Threat Assessment: Ryuk Ransomware

By Brittany Barbehenn, Doel Santos, Brad Duncan

Published: 2020-10-30 · Archived: 2026-04-05 14:00:59 UTC

Tactic Technique [Mitre ATT&CK ID] Product / Service Course of Action

Initial Access

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 Playbook - Endpoint Malware Investigation

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 that User Credential Submission uses the action of “block” or “continue” on the URL categories

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 XSOAR

Deploy XSOAR Playbook - Block URL Deploy XSOAR Playbook - Phishing Investigation - Generic V2

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 all zones have Zone Protection Profiles that drop specially crafted packets

Cortex XSOAR

Deploy XSOAR Playbook - Access Investigation Playbook Deploy XSOAR Playbook - Impossible Traveler Deploy XSOAR Playbook - Block Account Generic

Execution

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 Protection Enable Anti-Malware Protection

Cortex XSOAR

Deploy XSOAR Playbook - Phishing Investigation - Generic V2 Deploy XSOAR Playbook Cortex XDR - Isolate Endpoint Deploy XSOAR Playbook - Block Account Generic

Cortex XDR

Enable Anti-Exploit Protection Enable Anti-Malware Protection Enable Anti-Exploit Protection Enable Anti-Malware Protection

Persistence

Enable Anti-Exploit Protection Enable Anti-Malware Protection Privilege Escalation Process Hollowing [T1055.012]
(Process Injection [T1055]) Configure Behavioral Threat Protection under the Malware Security Profile

Defense Evasion

Enable Anti-Exploit Protection Enable Anti-Malware Protection Enable Anti-Exploit Protection Enable Anti-Malware Protection Configure Restrictions Security Profile WildFire† Configure Behavioral Threat Protection under the Malware Security Profile

Cortex XDR

Enable Anti-Exploit Protection Enable Anti-Malware Protection

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 Protection Enable Anti-Malware Protection

Credential Access

Enable Anti-Exploit Protection Enable Anti-Malware Protection Configure Restrictions Security Profile

Collection

Enable Anti-Exploit Protection Enable Anti-Malware Protection

Command and Control

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 (Deprecated)

Exfiltration

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 (Deprecated) Deploy XSOAR Playbook - PAN-OS Query Logs for Indicators

Impact

Data Encrypted for Impact [T1486] Deploy XSOAR Playbook - Ransomware Manual for incident response. Inhibit System Recovery [T1490] Deploy XSOAR Playbook - Palo Alto Networks Endpoint Malware Investigation

Cortex XDR

Enable Anti-Exploit Protection Enable Anti-Malware Protection

---