
  - Script
  - Configuration profile
  - Win32app/lineofbusiness
  - Win32App (Intunewin) check script
- Logging
- Verrijken
- Demo: oauth phish

WORK IN PROGRESS

rootsecdev
@rootsecdev

👀

LockBit ransomware automates Windows domain encryption via group policies

bleepingcomputer.com
LockBit ransomware now encrypts Windows domains using group policies
An new version of the LockBit 2.0 ransomware has been found that automates the encryption of a Windows domain using Active Directory gr

3:03 AM · Jul 28, 2021 · Twitter for iPhone

Voornamelijk PsExec, GPO, SCCM, Software Deployment systems zoals Kaspersky ;-) - Als het om ransomware deployments gaat.

Apr 16, 2022, 7:39 PM

- In another investigation, APT32 compromised the McAfee ePO infrastructure to distribute their malware as a software deployment task in which all systems pulled the payload from the ePO server using the proprietary SPIPE protocol.

IT'S A FEATURE, NOT A BUG

WHO CAN MANAGE INTUNE?

- AzureAD:
- Global Administrator (Read/Write)
- Intune Service Administrator (Read/Write)

- Builtin:
- **Application Manager**: Manages mobile and managed applications, can read device information and can view device configuration profiles.
- **Endpoint Security Manager**: Manages security and compliance features, such as security baselines, device compliance, conditional access, and Microsoft Defender for Endpoint.
- **Read Only Operator**: Views user, device, enrollment, configuration, and application information. Can't make changes to Intune.
- **School Administrator**: Manages Windows 10 devices in Intune for Education.
- **Policy and Profile Manager**: Manages compliance policy, configuration profiles, Apple enrollment, corporate device identifiers, and security baselines.
- **Help Desk Operator**: Performs remote tasks on users and devices, and can assign applications or policies to

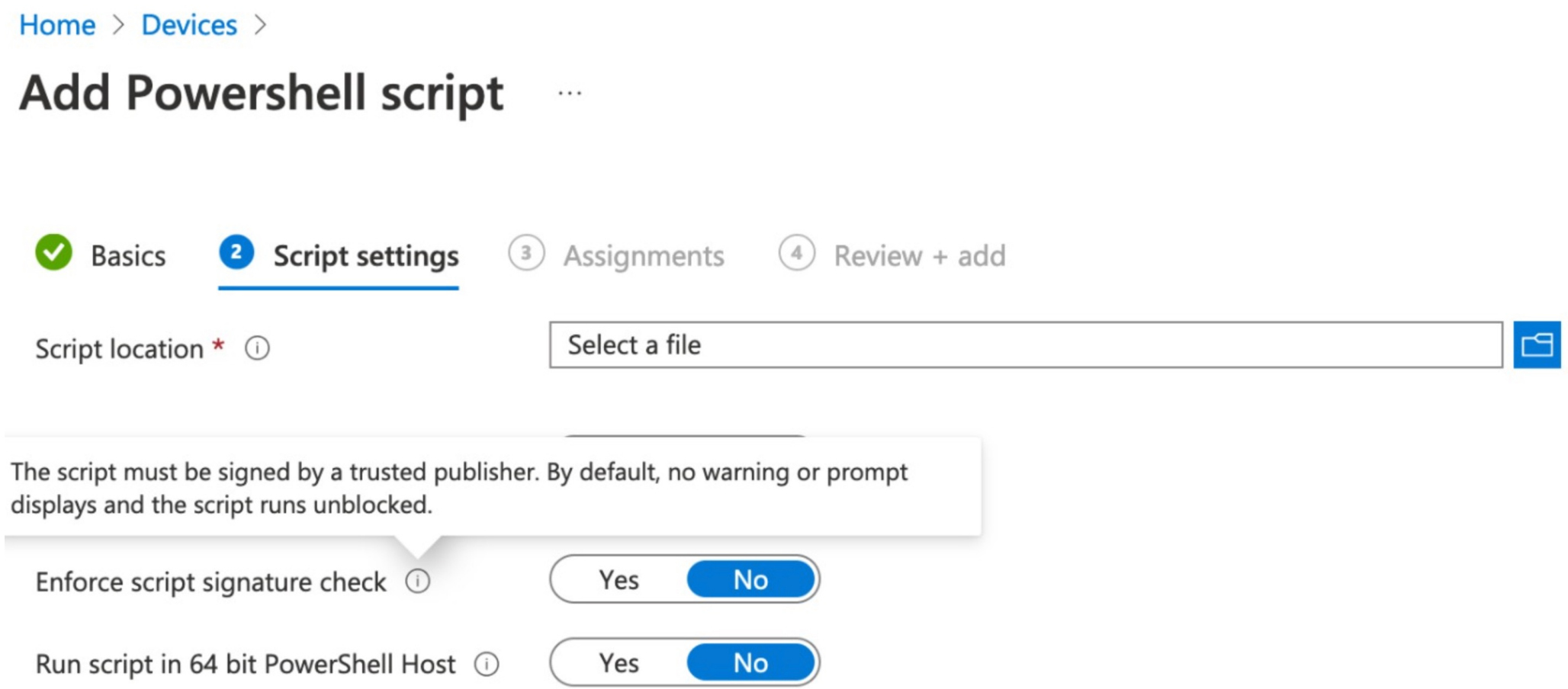
FEATURES DIE CODE-EXEC TOELATEN

- Script execution (duh)
- Check-scripts
- Configuration policies
- App packages
- Proactive remediations
- ??

Helemaal zelf bedacht ;)

- Waarschijnlijk meer, heb je tips? Ik hoor ze graag!

VIA SCRIPT


Home > Devices >
Add Powershell script
...
Basics
2 Script settings
3 Assignments
4 Review + add
Script location *
Select a file
The script must be signed by a trusted publisher. By default, no warning or prompt displays and the script runs unblocked.
Enforce script signature check
Yes
No
Run script in 64 bit PowerShell Host
Yes
No

VIA SCRIPT

DEATH FROM ABOVE:

LATERAL MOVEMENT FROM AZURE TO ON-PREM AD.

INTUNE | DUTCH M

PROCESSTREE

- Services.exe
  - Microsoft.Management.Services.Intune.WindowsAgent.exe
    - AgentExecutor.exe
      - Powershell.exe

[4500] **AgentExecutor.exe**

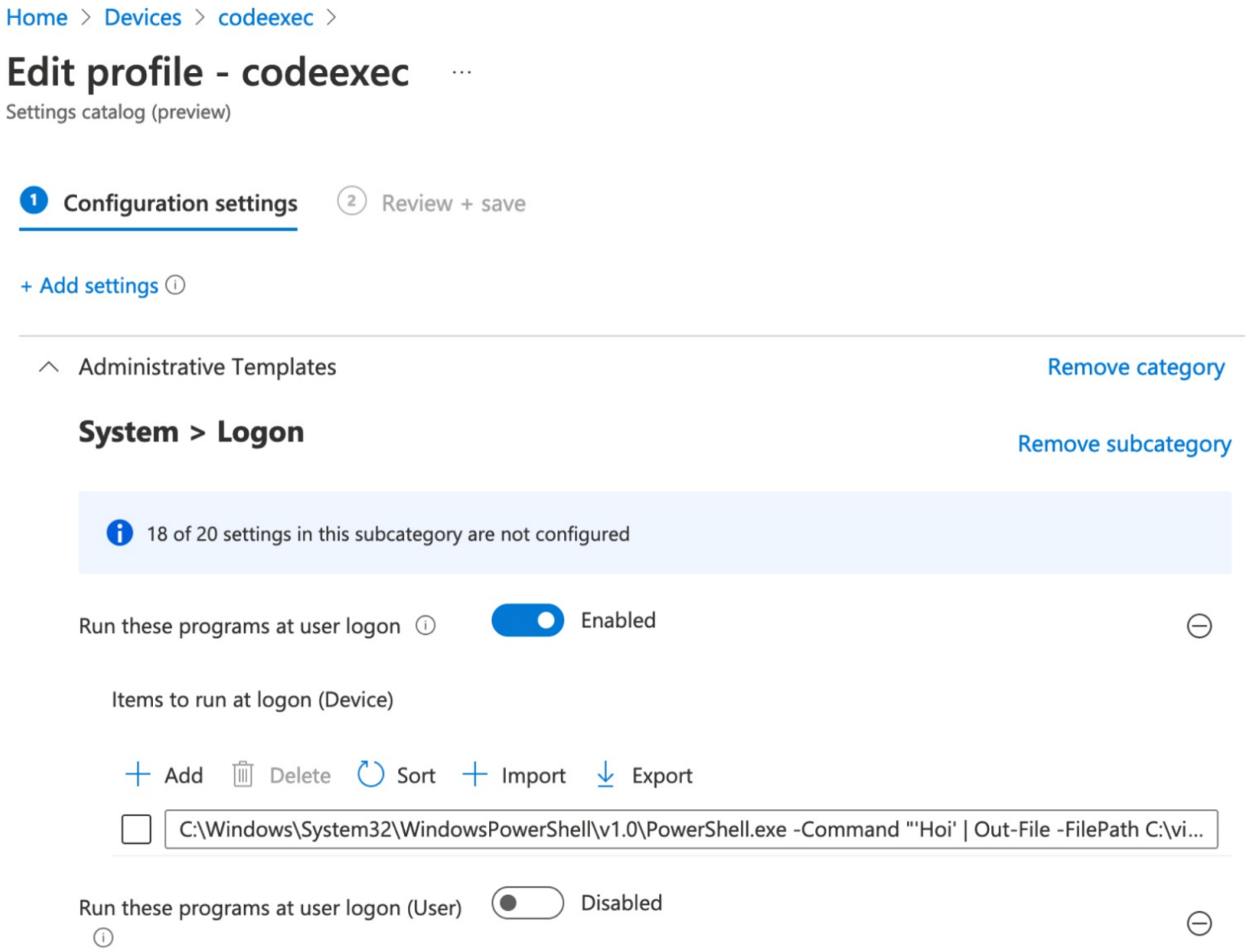
[10988] **powershell.exe** -NoProfile -executionPolic...

Process ID	10988
Execution time	Sep 3, 2022 3:12:48 PM
Command line	`"powershell.exe" -NoProfile -executionPolicy bypass -file "C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\93ba15ef-7597-4798-9e45-16f06b23ef55_f7d36dbe-a4ce-4f74-a609-725c02c97fc5.ps1"`
Image file path	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Image file SHA1	78d990d776f078517696a2415375ac9ebdf5d49a
Image file SHA256	88e1993beb7b2d9c3a9c3a026dc8d0170159afd3e574825c23a34b917ca61122
Execution details	Token elevation: Standard, Integrity level: System
Signer	Microsoft Windows
Issuer	Microsoft Windows Production PCA 2011
VirusTotal detection ratio	0/0

[3528] **powershell.exe** -Command "'Hoi' | Ou...

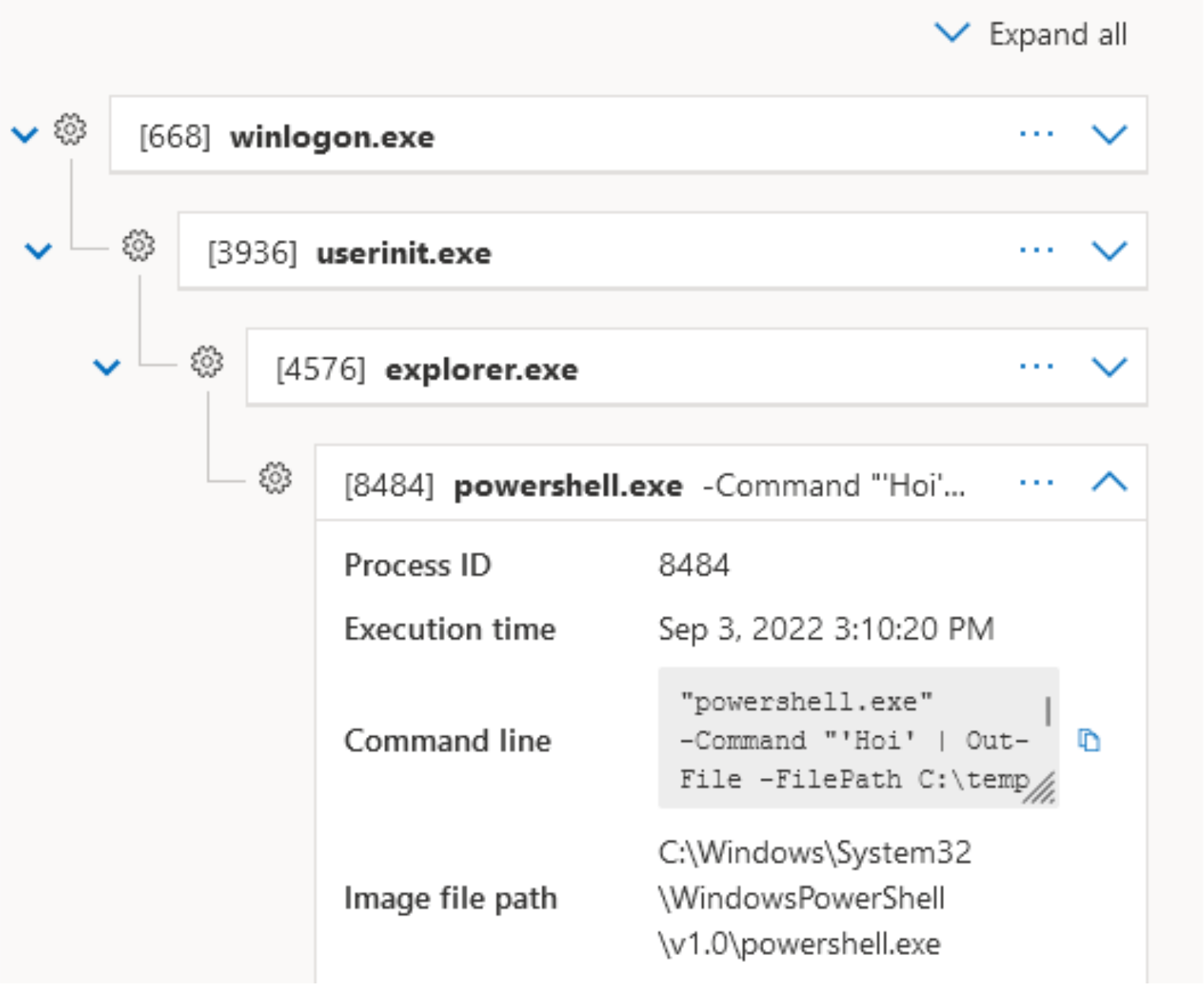
Process ID	3528
Execution time	Sep 3, 2022 3:12:49 PM
Command line	`"PowerShell.exe" -Command "'Hoi' | Out-File -FilePath C:\temp\via_intune_script.txt"`

VIA CONFIGURATION PROFILE

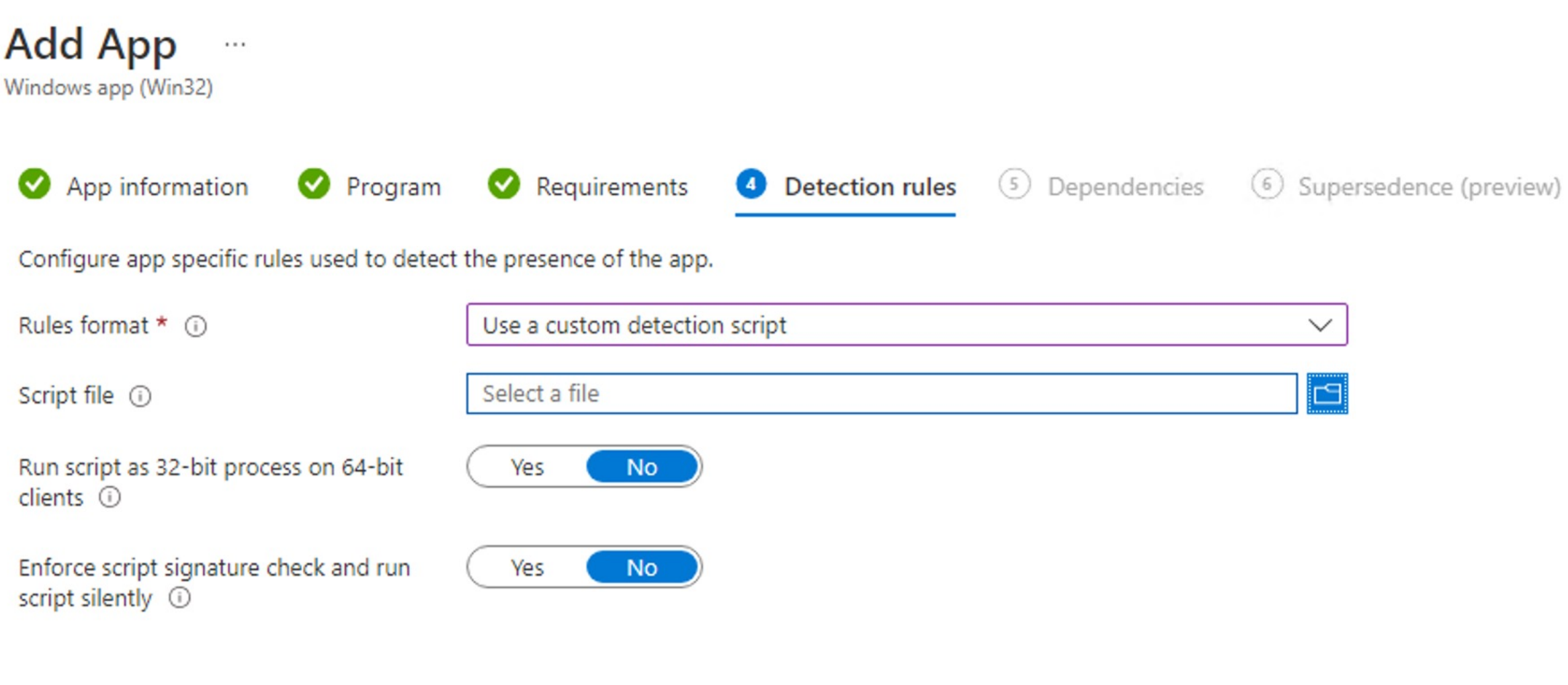


PROCESSTREE

- Winlogon.exe
  - Userinnit.exe
    - Explorer.exe
      - Powershell.exe



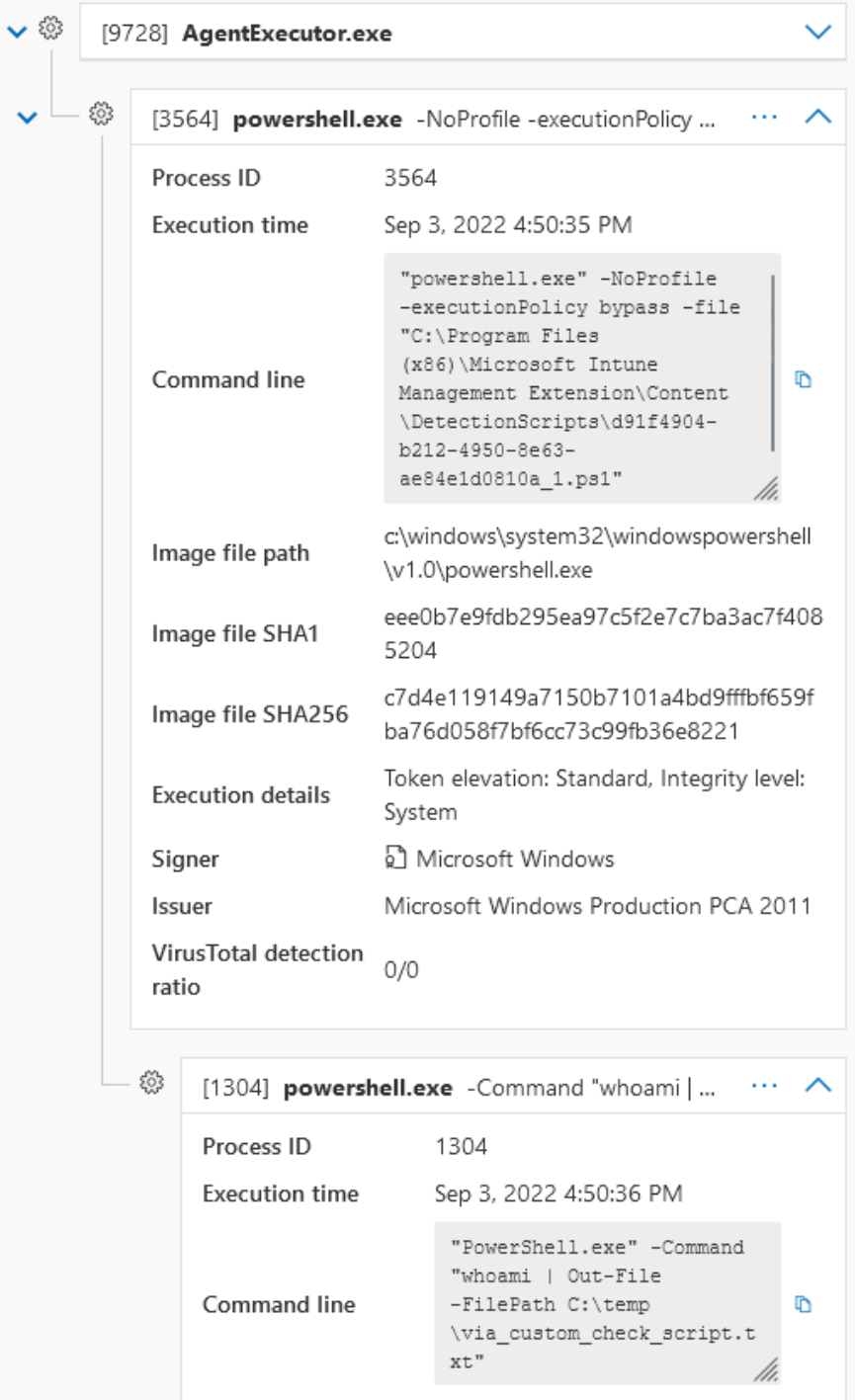
DETECTIE SCRIPT ALS BACKDOOR



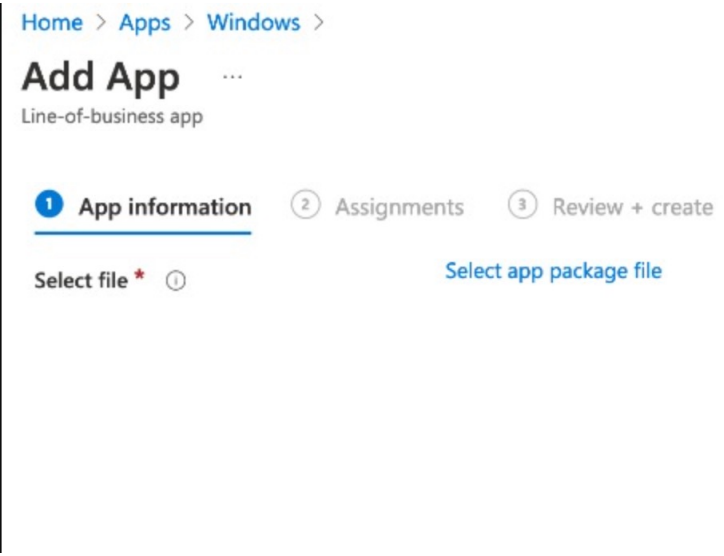
INTUNE | DUTCH M

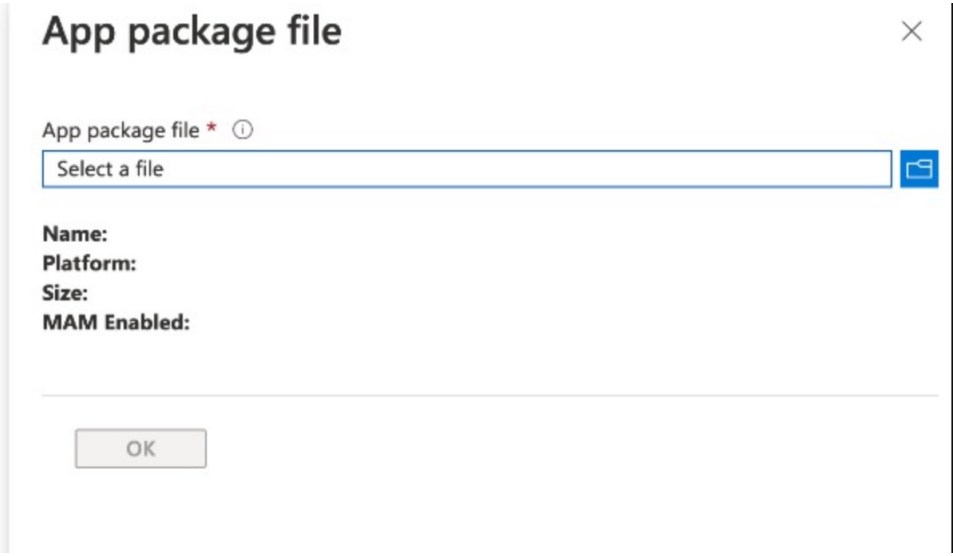
PROCESSTREE

- Services.exe
  - Microsoft.Management.Services.Intune.WindowsAgent.exe
    - AgentExecutor.exe (LOLBIN)
      - Powershell.exe
        - ???
        - Profit!



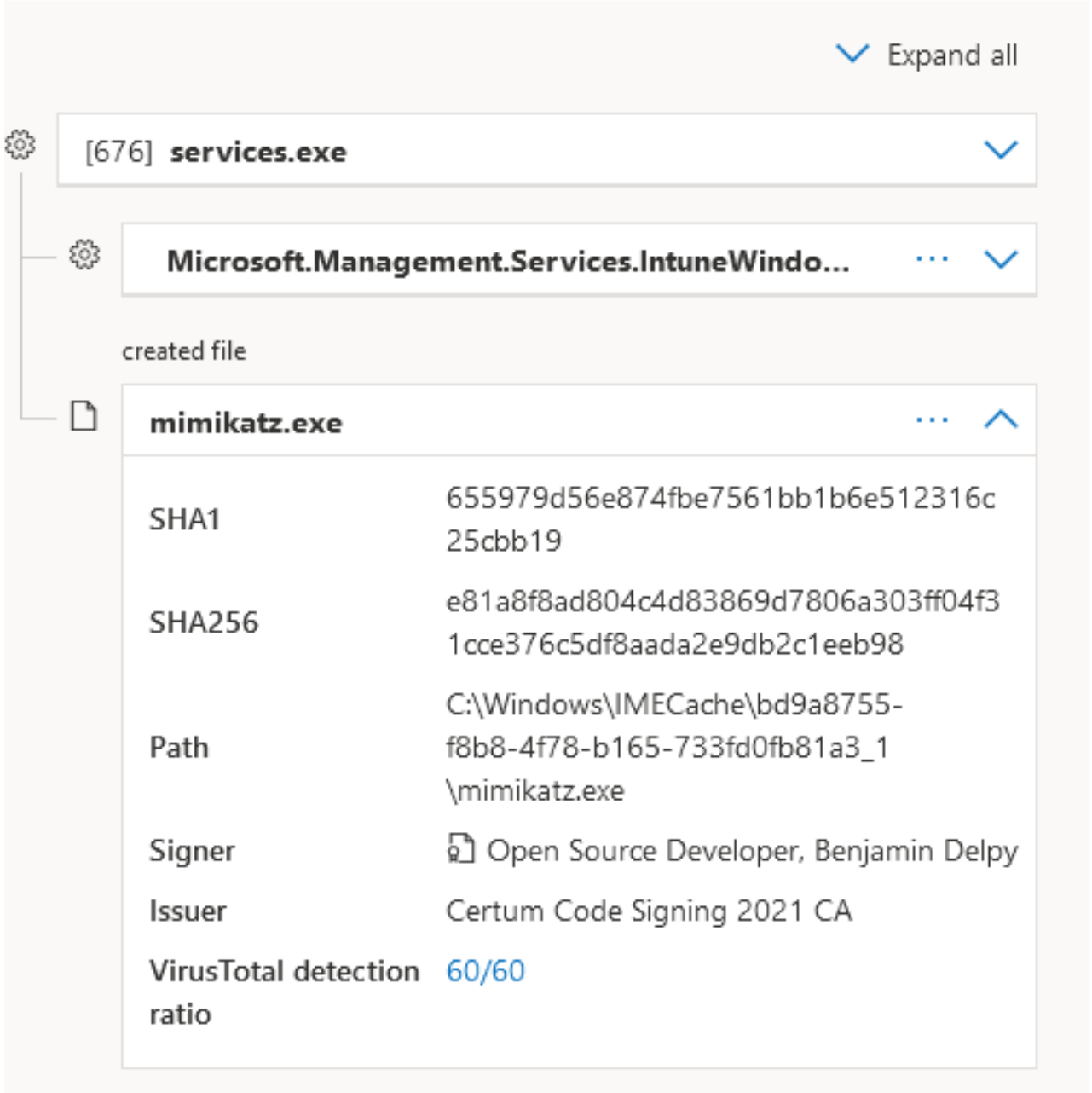
VIA APP DEPLOYMENT





VIA APP DEPLOYMENT

- Services.exe
  - Microsoft.Management.Services.IntuneWindowsAgent.exe
    - Malware.exe



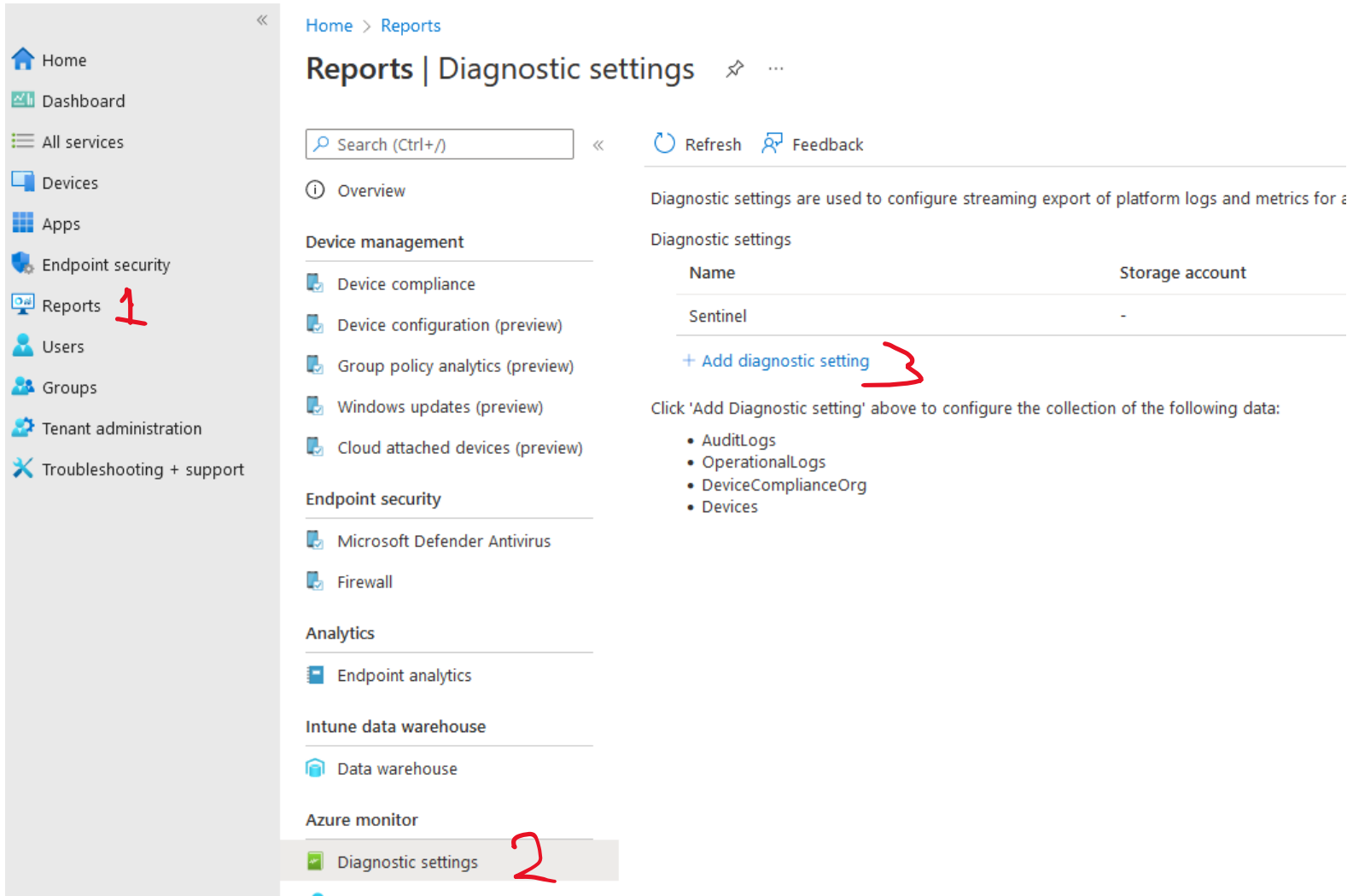
DEFENDER CHECKT NOG

mimikatz.exe

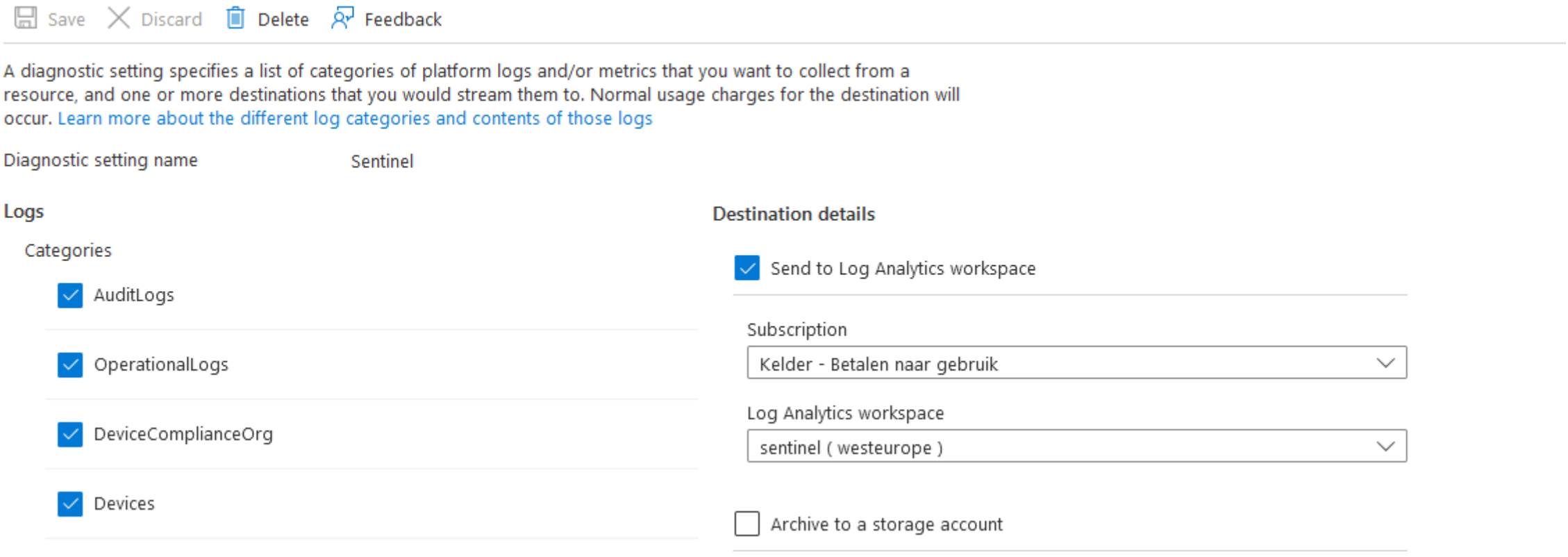
SHA1	655979d56e874fbe7561bb1b6e512316c25cbb19
Path	C:\Windows\IMECache\bd9a8755-f8b8-4f78-b165-733fd0fb81a3_1\mimikatz.exe
Size	1 MB
Is PE	True
Mitre techniques	T1003: OS Credential Dumping, T1550.003: Pass the Ticket
Signer	Open Source Developer, Benjamin Delpy
Issuer	Certum Code Signing 2021 CA
VirusTotal detection ratio	60/60
Blocking details	**Defender detected and quarantined active 'HackTool:Win32/LSADump' in file 'mimikatz.exe', during attempted creation by 'Microsoft.Managemen...**

LOGGING

CONNECTING INTUNE TO SENTINEL



CONNECTING INTUNE TO SENTINEL



SENTINEL LOGS BEPERKT

Run | Time range : **Last 24 hours** | Save | Share | New alert rule | Export | Pin to | Format

```
1  IntuneAuditLogs
2
3  IntuneOperationalLogs
4
5  IntuneDeviceComplianceOrg
6
7  IntuneDevices
8
```

Results Chart | Add bookmark

TimeGenerated [UTC]	OperationName	Category	ResultType	ResultDescription	C
16-4-2022 17:12:28.795	createDeviceManagementScript DeviceManagementScr...	AuditLogs	Success	None	c
16-4-2022 17:12:29.398	assignDeviceManagementScript DeviceManagementScr...	AuditLogs	Success	None	3
16-4-2022 13:36:23.760	Create DeviceManagementConfigurationPolicy	AuditLogs	Success	None	e
16-4-2022 13:36:24.148	Create DeviceManagementConfigurationPolicyAssignm...	AuditLogs	Success	None	7

AUDIT LOGS

Audit logs ...

« Columns Filter Refresh Export

Search by initiated by (actor)

Date	Initiated by (actor)	Application name	Activity	Target
9/04/2022, 4:21:18 PM	acid.burn@kelder.io	Microsoft Intune portal extension	Patch MobileApp	mimikatz.exe
9/04/2022, 4:00:45 PM	acid.burn@kelder.io	Microsoft Intune portal extension	assignDeviceManagementScript DeviceManagementSc...	
9/04/2022, 4:00:44 PM	acid.burn@kelder.io	Microsoft Intune portal extension	createDeviceManagementScript DeviceManagementSc...	
9/04/2022, 2:34:42 PM	acid.burn@kelder.io	Microsoft Intune portal extension	Create MobileAppAssignment	mimikatz.exe

Old Value:
Property: $Collection.DetectionRules.EnforceSignatureCheck[0]
New Value: False
Old Value: False
Property: $Collection.DetectionRules.RunAs32Bit[0]
New Value: False
Old Value: False
Property: $Collection.DetectionRules.ScriptContent[0]
New
Value: QzpcV2luZG93c1xTeXN0ZW0zMlxXaW5kb3dzUG93ZXJTaGVsbF
Old
Value: QzpcV2luZG93c1xTeXN0ZW0zMlxXaW5kb3dzUG93ZXJTaGVsbF

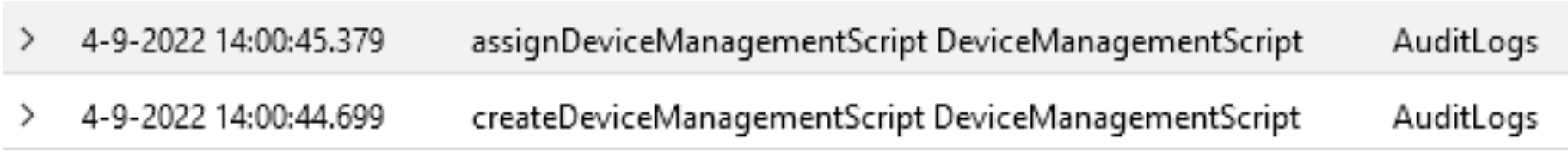
ENRICHMENT

4-9-2022 14:00:44.699	createDeviceManagementScript DeviceManagementScript	AuditLogs	Success	None	840d3dcc-b77d-410d-9965-d16e048e1...	acid.burn@kelder.io

TenantId	d75bef37-98a2-4b28-8bf2-2fced09c4401
SourceSystem	Microsoft Intune
TimeGenerated [UTC]	2022-09-04T14:00:44.699Z
OperationName	createDeviceManagementScript DeviceManagementScript
Category	AuditLogs
ResultType	Success
ResultDescription	None
CorrelationId	840d3dcc-b77d-410d-9965-d16e048e1480
Identity	acid.burn@kelder.io
Properties	{"ActivityDate":"9/4/2022 2:00:44 PM","ActivityResultStatus":1,"ActivityType":0,"Actor":{"ActorType":1,"Application":"5926fc8e-304e-4f59-8bed-58ca97cc39a4","ApplicationName":"Microsoft
ActivityDate	9/4/2022 2:00:44 PM
ActivityResultStatus	1
ActivityType	0
Actor	{"ActorType":1,"Application":"5926fc8e-304e-4f59-8bed-58ca97cc39a4","ApplicationName":"Microsoft Intune portal extension","IsDelegatedAdmin":false,"Name":null,"ObjectId":"93ba15ef
AdditionalDetails	
AuditEventId	1df5665d-d5a5-4494-b4bd-938e1d9196c7
Category	3
RelationId	null
TargetDisplayNam...	["<null>"]
TargetObjectIds	["3c7f2851-d07e-4d03-b7fc-28687662e9e8"]
Targets	[{"ModifiedProperties":[{"Name":"DeviceManagementAPIVersion","Old":null,"New":"5022-07-27"}],"Name":null}]
0	{"ModifiedProperties":[{"Name":"DeviceManagementAPIVersion","Old":null,"New":"5022-07-27"}],"Name":null}
ModifiedProperti...	[{"Name":"DeviceManagementAPIVersion","Old":null,"New":"5022-07-27"}]
0	{"Name":"DeviceManagementAPIVersion","Old":null,"New":"5022-07-27"}
Name	null
Type	IntuneAuditLogs

LOGGING

- Scriptexec
  - createDeviceManagementScript DevicemanagementScript
  - patchDeviceManagementScript DeviceManagementScript
- Policy
  - Create DeviceManagementConfigurationPolicy
  - Patch DeviceManagementConfigurationPolicy
- App check Script
  - Patch MobileApp
  - Create MobileApp
- App
  - Create MobileApp
  - Patch MobileApp

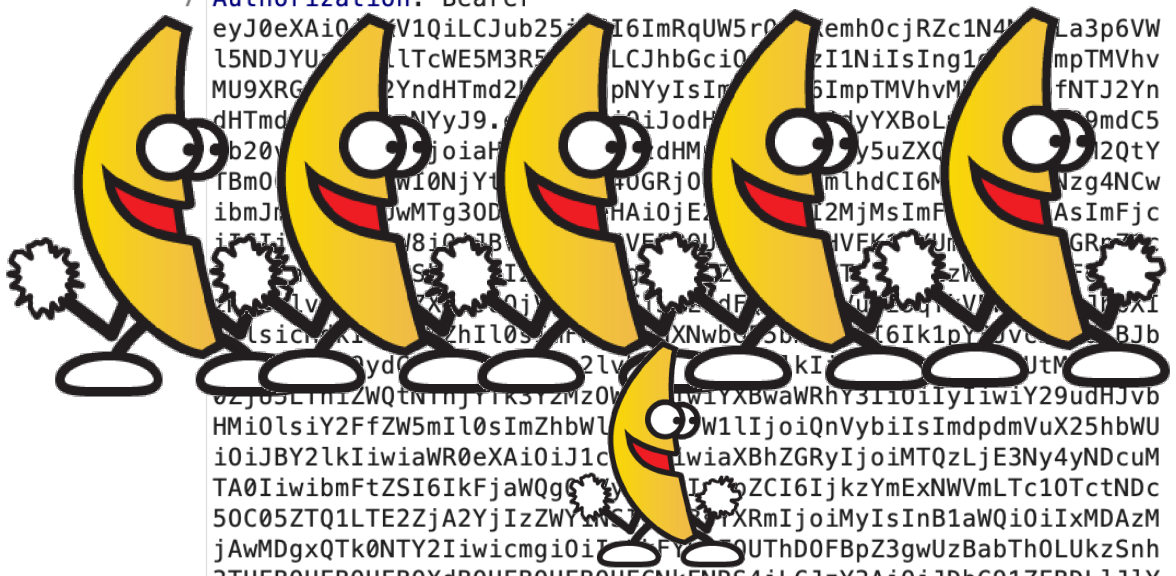


VERRIJKING

SCRIPT BASE64

- /beta/deviceManagement/deviceManagementScripts/245638dc-714e-4df2-bb98-210aa71bf7a1?$expand=assignments

```
GET
/beta/deviceManagement/deviceManagementScripts/245638dc-714e-4df2-bb98-210aa71bf7a1?$expand=assignments HTTP/1.1
Host: graph.microsoft.com
X-Ms-Client-Session-Id: ced6977f43324de5bb0dd7b8ccece1f5
X-Content-Type-Options: nosniff
X-Ms-Command-Name:
DeviceScriptManagementGraphProxy_fetchDeviceManagementScript
Accept-Language: en
Authorization: Bearer
```



```
Europe","Slice":"E","Ring":"5","ScaleUnit":"005","RoleInstance
":"AM4PEPF00015166"}}
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: ETag, Location,
Preference-Applied, Content-Range, request-id,
client-request-id, ReadWriteConsistencyToken, SdkVersion,
WWW-Authenticate, x-ms-client-gcc-tenant
OData-Version: 4.0
Date: Sun, 17 Apr 2022 09:36:40 GMT
Connection: close
Content-Length: 1060

{
  "@odata.context":
  "https://graph.microsoft.com/beta/$metadata#deviceManagement
  /deviceManagementScripts(assignments())/$entity",
  "enforceSignatureCheck":false,
  "runAs32Bit":true,
  "id":"245638dc-714e-4df2-bb98-210aa71bf7a1",
  "displayName":"script",
  "description":"",
  "scriptContent":
  "QzpcV2luZG93c1xTeXN0ZW0zMlxXaW5kb3dzUG93ZXJTaGVsbFx2MS4wXFB
  vd2VyU2hlbGwuZXhlIC1Db21tYW5kICInSG9pJyB8IE91dC1GaWxlIC1GaWx
  lUGF0aCBDOlx0ZW1wXHZpYV9pbnR1bmVfc2NyaXB0LnR4dCI=",
  "createdDateTime":"2022-04-17T07:07:33.4738867Z",
  "lastModifiedDateTime":"2022-04-17T07:07:33.4738867Z",
  "runAsAccount":"system",
  "fileName":"nla.ps1",
```

GRAPHCALL CONFIG POLICY

- /beta/deviceManagement/configurationPolicies('1b63eceb-2f29-477e-ba26-894a0b7ddaa0')/settings?$expand=settingDefinitions&top=1000

```
GET
/beta/deviceManagement/configurationPolicies('ba116dad-87dd-4ae5-8f07-099fb5c0c394
')/settings?$expand=settingDefinitions&top=1000 HTTP/1.1
Host: graph.microsoft.com
X-Ms-Client-Session-Id: a9fa7d2f3fd14d00a30dd889a3c02475
X-Content-Type-Options: nosniff
X-Ms-Command-Name: PolicyGraphProxy_getSettingsForPolicy
Accept-Language: en
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJub25jZSI6IlIOUWdBcEsyUGt2TWdfSFYycGQ3NGltdEVzZ1BtbVpoWjFVTWJSM3
kzcGciLCJhbGciOiJSUzI1NiIsImlkCI6IjJaUXBKM1VwYmpBWVhZR2FYRUpsOGxWMFRPSSIsImtpZCI6
IjJa[redacted]KM1VwYmpBWVhZR2F[redacted]bsOGxWMFRPSSJ9.ey[redacted]QiOiJodHRwczovL2[redacted]XBoLm1pY3Jvc29md
C5[redacted]IiwiaXNzIjoiaH[redacted]6Ly9zdHMud2luZG9[redacted]nZXQvZjAwMjBmM2[redacted]mOCOONGM3LWIONjY
t[redacted]Y4OGRjOWM3LyI[redacted]CI6MTY2MjQ0ODE[redacted]mJmIjoxNjYyNDQ[redacted]LCJleHAiOjE2NjION
[redacted]FjY3QiOjAs[redacted]jEiLCJhaW8iO[redacted]S84VEFBQUFJ[redacted]YmhTbmVGZzdQbEN
[redacted]WhZYVFzWU[redacted]eHBrVORkQU[redacted]X1dZSFB6Y[redacted]rcjQyTDdHUWJXb
[redacted]ZENXJXNHZ2[redacted]bUOS2VYYzOi[redacted]IsicHdkIiw[redacted]ImFwcF9kaXNwbGF
[redacted]6Ik1pY3Jvc2[redacted]R1bmUgcG9ydG[redacted]Vuc2lvbiIsIi[redacted]joiNTkyNmZjOGUtM
[redacted]ZjU5LThiZWQt[redacted]3Y2MzOWEOIiwi[redacted]bY3IiOiIyIiwi[redacted]YbHMiOlsiY2FfZW5
[redacted]hb[redacted]Vyb[redacted]Im[redacted]iG[redacted]Ai[redacted]c2VyIiwia
[redacted]Ny[redacted]ZS[redacted]Si[redacted]ExNWVmLTc
[redacted]S2TQ[redacted]YlNS1[redacted]IsInNia[redacted]AwMDgxQTkON
[redacted]OiIwLkFYb[redacted]Z3gwUzBabT[redacted]TUFBQUFBQ[redacted]BQUFBQUFCNkF
[redacted]JDh[redacted]Wxs[redacted]Fdy[redacted]Y2VNYW5hZ
```

```
"device_vendor_msft_policy_config_admx_logon_run_2",
"settingInstanceTemplateReference":null,
"choiceSettingValue":{
  "settingValueTemplateReference":null,
  "value":"device_vendor_msft_policy_config_admx_logon_run_2_1",
  "children":[
    {
      "@odata.type":
      "#microsoft.graph.deviceManagementConfigurationSimpleSettingCollec
      tionInstance",
      "settingDefinitionId":
      "device_vendor_msft_policy_config_admx_logon_run_2_runlistbox2",
      "settingInstanceTemplateReference":null,
      "simpleSettingCollectionValue":[
        {
          "@odata.type":
          "#microsoft.graph.deviceManagementConfigurationStringSettingVa
          lue",
          "settingValueTemplateReference":null,
          "value":
          "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\PowerShell.ex
          e -Command \"'Hoi' | Out-File -FilePath C:\\temp\\via_run_at_l
          ogon.txt\""
        }
```

APP PACKAGE TOEGEVOEGD

- /beta/deviceAppManagement/mobileApps/59d4753a-8e77-4655-a1ed-2efafdb6e759/microsoft.graph.windowsMobileMSI/contentVersions/1/files/d1c2ebdc-64f0-4d1e-a99a-7ec7833067e8

```
GET
/beta/deviceAppManagement/mobileApps/59d4753a-8e77-4655-a1ed-2efafdb6e759/microsoft.graph.windowsMobileMSI/contentVersions/1/files/d1c2ebdc-64f0-4d1e-a99a-7ec7833067e8 HTTP/1.1
Host: graph.microsoft.com
X-Ms-Client-Session-Id: ced6977f43324de5bb0dd7b8ccece1f5
X-Content-Type-Options: nosniff
X-Ms-Command-Name: _retrySaveLobAppContentFileRequest
Accept-Language: en
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJub25jZSI6ImRqUW5rQjBXemhOcjRZc1N4MnZLa3p6VW
l5NDJYUzVoZllTcWE5M3R5ZW8iLCJhbGciOiJSUzI1NiIsIng1dCI6ImpTMVhv
MU9XRGpfNTJ2YndHTmd2UU8yVnpNYyIsImtpZCI6ImpTMVhvMU9XRGpfNTJ2Yn
dHTmd2UU8yVnpNYyJ9.eyJhdWQiOiJodHRwczovL2dyYXBoLm1pY3Jvc29mdC5
jb2[illegible]iaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQv[illegible]jBmM2QtY
TR[illegible]GM3LWI0NjYtNmYwZGY4OGRjOWM3LyIsImlhdCI6[illegible]E4Nzg4NCw
i[illegible]iUwMTc[illegible]Dg0LCJleHAiOjE2NTAxOTI[illegible]iMsI[illegible]iAsImFjc
[illegible]aW8[illegible]BVlFBcS84VEFBQUFtMlh[illegible]FK1N[illegible]GRnZ1c
[illegible]aXBi[illegible]mI2RXJIMUg1ellXZTJ[illegible]ytO[illegible]FelVpZ
[illegible]VG[illegible]OQjVGRVNk[illegible]PL1dF[illegible]uU2[illegible]iLCJhbXI
[illegible]I[illegible]ImFw[illegible]XNwb[illegible]c29mdCBJb
[illegible]n[illegible]Vug[illegible]sImF[illegible]MzA0[illegible]C0
[illegible]0Zj[illegible]K3Y2[illegible]iwiY[illegible]9i[illegible]9
[illegible]Mj[illegible]sImZ[illegible]1[illegible]sI[illegible]U
[illegible]iOi[illegible]YAiO[illegible]aX[illegible]biM[illegible]DcuM
[illegible]aW[illegible]mF[illegible]mLTc[illegible]NDc
[illegible]XRm[illegible]iO
jAwMDgxQTk[illegible]zBabThOLUkzSnh
3TUFBQUFBQUF[illegible]JDbG91ZFBDLlJlY
WQuQWxsI[illegible]Z2VtZW50QXB
wcy5SZWFkV3JpdGUuQWxsIE[illegible]hZW1lbnRDb25maWd1cmF0aW9uL
lJlYWRXcml0ZS5BbGwgRGV[illegible]hWVudE1hbmFnZWREZXZpY2VzLlB
```

```
HTTP/1.1 200 OK
Content-Type:
application/json;odata.metadata=minimal;odata.streaming=true;IEEE754Compatible=false;charset=utf-8
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000
request-id: 9332722f-ea18-476c-92d5-6912c31a8145
client-request-id: 5d3a61ae-8b9c-4782-9d3d-8e1f7795f7f8
x-ms-ags-diagnostic: {"ServerInfo":{"DataCenter":"West Europe","Slice":"E","Ring":"5","ScaleUnit":"002","RoleInstance":"AM2PEPF0000C5F4"}}
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: ETag, Location, Preference-Applied, Content-Range, request-id, client-request-id, ReadWriteConsistencyToken, SdkVersion, WWW-Authenticate, x-ms-client-gcc-tenant
OData-Version: 4.0
Date: Sun, 17 Apr 2022 09:50:03 GMT
Connection: close
Content-Length: 1095

{
  "@odata.context":
  "https://graph.microsoft.com/beta/$metadata#deviceAppManagement/mobileApps('59d4753a-8e77-4655-a1ed-2efafdb6e759')/microsoft.graph.windowsMobileMSI/contentVersions('1')/files/$entity",
  "azureStorageUri":
  "https://mmcswdb01.blob.core.windows.net/ff080809-457e-461b-9b6d-7f08147853ed/4f7e00d2-17eb-4a1c-afde-f94c40c2bee8/d1c2ebdc-64f0-4d1e-a99a-7ec7833067e8.msi.bin",
  "isCommitted":true,
```

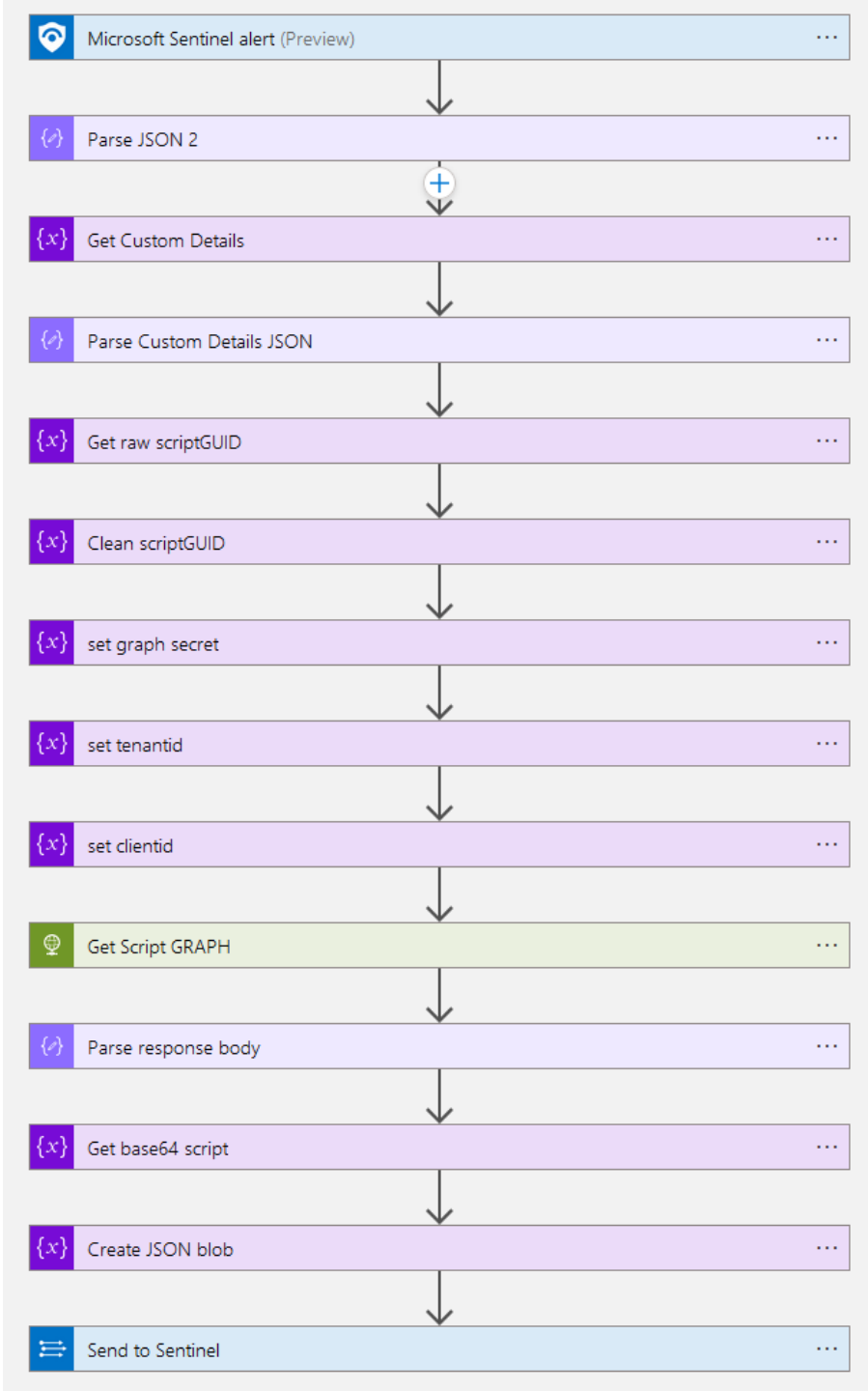
CHECKSCRIPT

- /beta/deviceAppManagement/mobileApps/bd9a8755-f8b8-4f78-b165-733fd0fb81a3/?$expand=categories,assignments

```
GET
/beta/deviceAppManagement/mobileApps/bd9a8755-f8b8-
4f78-b165-733fd0fb81a3/?$expand=
categories,assignments HTTP/1.1
Host: graph.microsoft.com
X-Ms-Client-Session-Id:
a9fa7d2f3fd14d00a30dd889a3c02475
X-Content-Type-Options: nosniff
X-Ms-Command-Name: fetchApplication
Accept-Language: en
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJub25jZSI6IjBCb3UzRnNvRUdBVWN2YkE
```

```
      "v10_1703":false,
      "v10_1709":false,
      "v10_1803":false,
      "v10_1809":false,
      "v10_1903":false,
      "v10_1909":false,
      "v10_2004":false,
      "v10_2H20":false,
      "v10_21H1":false
    },
    "detectionRules":[
      {
        "@odata.type":
        "#microsoft.graph.win32LobAppPowerShellScript
        Detection",
        "enforceSignatureCheck":false,
        "runAs32Bit":false,
        "scriptContent":
        "QzpcV2luZG93c1xTeXNOZWOzMlxXaW5kb3dzUG93ZXJT
        aGVsbFx2MS4wXFBvd2VyU2hlbGwuZXhlIC1Db21tYW5kI
        CJ3aG9hbWkgfCBPdXQtRmlsZSAtRmlsZVBhdGggQzpcdG
        VtcFx2aWFfY3VzdG9tX2NoZWNrX3Njcmlwdc50eHQi"
      }
```

AUTOMATISCH VERRIJKEN



AUTOMATISCH VERRIJKEN

6-9-2022

OUTPUTS — Show raw outputs

Status code

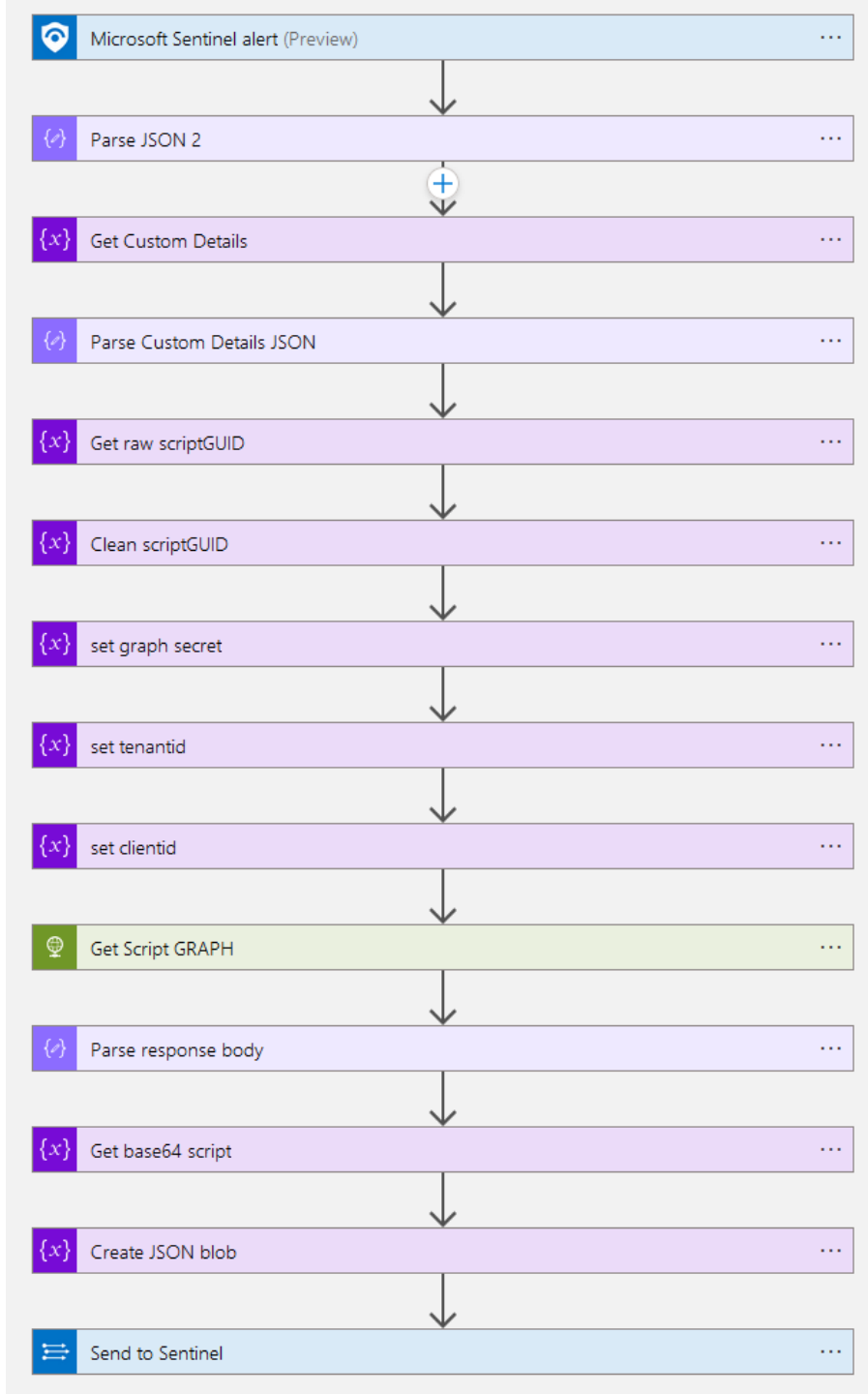
200

Headers

Key	Value
Transfer-Encoding	chunked
Vary	Accept-Encoding
Strict-Transport-Security	max-age=31536000

Body


```
"scriptContent": "QzpcV2luZG93c1xTeXN0ZW0zMlxXaW5kb3dzUG93ZXJTa
"createdDateTime": "2022-09-06T08:25:39.3669843Z",
"lastModifiedDateTime": "2022-09-06T08:25:39.3669843Z",
"runAsAccount": "system",
"fileName": "asd.ps1",
"roleScopeTagIds": [
  "0"
```

```
1  intune_scripts_cl_CL
2  | limit 10
3
```

Results | Chart

TimeGenerated [UTC]	_odata_context_s	enforceSignatureCheck_b	runAs32Bit_b	displayName_s	scriptContent_s
6-9-2022 09:24:19....	https://graph.microsoft.com/beta/$metadata#deviceMana...	false	true	zxczxczxc	QzpcV2luZG93c1xTeXN(

TenantId	d75bef37-98a2-4b28-8bf2-2fced09c4401
SourceSystem	RestAPI
TimeGenerated [UTC]	2022-09-06T09:24:19.474Z
_odata_context_s	https://graph.microsoft.com/beta/$metadata#deviceManagement/deviceManagementScripts(assignments())/$entity
enforceSignatureCheck_b	false
runAs32Bit_b	true
displayName_s	zxczxczxc
scriptContent_s	QzpcV2luZG93c1xTeXN0ZW0zMlxXaW5kb3dzUG93ZXJTaGVsbFx2MS4wXFBvd2VyU2hlbGwuZXhlIC1Db21tYW5kICJaG9hbWkgfCBPdXQtRmlsZSAtRmlsZVB
createdDateTime_t [UTC]	2022-09-06T09:16:05.244Z
lastModifiedDateTime_t [UTC]	2022-09-06T09:16:05.244Z
runAsAccount_s	system
roleScopeTagIds_s	["0"]
assignments_odata_context_s	https://graph.microsoft.com/beta/$metadata#deviceManagement/deviceManagementScripts('fbfba0ce-ac32-481a-b7fe-6dfbce0cfe15')/assignments
assignments_s	[]
fileName_s	asd.ps1
id_g	fbfba0ce-ac32-481a-b7fe-6dfbce0cfe15
Type	intune_scripts_cl_CL

```
1  intune_scripts_cl_CL
2  | extend a = base64_decode_tostring(scriptContent_s)
3  | project a
4
```

Results Chart | Add bookmark

a
>
> C:\Windows\System32\WindowsPowerShell\v1.0\PowerShell.exe -Command "whoami | Out-File -FilePath C:\temp\via_script_exec.txt"
> C:\Windows\System32\WindowsPowerShell\v1.0\PowerShell.exe -Command "whoami | Out-File -FilePath C:\temp\via_script_exec.txt"
> C:\Windows\System32\WindowsPowerShell\v1.0\PowerShell.exe -Command "whoami | Out-File -FilePath C:\temp\via_graph_api_demovideo.txt"
> C:\Windows\System32\WindowsPowerShell\v1.0\PowerShell.exe -Command "whoami | Out-File -FilePath C:\temp\via_graph_api.txt"
> C:\Windows\System32\WindowsPowerShell\v1.0\PowerShell.exe -Command "whoami | Out-File -FilePath C:\temp\via_script_exec.txt"

AUTOMATISCH VERRIJKEN

- Automatisch verwerken is lastig in sommige gevallen
- Opties voor vervolgstappen
  - Opslaan in Sentinel
  - Opslaan in blobstorage
  - Sigma webservice bouwen


```
"value": [
  {
    "id": "0",
    "settingInstance": {
      "@odata.type": "#microsoft.graph.deviceManagementConfigurationChoiceSettingInstance",
      "settingDefinitionId": "device_vendor_msft_policy_config_admx_logon_run_2",
      "settingInstanceTemplateReference": null,
      "choiceSettingValue": {
        "settingValueTemplateReference": null,
        "value": "device_vendor_msft_policy_config_admx_logon_run_2_1",
        "children": [
          {
            "@odata.type": "#microsoft.graph.deviceManagementConfigurationSimpleSettingCollectionInstance",
            "settingDefinitionId": "device_vendor_msft_policy_config_admx_logon_run_2_runlistbox2",
            "settingInstanceTemplateReference": null,
            "simpleSettingCollectionValue": [
              {
                "@odata.type": "#microsoft.graph.deviceManagementConfigurationStringSettingValue",
                "settingValueTemplateReference": null,
                "value": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\PowerShell.exe -Command \"'Hoi' | Out-File -FilePath C:\\temp\\via_ru
              }
            ]
          }
        ]
      }
    },
```

APP PACKAGES

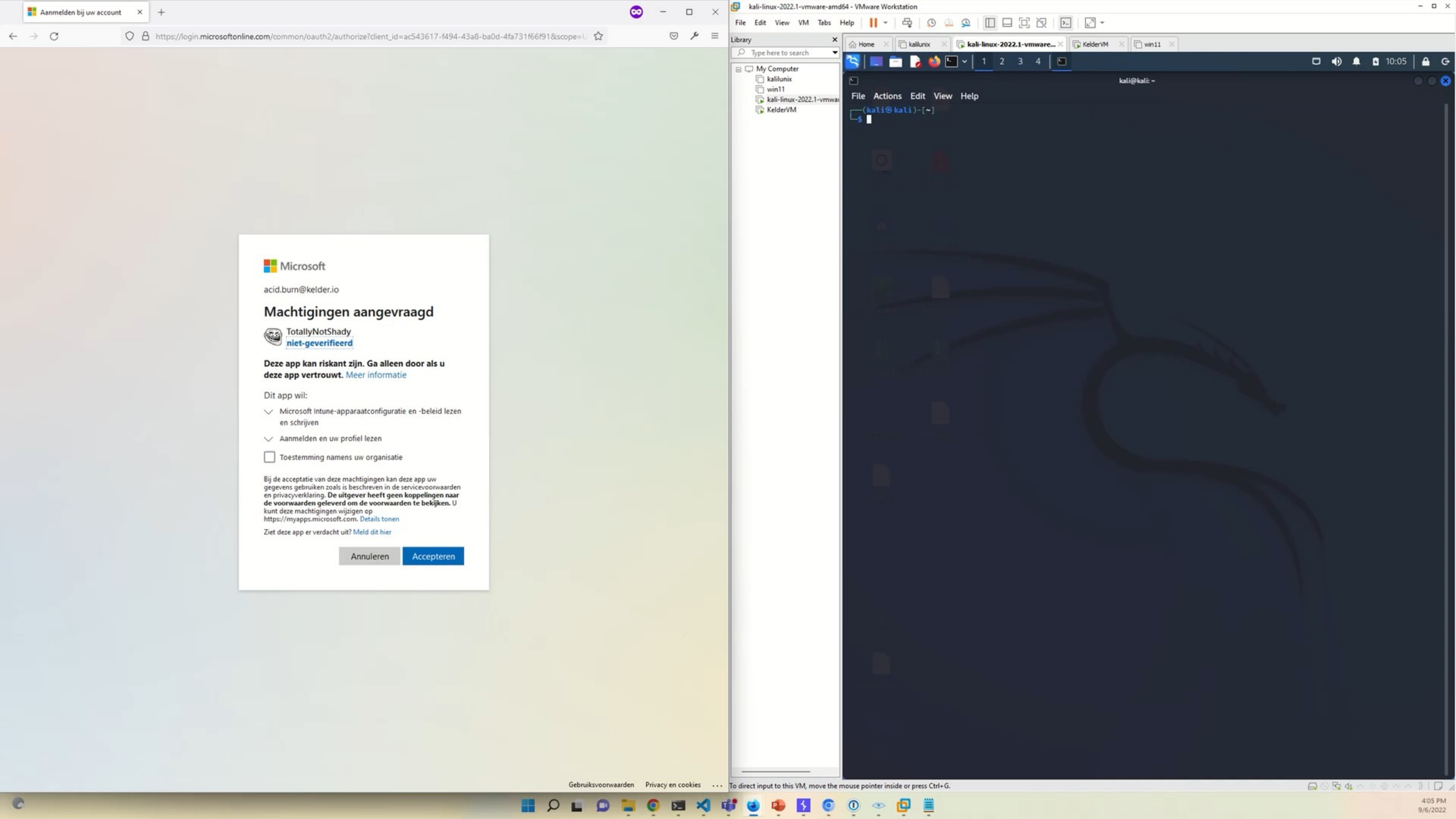
- Submitten naar sandbox?
- Msi packages zijn anoniem te downloaden
  - https://mmcswdb01.blob.core.windows.net/ff080809-457e-461b-9b6d-7f08147853ed/4f7e00d2-17eb-4a1c-afde-f94c40c2bee8/d1c2ebdc-64f0-4d1e-a99a-7ec7833067e8.msi.bin

- Encrypted packages, lastig verrijken.
- Als we die kunnen decrypten is het een interessante host voor backdoors ☺

OAUTH PHISH

OAUTH PHISH


Microsoft
acid.burn@kelder.io
Machtigingen aangevraagd
TotallyNotShady
niet-geverifieerd
Deze app kan riskant zijn. Ga alleen door als u deze app vertrouwt. Meer informatie
Dit app wil:
Microsoft Intune-apparaatconfiguratie en -beleid lezen en schrijven
Aanmelden en uw profiel lezen
Toestemming namens uw organisatie
Bij de acceptatie van deze machtigingen kan deze app uw gegevens gebruiken zoals is beschreven in de servicevoorwaarden en privacyverklaring. De uitgever heeft geen koppelingen naar de voorwaarden geleverd om de voorwaarden te bekijken. U kunt deze machtigingen wijzigen op https://myapps.microsoft.com. Details tonen
Ziet deze app er verdacht uit? Meld dit hier
Annuleren
Accepteren


Aanmelden bij uw account
https://login.microsoftonline.com/common/oauth2/authorize?client_id=ac543617-f494-43a8-ba0d-4fa731f66f91&scope=U
Microsoft
acid.burn@kelder.io
Machtigingen aangevraagd
TotallyNotShady
niet-geverifieerd
Deze app kan riskant zijn. Ga alleen door als u deze app vertrouwt. Meer informatie
Dit app wil:
Microsoft Intune-apparaatconfiguratie en -beleid lezen en schrijven
Aanmelden en uw profiel lezen
Toestemming namens uw organisatie
Bij de acceptatie van deze machtigingen kan deze app uw gegevens gebruiken zoals is beschreven in de servicevoorwaarden en privacyverklaring. De uitgever heeft geen koppelingen naar de voorwaarden geleverd om de voorwaarden te bekijken. U kunt deze machtigingen wijzigen op https://myapps.microsoft.com. Details tonen
Ziet deze app er verdacht uit? Meld dit hier
Annuleren
Accepteren
Gebruiksvoorwaarden
Privacy en cookies
kali-linux-2022.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kalilunix
win11
kali-linux-2022.1-vmwar
KelderVM
Home
kalilunix
kali-linux-2022.1-vmware...
KelderVM
win11
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
4:05 PM
9/6/2022

Search (Ctrl+/)

Overview

Manage

Properties

Monitor

Device status

User status

Basics Edit

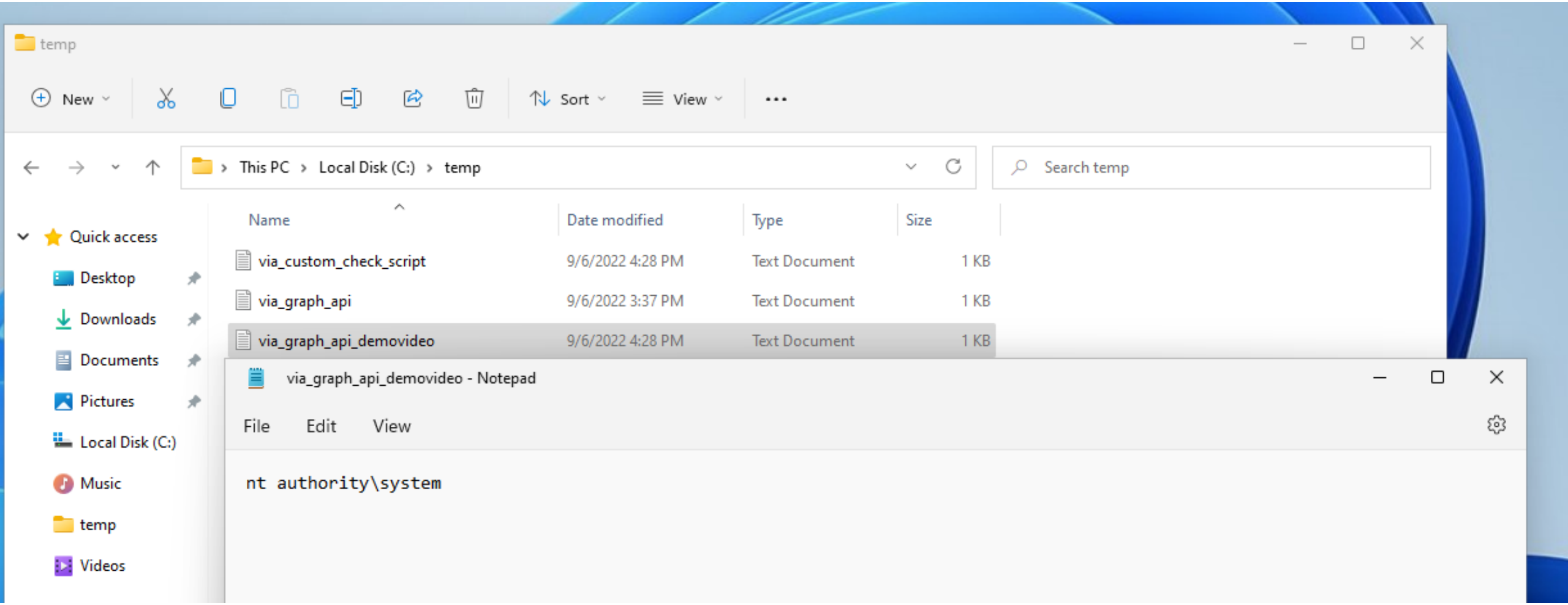
Name	via_graph_api_demo
Description	--

Script settings Edit

PowerShell script	asd.ps1
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	No

Assignments Edit

Included groups	--
Excluded groups	--


temp
New
Sort
View
This PC › Local Disk (C:) › temp
Search temp
Quick access
Desktop
Downloads
Documents
Pictures
Local Disk (C:)
Music
temp
Videos
Name
Date modified
Type
Size
via_custom_check_script 9/6/2022 4:28 PM Text Document 1 KB
via_graph_api 9/6/2022 3:37 PM Text Document 1 KB
via_graph_api_demovideo 9/6/2022 4:28 PM Text Document 1 KB
via_graph_api_demovideo - Notepad
File Edit View
nt authority\system

Edit application

...

Windows app (Win32)

App information | Program | Requirements | **Detection rules** | Review + save

Configure app specific rules used to detect the presence of the app.

Rules format * : Use a custom detection script

Script file : Select a file

Run script as 32-bit process on 64-bit clients : Yes / No

Enforce script signature check and run script silently : Yes / No

DEFENCE

- User risk detectie lijkt te helpen
- Monitor logs het toevoegen van scripts en packages zou gekoppeld moeten zijn aan een change process?
- Verrijk je logs
  - -> Logic apps zal ik publiceren als ze af zijn
- Let op AV detecties uit:
  - C:\Windows\IMECache*
  - C:\Program Files (x86)\Microsoft Intune Management Extension*

VRAGEN?