Discovering a large-scale APT attack into Vietnam, users need to quickly download the malicious tool

The Department of Information Security recommends that users urgently download this malicious code-checking and removal tool on ais.gov.vn; vncert.vn was built and provided by the Department.

Recently, the Department of Information Security has discovered a large-scale targeted attack (APT) campaign taking place in Vietnam's cyberspace. The host of this attack is located outside of Vietnam. The objective of this APT attack campaign is to spread malicious code into the information systems of Government agencies and to the national important national information infrastructure system of our country.

This morning (October 30, 2019), the Department of Information Security issued an order to coordinate and rescue incidents to specialized IT units, agencies, organizations, enterprises, etc. removed malicious files of the targeted attack (APT) campaign.

According to the Department of Information Security, this targeted attack campaign (APT) has now infected more than 400,000 IP addresses in Vietnam.

The agency also recommends that users urgently download this malicious code-checking and removal tool built and provided by the Department according to the link below.

```
http://remove-apt.vnpt.vn/download/tools/incident-response-v1.0.exe
```

For agencies, organizations, businesses and the Information Security Department, it is recommended that measures should be urgently implemented to monitor and monitor connections to malicious server control according to the list provided by the Information Security Department. summarize in the table below and instruct users, customers to download scanning tools, remove malicious code of APT campaign on ais.gov.vn, vncert.vn.

STT	C&C	STT	C&C
1	adobephotostage.com	28	207.148.12.47
2	olk4.com	29	149.28.74.41
3	apple-net.com	30	207.148.78.101
4	wbemsystem.com	31	149.28.74.149
5	yahoorealtors.com	32	50.63.202.59
6	airdndvn.com	33	198.54.117.200
7	officeproduces.com	34	198.54.117.199
8	web.adobephotostage.com	35	198.54.117.197
9	Web.officeproduces.com	36	198.54.117.198
10	Up.officeproduces.com	37	162.255.119.150
11	We.officeproduces.com	38	167.88.180.148
12	Download.officeproduces.com	39	167.88.177.224
13	geocities.jp	40	167.88.180.3
14	update.olk4.com	41	45.248.87.14
15	www.cab-sec.com	42	91.195.240.117
16	167.88.178.24	43	103.224.182.250
17	43.254.217.67	44	167.88.177.224
18	154.221.24.47	45	167.88.178.24
19	144.202.54.86	46	185.239.226.19
20	50.63.202.94	47	185.239.226.19
21	50.63.202.67	48	45.77.209.52
22	50.63.202.82	49	167.88.178.118
23	184.168.221.94	50	185.239.226.61
24	184.168.221.82	51	45.77.184.12
25	184.168.221.71	52	167.88.178.118
26	50.63.202.73	53	185.239.226.61
27	45.32.50.150	54	45.77.184.12

List of domain / IP server control malicious code provided by the Department of Information Security.

STT	Mã băm – MD5
1	165F8683681A4B136BE1F9D6EA7F00CE
2	9FF1D3AF1F39A37C0DC4CEEB18CC37DC
3	4FE276EDC21EC5F2540C2BABD81C8653
4	43067F28DC5208D4A070CF3CC92E29FB
5	11ADDA734FC67B9CFDF61396DE984559
6	08F25A641E8361495A415C763FBB9B71
7	01D74E6D9F77D5202E7218FA524226C4
8	6198D625ADA7389AAC276731CDEBB500
9	9B39E1F72CF4ACFFD45F45F08483ABF0
10	748DE2B2AA1FA23FA5996F287437AF1B
11	5F094CB3B92524FCED2731C57D305E78
12	9A180107EFB15A00E64DB3CE6394328D
13	05CF906B750EB335125695DA42F4EAFC
14	F62DFC4999D624D01E94B89946EC1036
15	CA775717D000888A7F71A5907B9C9208
16	AA115F20472E78A068C1BBF739C443BF
17	CE78EA4ED30DBDF6BEA66561636298F0
18	684EE90242C8552561EE58EE66016640
19	B9C10D6E459061CA6304BCCD7C94A471

List of hash codes of APT attack campaigns. (Source: Department of Information Security)

The malicious code used by the hacker group during the large-scale APT attack was emphasized as particularly dangerous with more than 16 variants, so the Department of Information Security requested units to send a love report. infection and treatment results (if any) to the Department before November 5, 2019.

This malware is mainly spread by deceiving users into clicking the word (.doc) file attached to an email. The purpose of hackers is to steal information, mobilize infected computers into a computer network to attack DDoS on large systems, perform escalating attacks on critical information systems. .

According to experts' recommendations, to prevent the spread of malicious malware on purpose of APT's attacks, users should pay attention to:

1. Be careful when opening emails, especially 'strange' emails.
2. When suspecting mail has malware installed, never open the attachment.
3. It is necessary to quickly download and run APT's anti-malware scanning and removal tool at the website of the Information Security Department at ais.gov.vn.

New malware using web application has turned into a source of attack, very difficult to detect

Chinese hackers use fingerprints on glass to crack smartphones