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 Ransomeware?

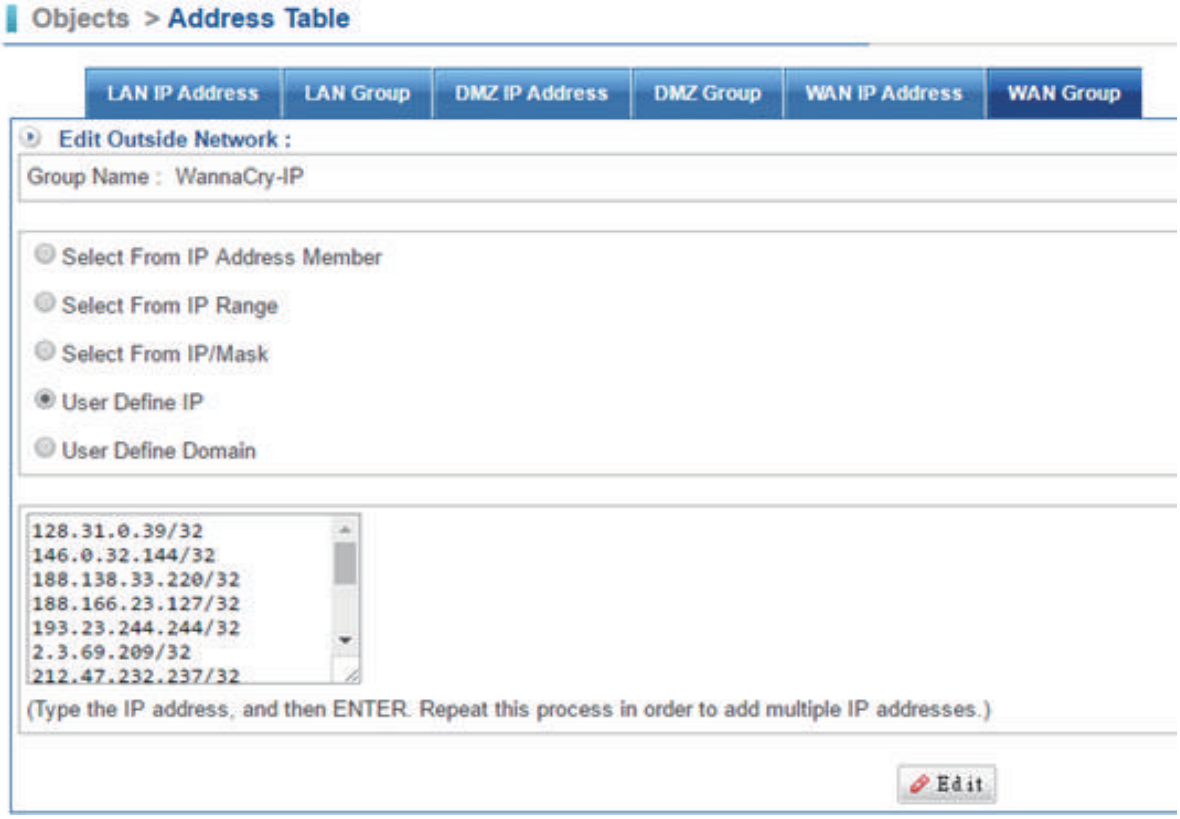
To shut down WanaCrypt0r 2.0 ransomeware, there are 3 steps administrators can follow: block IP, block port, allow domain and apply policies.

1. Block the following WannaCry ransomeware IP lists.

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
213.61.66.116/32
217.79.179.77/32
38.229.72.16/32
50.7.161.218/32
79.172.193.32/32
81.30.158.223/32
89.45.235.21/32

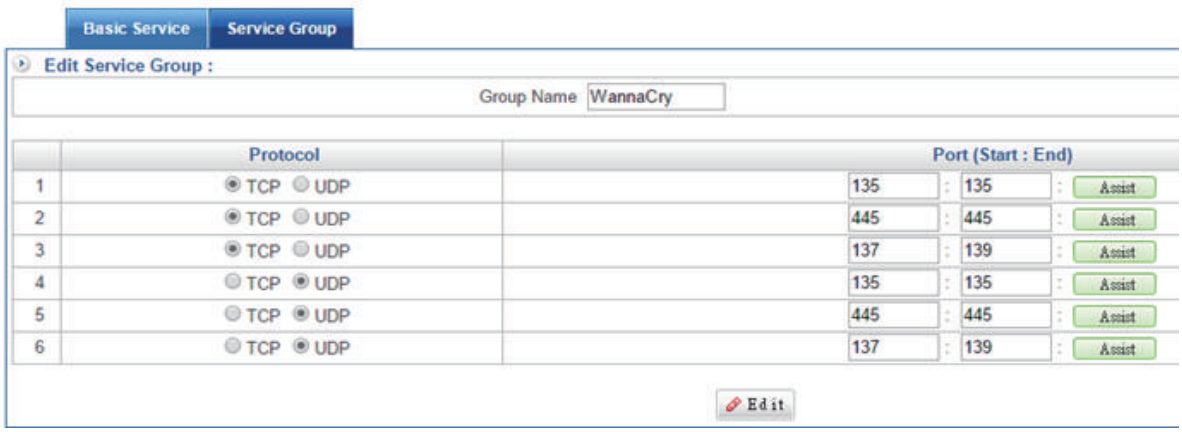
URL | www.sharetech.com.tw
Sales | sales@sharetech.com.tw
Support | help@sharetech.com.tw

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

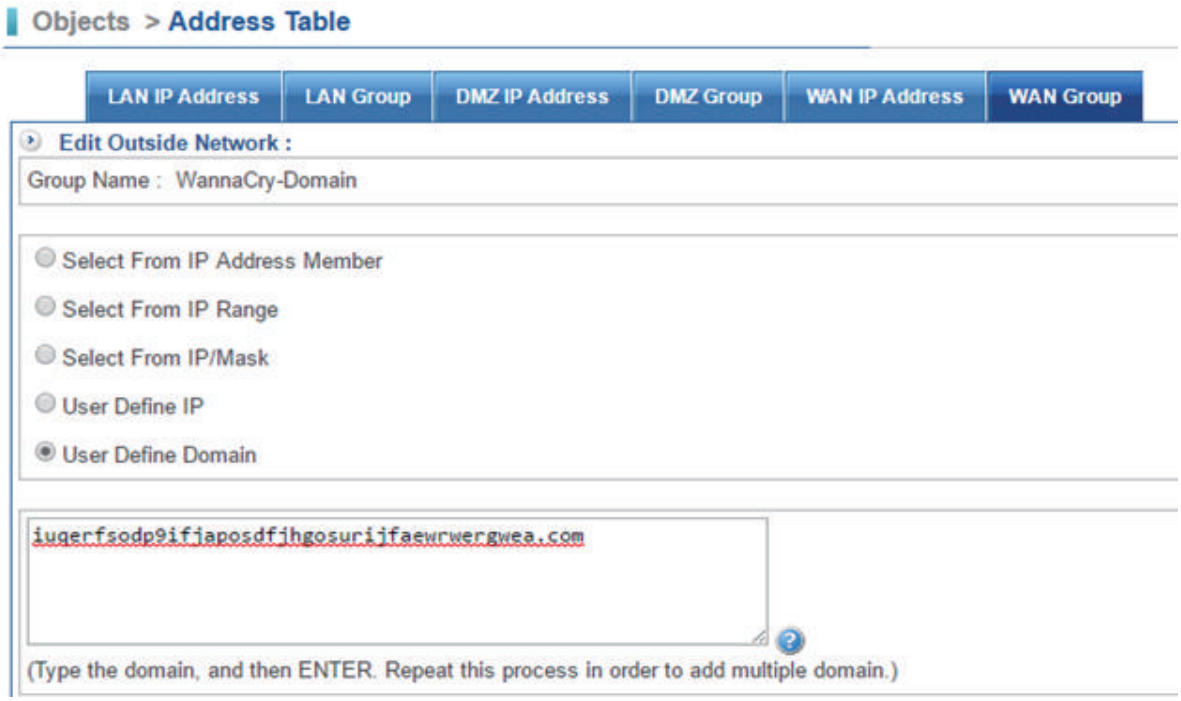


2. Block ports of WannaCry ransomeware

Go to **Objects > Services Table > Service Group > Add**



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.



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)

4-3. Add a policy.

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

Action: Drop

4-4. Add a policy.

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

Policies completed as follows.