How to identify WannaCry malicious code from Vietnam Computer Emergency Response Center (VNCERT)

VNCERT issued an urgent order to coordinate agencies and units nationwide to prevent connecting computers to WannaCry malware control servers.

WannaCry malicious code is becoming the most dangerous threat today to cyber security worldwide, including Vietnam. When the computer is infected with this malicious code, you will not be able to access the files and data on the computer and must pay a virtual bit of Bitcoins to redeem that data.

In the face of such a dangerous situation, the Vietnam Computer Emergency Response Center (VNCERT) has issued urgent orders to monitoring units and agencies, preventing computers from connecting to the code control server. poison WannaCry.

1. How to handle the emergency WannaCry malicious code from the National Information Security Department
2. How to remove / fix ransomware WannaCry

Accordingly, each agency or unit should prevent connection to WannaCry malware control servers and update IDS / IPS and Firewall protection systems . information to identify malicious code WannaCry blackmail. To identify this extremely dangerous new malicious code, we can pass 33 IP addresses of WannaCry malware control servers (C&C Server), 10 WannaCry malicious files and 22 hash codes (Hash SHA- 256).

1. List of WannaCry malware control servers (C&C Server)

STT	Địa chỉ IP C&C	STT	Địa chỉ IP C&C
1	128.31.0.39	18	213.239.216.222
2	136.243.176.148	19	213.61.66.116
3	146.0.32.144	20	38.229.72.16
4	163.172.153.12	21	50.7.151.47
5	163.172.185.132	22	50.7.161.218
6	163.172.25.118	23	51.255.41.65
7	171.25.193.9	24	62.138.10.60
8	178.254.44.135	25	62.138.7.231
9	178.254.44.135	26	79.172.193.32
10	178.62.173.203	27	81.30.158.223
11	185.97.32.18	28	82.94.251.227
12	188.138.33.220	29	83.162.202.182
13	188.166.23.127	30	83.169.6.12
14	192.42.115.102	31	86.59.21.38
15	193.23.244.244	32	89.45.235.21
16	198.199.64.217	33	94.23.173.93
17	212.47.232.237		

2. List of WannaCry malicious files

STT	File name	STT	File Name
1	@WanaDecryptor@.exe	6	taskse.exe
2	b.wnry	7	t.wnry
3	c.wnry	8	u.wnry
4	s.wnry	9	Các file với phần mở rộng ".wnry"
5	taskdl.exe	10	Các file với phần mở rộng ".WNCRY"

3. List of hash codes (Hash SHA-256)

STT	SHA-256
1	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
2	c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
3	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
4	0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
5	428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
6	5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
7	62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
8	72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
9	85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
10	a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
11	a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
12	b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
13	eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
14	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
15	2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
16	7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
17	a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
18	fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
19	9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
20	b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
21	4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
22	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa

One of the recommendations from VNCERT is that agencies need to quickly update official warnings on Microsoft websites for operating systems including Windows Server 2003 SP2 x64, Windows Server 2003 SP2 x86 , Windows XP SP2 x64, Windows XP SP3 x86, Windows XP Embedded SP3 x86, Windows 8 x86, Windows 8 x64.

1. Microsoft released an emergency patch to prevent ransomware from attacking
2. Downloading Windows patches for all versions to avoid being hit by a massive cyber attack, has affected 150 countries and is still spreading