Threat Assessment: EKANS Ransomware

By Alex Hinchliffe, Doel Santos

Published: 2020-06-26 · Archived: 2026-04-02 11:26:06 UTC

Unit 42 researchers have observed recent EKANS (Snake backward) ransomware activity affecting multiple industries in the U.S and Europe. As a result, we've created this threat assessment report for the activities of this ransomware. Identified techniques and campaigns can be visualized using the Unit 42 Playbook Viewer.

EKANS, which was first observed in January 2020, has relatively basic ransomware behavior, as it primarily seeks to encrypt your files and display a ransom note when finished. Although EKANS is basic in terms of file encryption, it's worth mentioning that it does have some interesting functionalities that make it distinct from other ransomware strains. EKANS ransomware is written in Golang and includes a static "kill list" that will stop numerous antivirus and Industrial Control Systems (ICS) processes and services. After killing the processes, it then proceeds to delete shadow copies to disable any restoration capabilities. Like many ransomware malware families, EKANS attempts to also encrypt resources connected to the victim's machine via the network.

After encrypting files, EKANS doesn't follow a uniform extension change like other active ransomware. Instead, EKANS modifies the extension with five random characters. This may be an attempt by the creators of the ransomware to evade instant detection by just looking at the file extensions. One way to identify an EKANS infection is by looking for the hexadecimal string of EKANS at the end of the file, which is added by the ransomware.

EKANS' intrusion vector at the moment seems to be spearphishing, to compromise credentials. Having file-blocking policies in place, and securing any open Remote Desktop Protocol (RDP) ports will help prevent the malware from entering the network. We encourage ICS asset owners to review their security posture against malware, such as EKANS, that aims to disrupt ICS operations. The EKANS operators have affected different industries including energy, architecture firms, healthcare, transportation, and manufacturing.

Palo Alto Networks Threat Prevention platform with WildFire, and Cortex XDR detects activity associated with this ransomware. Customers can also review activity associated with this Threat Assessment using AutoFocus with the following tag: EKANS.

Several adversarial techniques were observed in this activity and the following measures are suggested within Palo Alto Networks' products and services to ensure mitigation of threats related with the EKANS ransomware, as well as other malware using the similar techniques:

Tactic	Technique (Mitre ATT&CK ID)	Product / Service	Course of Action

Initial Access	Spearphishing Attachment (T1193)	NGFW	Setup File Blocking
		Threat Prevention†	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
			Ensure a secure antivirus profile is applied to all relevant security policies
		WildFire	Ensure that WildFire file size upload limits are maximized
			Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles
			Ensure a WildFire Analysis profile is enabled for all security policies
			Ensure forwarding of decrypted content to WildFire is enabled
			Ensure all WildFire session information settings are enabled
			Ensure alerts are enabled for malicious files detected by WildFire
			Ensure 'WildFire Update Schedule' is set to download and install updates every minute
		Cortex XDR	Configure Malware Security Profile
		Cortex XSOAR	Deploy XSOAR Playbook - Phishing Investigation - Generic V2
			Deploy XSOAR - Endpoint Malware Investigation
Execution	Scheduled Task (T1053)	Cortex XDR	Enable Anti-Exploit
			Enable Anti-Malware Protection
	User Execution (T1204)	NGFW	Ensure that User-ID is only enabled for internal trusted interfaces
			Ensure that 'Include/Exclude Networks' is used if User-ID is enabled

			Ensure that the User-ID Agent has minimal permissions if User-ID is enabled
			Ensure that the User-ID service account does not have interactive logon rights
			Ensure remote access capabilities for the User-ID service account are forbidden.
			Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones
		Threat Prevention†	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
			Ensure a secure antivirus profile is applied to all relevant security policies
			Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats
			Ensure DNS sinkholing is configured on all anti-spyware profiles in use
			Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use
			Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet
		DNS Security	Enable DNS Security in Anti-Spyware profile
		URL Filtering	Ensure that PAN-DB URL Filtering is used
			Ensure that URL Filtering uses the action of “block” or “override” on the <enterprise approved value> URL categories
			Ensure that access to every URL is logged
			Ensure all HTTP Header Logging options are enabled
			Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet

		WildFire	Ensure that WildFire file size upload limits are maximized
			Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles
			Ensure a WildFire Analysis profile is enabled for all security policies
			Ensure forwarding of decrypted content to WildFire is enabled
			Ensure all WildFire session information settings are enabled
			Ensure alerts are enabled for malicious files detected by WildFire
			Ensure 'WildFire Update Schedule' is set to download and install updates every minute
		Cortex XDR	Enable Anti-Exploit
			Enable Anti-Malware Protection
		Cortex XSOAR	Deploy XSOAR Playbook - Phishing Investigation - Generic V2
			Deploy XSOAR Playbook - Cortex XDR - Isolate Endpoint
			Deploy XSOAR - Block Account Generic
Persistence	Bootkit (T1067)	Cortex XDR	Enable Anti-Exploit
			Enable Anti-Malware Protection
	Scheduled Task (T1053)		Enable Anti-Exploit
			Enable Anti-Malware Protection
Privilege Escalation			Enable Anti-Exploit
			Enable Anti-Malware Protection
Credential Access	Credential in Files (T1080)		Enable Anti-Exploit
			Enable Anti-Malware Protection

			Configure Restrictions Security Profile
Discovery	File and Directory Discovery (T1083)		XDR monitors for behavioral events via BIOCs along a causality chain to identify discovery behaviors
	Process Discovery (T1057)		XDR monitors for behavioral events via BIOCs along a causality chain to identify discovery behaviors
Collection	Automated Collection (T1119)		Enable Anti-Exploit
			Enable Anti-Malware Protection
	Data from Local System (T1005)		Enable Anti-Exploit
			Enable Anti-Malware Protection
Command and Control	Custom Command and Control (T1094)	NGFW	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
			Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
			Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists
		Threat Prevention†	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
			Ensure a secure antivirus profile is applied to all relevant security policies
			Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats
			Ensure DNS sinkholing is configured on all anti-spyware profiles in use
			Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use
			Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet

		DNS Security	Enable DNS Security in Anti-Spyware profile
		URL Filtering	Ensure that PAN-DB URL Filtering is used
			Ensure that URL Filtering uses the action of “block” or “override” on the <enterprise approved value> URL categories
			Ensure that access to every URL is logged
			Ensure all HTTP Header Logging options are enabled
			Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet
		Cortex XSOAR	Deploy XSOAR Playbook - Block IP
			Deploy XSOAR Playbook - Block URL
			Deploy XSOAR Playbook - Hunting C&C Communication Playbook
			Deploy XSOAR Playbook - PAN-OS Query Logs for Indicators
Impact	Data Encrypted for Impact (T1486)	Cortex XDR	Enable Anti-Malware Protection
			Enable the “Anti-Ransomware” security module in your security profile
		Cortex XSOAR	Deploy XSOAR Playbook - Ransomware Manual for incident response.

Table 1. Courses of Action for EKANS ransomware
†These capabilities are part of the NGFW security subscriptions service

---