SAC

Saving Code and Intelligence to Custom Repositories

Uncoder Al

Confidential and Proprietary. Do not distribute without consent. © SOC Prime 2025. All rights reserved.

Saving Code and Intelligence to Custom Repositories

C Detection Rules Sigma Select Platform Image: TRANSLATE Image: Transmarker Selection Image: Transmarker Selection Image: Transmarker Selection Select Platform Image: Transmarker Selection Image: Transmarker Selection Image: Transmarker Selection Select Platform Image: Transmarker Selection Select Platform Select Platform Image: Transmarker Selection Image: Transmarker Selection Select Platform Select Platform Select Platform Image: Transmarker Selection Image: Transmarker Selection Select Platform Select Platform Select Platform Image: Transmarker Selection Image: Transmarker Selection Select Platform Select Platform Select Platform Image: Transmarker Selection Image: Transmarker Selection Select Platform Select Platform Select Platform Image: Transmarker Selection Image: Transmarker Selection Select Platform Select Platform Select Platform Image: Transmarker Selection Image: Transmarker Selection Select Platform Select Platform Select Platform Image: Transmarker Selection Image: Transmarker Selection Select Platform Select Platform Select Platform Select Platfo					ln p	roduction	
ittle: Rorschach Ransomware Execution Activity Save		Sigma 🗸	← Select Platform	m •	\$	TRANSLATE	
<pre>1 itile: Rorshank Ransommere Execution Activity itile: Rorshank Ransommere Execution Activity itile: Rorshank Ransommere execution activity references:</pre>	1 🗿 🔖 Al Tools 🗸 🕸 🕒 Save As 🗸 🤀 Contribute 🖉	လ Validate 📫 Intelligence ြည ပြို 🗊	Save			Cancel Save	
4 description: Detects Rorschach ransomware execution activity Sigma 5 - https://research.checkpdint.com/2023/norschach-a-new-sophisticated-and-fast-ransomware/ Content from M3 Sigma 7 author: X_Junior (Mextron Systems) Content from M3 Sigma 7 author: X_Junior (Mextron Systems) Content from M3 Sigma 7 author: X_Junior (Mextron Systems) Content from M3 Sigma 7 author: X_Junior (Mextron Systems) Content from M3 Sigma 7 author: X_Junior (Mextron Systems) Content from M3 Sigma 7 author: X_Junior (Mextron Systems) Content from M3 Content Name 8 author: X_Junior (Mextron Systems) Content from M3 Content Name 7 author: X_Junior (Mextron Systems) Content from M3 Content Name 8 author: X_Junior (Mextron Systems) Description Description 13 - attack.definits exection Description Severity Status 15 Lossource: Content from M3 Severity Status 16 - Vettion: Content Name Content Name Severity	1 title: Rorschach Ransomware Execution Activity 2 id: 0e9e6c63-1350-48c4-9fa1-7ccb235edc68						
 - https://research.checkopinf.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/ - uthor: X_Junior (Nextron Systems) date: 2023-04-02 - datex.ktu659.0081 - attack.ktu659.0081 - attack.defense-evasion - detection - detection: - detection: - detection: - bodedit.axe - hoetlense - hoetlense<	4 description: Detects Rorschach ransomware execution activity			~	Sigma	~	
attroit A_Johnor (Nextron systems) date: 22-64-64 modified: 2023-64-22 in task.	6 - https://research.checkpoint.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/			Content Name			
<pre>product whether is a set of the set of</pre>							
111 - attack.execution Description 12 - attack.tdefs.execution Description 13 - attack.defsnse-evasion - detection.emerging-threats 14 - detection.emerging-threats - detection attivity 15 - togsource: - detection: 16 - detection: - selection: 17 - product: windows - selection: 18 - detection: - selection: 19 - selection: - vhet.exe 21 - Vhotdedit.exe - vhet.exe 22 - Vhetsh.exe - vhet.exe 23 - Vhetl.exe - Vestine: 24 - Vhetsh.exe - vestine: 25 - Vissadmin.exe • MiTRE ATT&CK 26 - ImageIendswith: - vestine: 27 - CommendLine[contains: 'l111111' 28 - Condition: selection • Test 29 - ImageIendswith: - vestine: 20 - ImageIendswith: - vestine: 24 - Vhetsh.exe • Parse Metadata 25 - Vissadmin.exe • Parse Metadata 26 - Outperse Evasion (TA0005) × Execution (TA0002) × 27 - GrammadLine[contains: 'l111111' 28 - condition: selection 29 - falsepositives: Defense Evasion (TA0005) × Execut				Rorschach Ransomware Execution Activity			
13 - attack.defense-evasion 14 - detection.energing-threats 15 Logsource: 16 category: process_creation 17 product: windows 16 category: process_creation 17 product: windows 18 detection: 19 selection: 12 - \bcdedit.exe 22 - \net.exe 23 - \net.exe 24 - \net.exe 25 - \wevtutil.exe 26 - \wevtutil.exe 27 CommandLine[contains: 'lillilli' 28 condition: selection 29 falsepositives: 30 - Unlikely				Description			
14 - detection.emerging-threats 15 logsource: 16 category: process_creation 17 product: windows 18 detection: 19 selection: 21 - \hocdedit.exe 22 - \hotdedit.exe 23 - \hott.exe 24 - \hottsh.exe 25 - \westufil.exe 26 - \vestufil.exe 27 CommendLine[contains: '1111111' 28 condition: selection 29 falsepositives: 30 - Unlikely	12 - attack.t1059.003						
15 - logsource: 16 category: process_creation 17 product: windows 18 - detection: 19 - selection: 20 - Imagelendswith: 21 21 - \bcdedit.exe 22 - \net.exe 23 24 - \netsh.exe 25 26 - \vssadmin.exe 26 27 CommandLine[contains: '1111111' 28 condition: selection 29 - falsepositives: 20 - Unlikely Mittre Attack 21 - \vssadmin.exe 22 - \net.exe 23 - \netsh.exe 24 - \netsh.exe 25 - \wssadmin.exe 26 - \vssadmin.exe 27 - CommandLine[contains: '1111111' 28 - Gondition: selection 29 - falsepositives: 29 - Inlikely Defense Evasion (TA0005) × Execution (TA0002) ×				Detects Rorschach ransomware execution activity			
16 category: process_creation 17 product: windows 18 detection: 29 Image[endswith: 21 - \bodedit.exe 23 - \net.exe 23 - \net.exe 24 - \netsh.exe 25 - \weytutil.exe 26 - \veytutil.exe 27 CommandLine[contains: '1111111' 28 condition: selection 29 - Unlikety							
17 product: windows 18 detection: 19 selection: 19 selection: 20 Imagelendswith: 21 - \bcdedit.exe 22 - \net.exe 23 - \net.exe 24 - \netsh.exe 25 - \wevtutil.exe 26 - \vestufin.exe 27 CommandLine[contains: '1111111' 28 condition: selection 29 - falsepositives: 30 - Unlikety							
18 · detection: 19 · selection: 10 · Imagelendswith: 11 · \boddit.exe 22 · \net.exe 23 · \netl.exe 24 · \netsh.exe 25 · \wevtutil.exe 26 · \vssadmin.exe 27 · CommandLine[contains: '1111111' 28 · condition: selection 29 · falsepositives: 30 · Unlikety							
19 - selection: 20 - Image[endswith: 21 - \bodedit.exe 22 - \net.exe 23 - \neti.exe 23 - \neti.exe 24 - \netsh.exe 25 - \weytutil.exe 26 - \veysamin.exe 27 CommandLine[contains: '1111111' 28 condition: selection 29 - falsepositives: 30 - Unlikely							
28 - Image[endswith: Severity Status 21 - \bcdedit.exe Severity Status 22 - \net.exe Critical Test 23 - \netl.exe Critical Test 24 - \netsh.exe MMITRE ATT&CK Parse Metadata 25 - \wssdmin.exe CommandLine[contains: '1111111' 28 - Unit: Severity Status 29 - falsepositives: Test 29 - Unitkety Defense Evasion (TA0005) × Execution (TA0002) ×							
21 - \bcdedit.exe Severity Status 22 - \net.exe Critical Test 23 - \netsh.exe Critical Image: Critical 24 - \netsh.exe Image: Critical Image: Critical 25 - \weytutil.exe Image: Critical Image: Critical 26 - \veytutil.exe Image: Critical Image: Critical 27 CommandLine[contains: '1111111' Image: Critical Image: Critical 28 condition: selection Image: Critical Image: Critical 29 falsepositives: Tactics Defense Evasion (TA0005) × 30 - Unlikety Image: Critical Image: Critical							
23 - \net1.exe 24 - \netsh.exe 25 - \wevtutil.exe 26 - \vssadmin.exe 27 CommandLine[contains: '1111111' 28 condition: selection 29 - falsepositives: Tactics 30 - Unlikety			Severity		Status		
24 - \netSh.exe 25 - \weytutil.exe 26 - \vssadmin.exe 27 CommandLine contains: '11111111' 28 condition: selection 29 falsepositives: 30 - Unlikely	22 - \net.exe						
25 - \wevtutil.exe 26 - \vssadmin.exe 27 CommandLine[contains: '1111111' 28 condition: selection 29 - falsepositives: Tactics 30 - Unlikely	23 - \net1.exe		Critical		Test		
26 - \vssadmin.exe 27 CommandLine[contains: '1111111' 28 condition: selection 29 - falsepositives: Tactics 30 - Unlikely							
27 CommandLine contains: '11111111' 28 condition: selection 29 - falsepositives: Defense Evasion (TA0005) × Execution (TA0002) × 30 - Unlikely							
28 condition: selection 29 - falsepositives: Tactics 30 - Unlikely			MITRE ATT&CK			😵 Parse Metadata	
29 falsepositives: 30 - Unlikely Defense Evasion (TA0005) × Execution (TA0002) ×							
30 - Unlikely			Tactics	Defense Evasion (TA0005) ×	Execution (TA0002) ×		
			Tactics				
	30 - Unlikely 31 level: critical						

Saving Code and Intelligence to Custom Repositories

Enable full detection content life cycle on the SOC Prime Platform. Save rules together with their intelligence and metadata in the standard Threat Detection Marketplace format. Use them just as stock content for manual or automated deployment, Attack Detective scans, etc.

- Storing in secure SOC Prime Platform's cloud infrastructure (with an encrypted rule body at rest)
- Enables centralized full detection content life cycle from development to deployment and documenting
- Native GitLab, GitHub, and Azure DevOps integrations supported
- Convenient access to and format consistency with Threat Detection Marketplace stock content