



Wanna Cry Ransomware Guidelines to Stay Safe

The WannaCry ransomware attack is an ongoing cyber-attack of the WannaCry ransomware computer worm targeting the Microsoft Windows operating system. The attack started on Friday, 12 May 2017, infecting more than 230,000 computers in 150 countries, with the software demanding ransom payments in the cryptocurrency Bitcoin in 28 languages.

How do ShareTech UTM and Next-Gen UTM help administrators shut down Wanna Cry Ransomware?

To shut down WanaCrypt0r 2.0 ransomware, there are 3 steps administrators can follow: block IP, block port, allow domain and apply policies.

1. Block the following WannaCry ransomware IP lists.

128.31.0.39/32	
146.0.32.144/32	213.61.66.116/32
188.138.33.220/32	217.79.179.77/32
188.166.23.127/32	38.229.72.16/32
193.23.244.244/32	50.7.161.218/32
2.3.69.209/32	79.172.193.32/32
212.47.232.237/32	81.30.158.223/32
	89.45.235.21/32

Wanna Cry Ransomware Guidelines to Stay Safe

Go to Objects > Address Table > WAN Group > Add> User Define IP

Objects > Address Table

LAN IP Address | LAN Group | DMZ IP Address | DMZ Group | WAN IP Address | WAN Group

▶ Edit Outside Network :

Group Name : WannaCry-IP

Select From IP Address Member

Select From IP Range

Select From IP/Mask

User Define IP

User Define Domain

128.31.0.39/32
146.0.32.144/32
188.138.33.220/32
188.166.23.127/32
193.23.244.244/32
2.3.69.209/32
212.47.232.237/32

(Type the IP address, and then ENTER. Repeat this process in order to add multiple IP addresses.)

Edit

2. Block ports of WannaCry ransomware

Go to Objects > Services Table > Service Group > Add

Objects > Services Table

Basic Service | Service Group

▶ Edit Service Group :

Group Name : WannaCry

	Protocol	Port (Start : End)	
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	135 : 135	Assoc
2	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	445 : 445	Assoc
3	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	137 : 139	Assoc
4	<input type="radio"/> TCP <input checked="" type="radio"/> UDP	135 : 135	Assoc
5	<input type="radio"/> TCP <input checked="" type="radio"/> UDP	445 : 445	Assoc
6	<input type="radio"/> TCP <input checked="" type="radio"/> UDP	137 : 139	Assoc

Edit

Wanna Cry Ransomware Guidelines to Stay Safe

3. Allow WannaCry domain - iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

If the domain name resolves to your IP addresses and it's got package tracking/logging, it means pcs inside your network tries connecting to this domain. Please pay extra attention to the potential ransomware infection.

Objects > Address Table

LAN IP Address | LAN Group | DMZ IP Address | DMZ Group | WAN IP Address | WAN Group

▶ Edit Outside Network :

Group Name : WannaCry-Domain

Select From IP Address Member

Select From IP Range

Select From IP/Mask

User Define IP

User Define Domain

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

(Type the domain, and then ENTER. Repeat this process in order to add multiple domain.)

4. Please refer to our online DEMO to create policies.

4-1. Go to Policy > LAN Policy > LAN to WAN > Add

4-2. Add a policy. Source: inside_any ; Destination: Outside_any ;

Action: Drop ; Service Port or Group: WannaCry (the group created in step 2)

Policy > LAN Policy

LAN to WAN | LAN to DMZ | LAN to LAN | LAN to WAN (IPv6)

▶ Basic Setting

Policy Name

Source ? Inside_Any IP Address

Destination ? Outside_Any IP Address

Action Drop

▶ Policy

Protocol ALL

Service Port or Group ? WannaCry Service Port

Wanna Cry Ransomware Guidelines to Stay Safe

4-3. Add a policy.

Source: inside_any ; Destination: WannaCry-IP (the IP created in step 1);

Action: Drop

Policy > LAN Policy

LAN to WAN | LAN to DMZ | LAN to LAN | LAN to WAN (IPv6)

Basic Setting

Policy Name

Source Inside_Any IP Address

Destination WannaCry-IP IP Address

Action Drop

4-4. Add a policy.

Source: inside_any ; Destination: WannaCry-Domain (the domain created in step 3); Action: Permit

Policy > LAN Policy

LAN to WAN | LAN to DMZ | LAN to LAN | LAN to WAN (IPv6)

Basic Setting

Policy Name

Source Inside_Any IP Address

Destination WannaCry-Domain IP Address

Action Permit

Policies completed as follows.

Policy > LAN Policy

LAN to WAN | LAN to DMZ | LAN to LAN | LAN to WAN (IPv6)

LAN to WAN Policy : ?

No.	Policy Name	Source	Destination	Services	Action	On/Off
1		Inside_Any	Outside_Any	ANY Wann	⊖	▶
2		Inside_Any	WannaCry-IP	ANY	⊖	▶
3		Inside_Any	WannaCry-Domain	ANY	▶	▶