Threat Assessment: Ryuk Ransomware

unit42.paloaltonetworks.com/ryuk-ransomware/

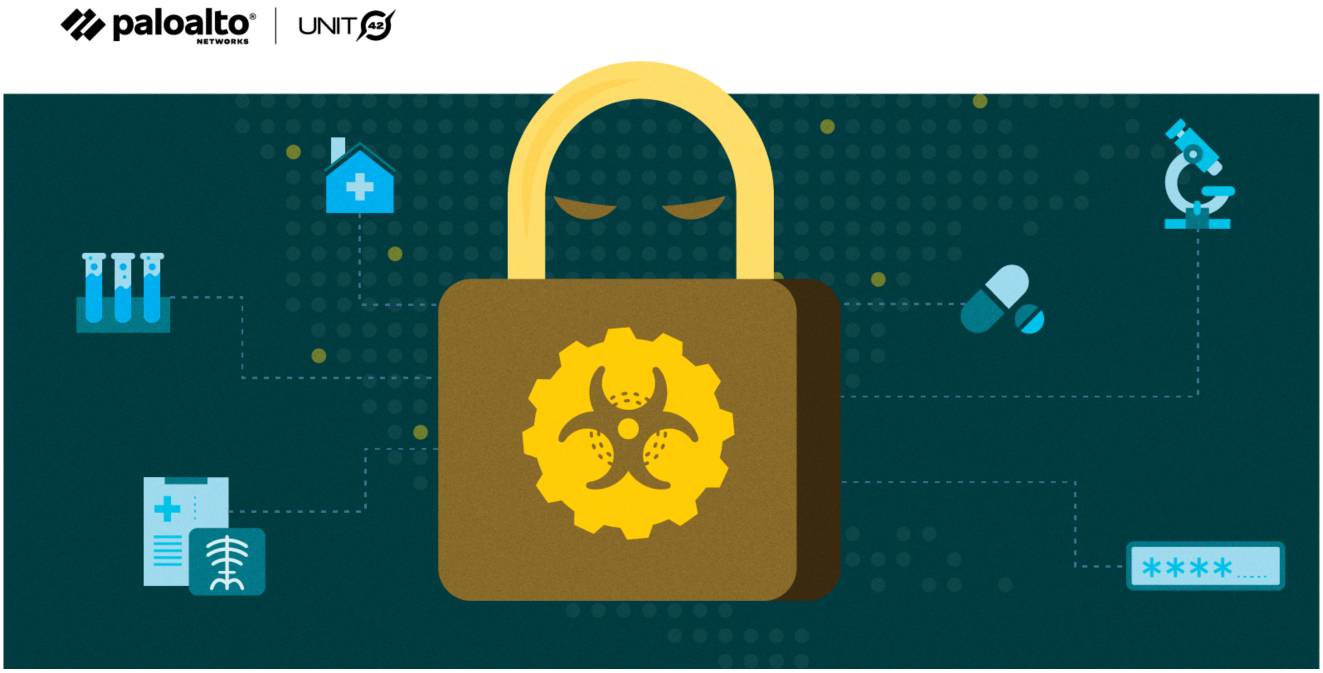
Brittany Barbehenn, Doel Santos, Brad Duncan October 30, 2020

By Brittany Barbehenn, Doel Santos and Brad Duncan

October 29, 2020 at 5:45 PM

Category: Malware, Ransomware, Unit 42

Tags: BazaLoader, joint cybersecurity alert, Ryuk, threat assessment, Trickbot



This post is also available in: 日本語 (Japanese)

Executive Summary

On Oct. 28, 2020, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS) released a joint cybersecurity alert regarding an increased and imminent cybersecurity threat to the U.S. healthcare system.

Threat operators have displayed a heightened interest in targeting the healthcare and the public health sector, potentially disrupting healthcare services and operations. Activities observed include the use of Trickbot malware, a well-known information stealer that can lead to the installation of other malicious files, including Ryuk ransomware.

This alert comes shortly after Universal Health Services (UHS) reported a Ryuk ransomware attack that disrupted all U.S. UHS sites for weeks. Other U.S.-based hospitals have reported similar ransomware attacks, including a hospital in Oregon and one in New York. Similarly, a health tech organization in Philadelphia was also the target of a ransomware attack.

Palo Alto Networks security subscriptions for the Next-Generation Firewall with WildFire detects activity associated with Trickbot and Ryuk. The DNS Security subscription is able to detect the Anchor_DNS DNS tunneling described in this blog. Cortex XDR also contains an Anti-Ransomware Protection module and an Anti-Malware Protection module, which target encryption-based activities associated with ransomware and other malicious file behaviors. Additionally, AutoFocus customers can review activity related to this threat activity with the following tags: Ryuk, Trickbot and BazaLoader.

Malware Overview

Trickbot is modular malware that provides backdoor access, enabling operators to distribute additional malware onto victim systems, and includes other capabilities such as worm functionality and system enumeration. One of the newest modules, Anchor_DNS, is used for DNS tunneling during command and control (C2) actions.

The Anchor_DNS module uses PowerShell to run scripts and makes multiple DNS requests including connectivity checks to benign legitimate domains. Malware often does this to confirm an active network connection that will allow the threat operator to communicate with that system during C2 activities. The following legitimate domains may be used during this check:

ipecho[.]net
api[.]ipify[.]org
checkip[.]amazonaws[.]com
ip[.]anysrc[.]net
wtfismyip[.]com
ipinfo[.]io
icanhazip[.]com
myexternalip[.]com

Table 1. Legitimate domains used by Trickbot Anchor_DNS module to conduct internet connectivity checks.

Ryuk ransomware is typically denoted by a file named “RyukReadMe” placed onto the system. This ransomware is often seen at the end of multi-stage attacks involving malware such as Trickbot and, more recently, BazaLoader (also known as "BazarLoader"). In many cases, Ryuk is not loaded onto the system until weeks or months after the initial infection. Ryuk operators learn the victim network by enumerating the impacted environment with tools that may be familiar to that environment, such as PowerShell and Windows Management Instrumentation.

Prior to encryption, the following commands may be run on a compromised system:

```
C:\Windows\System32\net.exe stop audioendpointbuilder /y
```

```
C:\Windows\System32\net.exe stop samss /y
```

```
C:\Windows\System32\net.exe stop MSSQL$SQLEXPRESS /y
```

You can review the joint cybersecurity advisory for additional details on Ryuk and Trickbot activities associated with the targeting of Healthcare and the Public Health Sector.

The initial intrusion vector for both Trickbot and BazaLoader infections is most often observed through malicious emails.

You can find recently confirmed Trickbot samples on MalwareBazaar and additional information on Trickbot modules on the Unit 42 blog.

Recent samples of Ryuk and BazaLoader can also be found on MalwareBaazar.

More information on ransomware can be found in the 2021 Unit 42 Ransomware Threat Report.

Courses of Action

This section documents the relevant tactics and techniques associated with Ryuk and Trickbot activities and maps them directly to Palo Alto Networks product(s) and service(s). Palo Alto Networks customers can utilize this table to verify current configurations within their environments.

Tactic	Technique [Mitre ATT&CK ID]	Product / Service	Course of Action
Initial Access	Spearphishing Attachment [T1566.001] (Phishing [T1566])	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		
Spearphishing Link [T1566.002] (Phishing [T1566])	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		
Local Accounts [T1078.003] (Valid Accounts [T1078])	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	Malicious File [T1204.002] (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 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		
Windows Command Shell [T1059.003] (Command and Scripting Interpreter [T1059])	Cortex XDR	Enable Anti-Exploit Protection
Enable Anti-Malware Protection		
Scheduled Task [T1053.005] (Scheduled Task/Job [T1053])	Enable Anti-Exploit Protection	
Enable Anti-Malware Protection		
Persistence	Windows Service [T1543.003] (Create or Modify System Process [T1543])	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	Disable or Modify Tools [T1562.001] (Impair Defenses [T1562])	Enable Anti-Exploit Protection
Enable Anti-Malware Protection		
Match Legitimate Name or Location [T1036.005] (Masquerading [T1036])	Enable Anti-Exploit Protection	
Enable Anti-Malware Protection		
Configure Restrictions Security Profile		
Modify Registry [T1112]	WildFire†	Configure Behavioral Threat Protection under the Malware Security Profile
Cortex XDR	Enable Anti-Exploit Protection	
Enable Anti-Malware Protection		
Software Packing [T1027.002] (Obfuscated Files or Information [T1027])	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	Credentials in Files [T1552.001] (Unsecured Credentials [T1552])	Enable Anti-Exploit Protection
Enable Anti-Malware Protection		
Configure Restrictions Security Profile		
Collection	Data from Local System [T1005]	Enable Anti-Exploit Protection

Enable Anti-Malware Protection			
Command and Control	DNS [T1071.004] (Application Layer Protocol [T1071])	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	Exfiltration Over C2 Channel [T1041]	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	

Service Stop [T1489]	Cortex XDR	Enable Anti-Exploit Protection
Enable Anti-Malware Protection		

Table 2. Courses of Action for Ryuk and Trickbot.

†These capabilities are part of the NGFW security subscriptions service.

Conclusion

Ryuk ransomware infections often result from multi-stage threat activities originating from malware such as Trickbot and BazaLoader. Once the backdoor malware is established, attackers use tools such as PowerShell and CobaltStrike to attain remote connection and drop Ryuk onto the compromised system, sometimes weeks to months after initial infection.

The U.S. Government has deemed this threat activity as an imminent threat to Healthcare and the Public Health Sector industry.

Indicators associated with this Threat Assessment and the joint cybersecurity alert are available on GitHub, have been published to the Unit 42 TAXII feed and are viewable via the ATOM Viewer:

https://unit42.paloaltonetworks.com/atoms/ryuk-ransomware/

https://unit42.paloaltonetworks.com/atoms/trickbot/

Palo Alto Networks security subscriptions for the Next-Generation Firewall with WildFire detect activity associated with Trickbot and Ryuk. The DNS Security subscription is able to detect the Anchor_DNS DNS tunneling described in this blog. Cortex XDR also contains an Anti-Ransomware Protection module as well as an Anti-Malware Protection module, which targets encryption-based activities associated with ransomware and other malicious file behaviors. Additionally, AutoFocus customers can review activity related to this threat activity with the following tags: Ryuk, Trickbot and BazaLoader.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

Additional Resources

Mitre ATT&CK Framework

Alert (AA20-302A) - Ransomware Activity Targeting the Healthcare and Public Health Sector

Unit 42 Trickbot reporting