

Samodejna klasifikacija in prioritizacija Detekcije

New ▾

Summary Analysis Comments Log

Info and above (default) ▾

Quick actions

Isolate affected device

Scan device

Collect forensics package

More response actions ⓘ

Elevate to WithSecure

Elevate

Company

A1 Trainer

Affected devices (1)

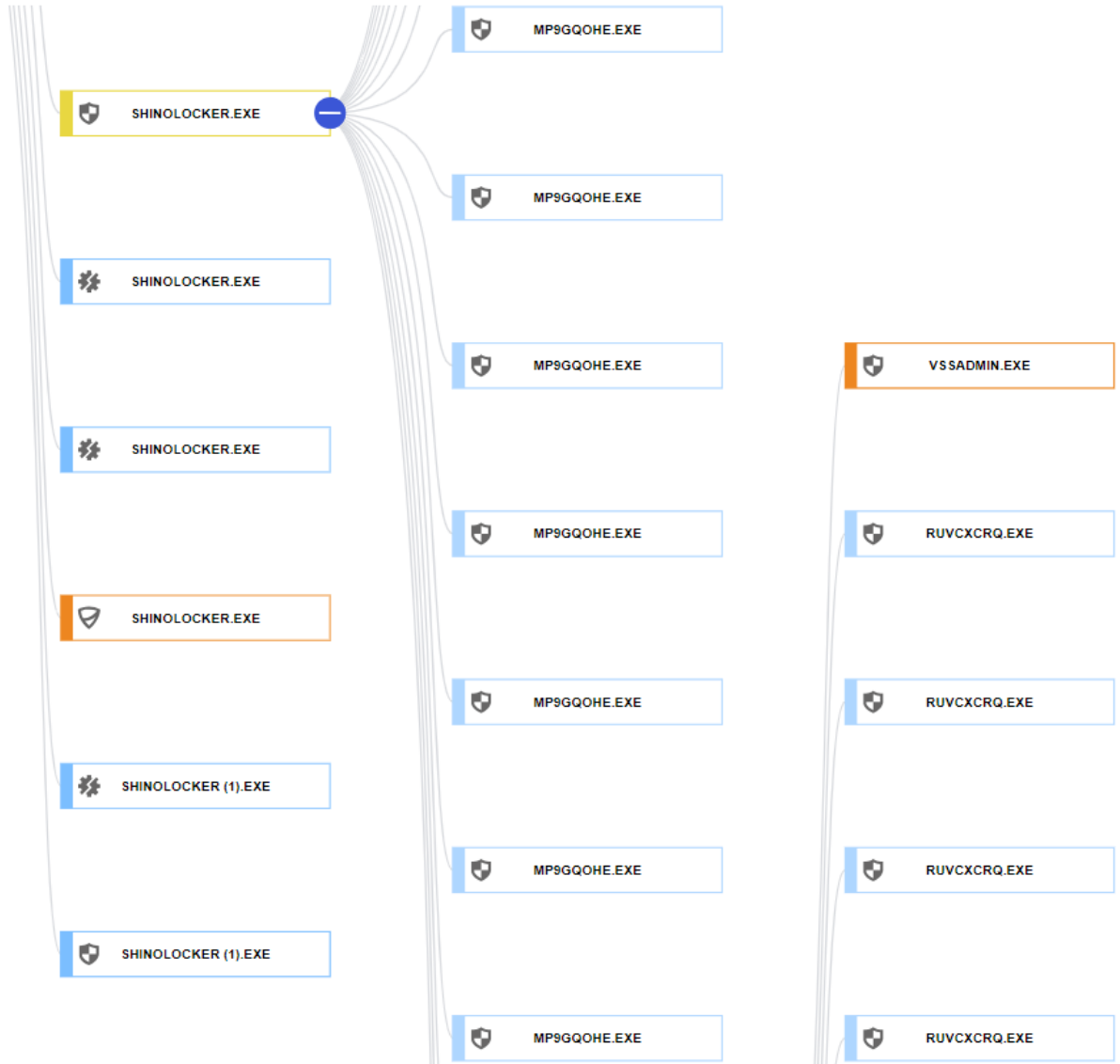
WinDev2310Eval

Identical detections (0)

Similar detections (0)



WINDEV2310EVAL



BCD združuje več security eventov v skupen pogled

DeepGuard je pred ugasnitvijo Real-Time Scanninga na EPP delu uspešno blokiral vse kriptoloker poskuse

Ko je Real-Time Scan izklopljen, vidimo da je kriptoloker najprej pobrisal shadow copies preko vssadmin

209 detections, 50 processes, 1 device

Search detection or process name

- Shadow copies deleted, High (2 occurrences)
vssadmin.exe
vssadmin.exe
- Epp deepguard block detection, High (4 occurrences)
explorer.exe
shinolocker.exe
explorer.exe
explorer.exe
- Malicious module by orsp, High (1 occurrence)
shinolocker.exe
- Epp on access detection, Medium (3 occurrences)
explorer.exe
explorer.exe
explorer.exe
- Selfdeletion with cmd, Medium (1 occurrence)
cmd.exe
- Network connection by malicious module, Medium (1 occurrence)
shinolocker.exe
- Pe file operation by shinolocker (1).exe, Low (4 occurrences)
shinolocker (1).exe

Proces, ki je izvajal kriptiranje

mp9gqohE.exe ⓘ

Remove

Username	WINDEV2310EVAL\User
Command line	"C:\Users\User\AppData\Local\Temp \MP9gqohE.exe" E Wez03hsEhpTFfclBCH1CnQ== D91JCmnNvM0WuimxR7PuQ== "C:\Users\User\Desktop\logos\iStor_ swiss.png"
Path	%temp%
PID	10964
SHA1	f577d8bd839161bf5101afb4bc553d1 cdfee7c3 ↗
Execution start	08.11.2023 09:41:06 UTC+01:00
Execution end	08.11.2023 09:41:06 UTC+01:00

Iz Command line se vidi,
katero datoteko je spremenil

Event search s filtrom za najden proces in tip „file_access“

Najdene vse datoteke, ki jih je kriptolocker kriptiral

Filter: Please Select Please Select Enter filter value Add

Clear all filters

Created Estimate Within Last 7 Days Organization Equals A1 Trainer Event Type Equals file_access Process Name Equals MP9gqoh.exe

	Created Estimate	Received	Process Na...	Event Type	Process CMDL	
✓	2 days ago 08.11.2023 09:41:17 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\WithSecure_mark_charcoal_black.png"
✓	2 days ago 08.11.2023 09:41:17 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\Vade Logo RGB.png"
✓	2 days ago 08.11.2023 09:41:17 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\WithSecure_logo_charcoal_black.png"
✓	2 days ago 08.11.2023 09:41:17 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\WithSecure_mark_charcoal_black.png"
✓	2 days ago 08.11.2023 09:41:17 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\Vectra-Logo-with-Tagline.png"
✓	2 days ago 08.11.2023 09:41:17 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\Vectra-Logo-with-Tagline.png"
✓	2 days ago 08.11.2023 09:41:16 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\Logo PORT Designs Connect.png"
✓	2 days ago 08.11.2023 09:41:16 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\Logo_A1_Logo_Std_Red_Pos_3_L.png"
✓	2 days ago 08.11.2023 09:41:16 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\Vade Logo RGB.png"
✓	2 days ago 08.11.2023 09:41:16 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\logo-Stormshield-center.png"
✓	2 days ago 08.11.2023 09:41:16 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\WithSecure_logo_charcoal_black.png"
✓	2 days ago 08.11.2023 09:41:16 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\Logotype_WALLIX_2020_White-Orange.png"
✓	2 days ago 08.11.2023 09:41:16 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\Logo_A1_Logo_Std_Red_Pos_3_L.png"
✓	2 days ago 08.11.2023 09:41:15 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\Logo PORT Designs Connect.png"
✓	2 days ago 08.11.2023 09:41:15 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\F-SECURE_LOGO_HORIZONTAL_POSITIVE_...
✓	2 days ago 08.11.2023 09:41:15 UTC+0...	2 days ago 08.11.2023 09:41:54 UTC+01:00	MP9gqoh.exe	file_access	"C:\Users\User\AppData\Local\Temp\MP9gqoh.exe" E Wez03hsEhpTffclBCH1CnQ== D91JCmhNvM0wulmxRf7PuQ==	C:\Users\User\Desktop\logos\iStor_swiss.png"

Uporabljen Encryption KEY za kriptolocker

Ročni odziv na zaznave: zaustavitev procesa + memory dump IN/ALI izbris datoteke (hkrati upload na Elements portal)

- ENDPOINT PROTECTION
- ENDPOINT DETECTION AND RESPONSE
- Dashboard
- Broad Context Detections
- Event search
- Devices
- Software
- Response**
- Downloads
- Reports
- Settings
- Support
- Subscriptions
- VULNERABILITY MANAGEMENT
- Dashboard

Actions

process

- Process memory dump (Windows)
Retrieves memory dumps of one or more processes.
- Kill Process (Windows)
Kills processes with memory capture.
- Enumerate processes
Enumerates running processes.

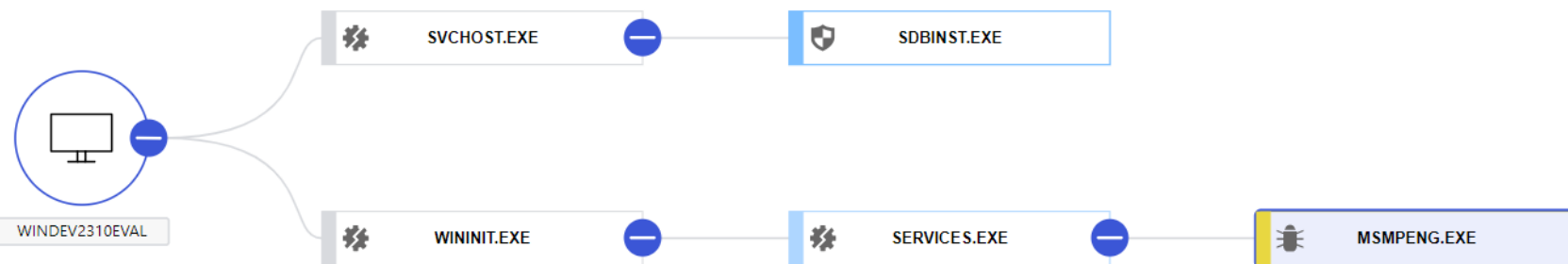
delete

- Delete registry
Deletes a registry key or value. This deletes a value if one is specified, otherwise deletes the key.
- Delete files
Deletes files or folders and verifies the file system state afterwards. Files may optionally be retrieved before deletion.
- Delete scheduled tasks
Deletes Windows scheduled tasks.
- Delete services
Deletes Windows services.

2
Actions

3
Parameters

4
Summary



Info and above (default)

Tudi Windows Defender zaznave ransomware-a so vidni kot EDR detection

WinDev2310Eval
1 processes added

msmpeng.exe

EPP scan
Infection name Ransom:MSIL/ShinoLock.A
Type FILE
Reference file:_C:\Users\User\AppData\Local\Temp\EB9KZ9bV.exe
System wide false

Detection 2/3 : Defender detected threat **Medium**
08.11.2023 09:58:15 UTC+01:00

Description Microsoft Defender has detected a threat in file:_C:\Users\User\AppData\Local\Temp\EB9KZ9bV.exe

Event ID(s) 01328d84-7e15-11ee-aed8-0242ac110008

EPP scan
Infection name Ransom:MSIL/ShinoLock.A
Type FILE
Reference file:_C:\Users\User\AppData\Local\Temp\EB9KZ9bV.exe
System wide false

Detection 3/3 : Defender action threat **Low**
08.11.2023 09:58:31 UTC+01:00