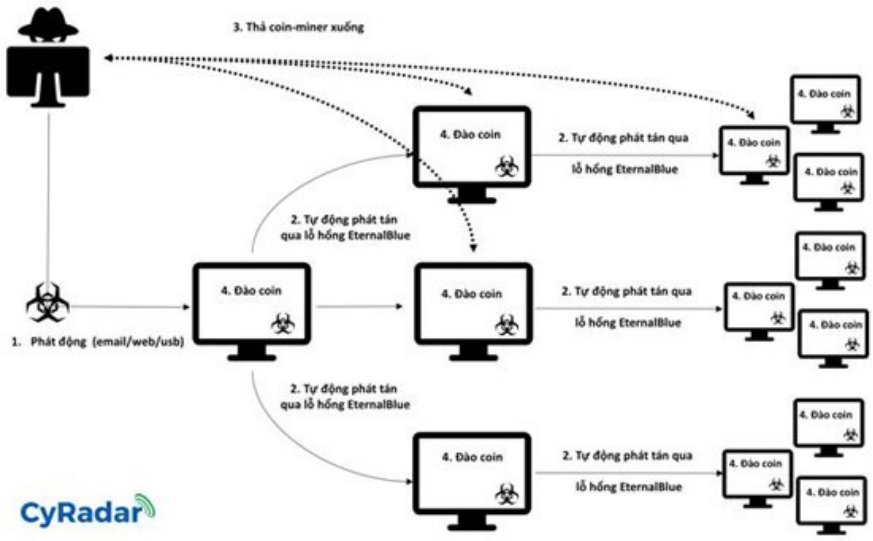
Warning: A new code of virtual money training is spreading strongly in Vietnam

In just a few hours, hundreds of businesses' computers were infected with malicious code.

From mid-January 2018 up to now, the monitoring system CyRadar - a startup created and developed by FPT has discovered SMB protocol packets continuously sent back and forth between computers in the network of many businesses. , organization. In just a few hours, hundreds of businesses' computers were infected with malicious code.

CyRadar experts said that SMB packets sent internally between the main computers exploiting Windows' MS17-010 vulnerability, also known as EternalBlue, were developed by the National Security Agency (National Security Agency). revealed in 4/2017.



How to spread the malicious code.

When a computer on the network is infected, the malicious code will automatically scan for IPs in the same local area network (LAN). Later, it will use the EternalBlue exploit code to spread through port 445 of computers that exist vulnerabilities. If infected new machines connect to another network, the spread continues and extends.

This new malware not only has the ability to maintain connectivity to the control server, is ready to receive commands, download files, as a normal backdoor, but also can perform virtual money digging for hackers. The money that it exploits is Monero.

```
memset(&FileName, 0, 0x104ui64);
sub_180001C00((__int64)&FileName, (__int64)"%s\\%s", (__int64)&Buffer, (__int64)"SecUpdateHost.exe");
v7 = CreateFileA(&FileName, 0x80000000, 1u, 0i64, 3u, 0, 0i64);
if ( v7 == (HANDLE)-1i64 )
{
  sub_180003800(&Dst, "hash64", &Buffer);
  sub_180003740(&Buffer, &Buffer, "hash64", "SecUpdateHost.exe");
}
else
{
  CloseHandle(v7);
}
memset(&CommandLine, 0, 0x800ui64);
sub_180001C00((__int64)&CommandLine, (__int64)&v16, v9, v10);
v4 = CreateProcess_fn_1(&FileName, &CommandLine);
Sleep(0x12Cu);
```

SecUpdateHost.exe file is actually a 'coin miner'.
CyRadar detected the parameter passed to the miner file at runtime:

```
-o p3.qsd2xjpzfky.site:45560 -u wvsymvtjeg@protonmail.com -p x -t 1 --donate-level=1 --nicehash
```

CyRadar experts conducted virus analysis, the results show that the domain name used for this malicious code is:

1. ccc.njaavfxcgk3.club, registered on November 17, 2017, and started pointing to a server (IP 45.32.127.108) from 08/01/2018.
2. "phimhayhdviet1.us" and "phimhayhdviet2.us", registered at the end of 2017, and pointed to server 45.32.127.108 at the beginning of 2018.

When checking on this server, experts discovered port 36215 for this version of the virus to download the file that was closed, but there are some other 'strange' ports open (48882, 48883):

```
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 0a:93:d4:de:a3:34:da:26:01:2c:30:5c:87:5c:76:dc (RSA)
|   256 7d:47:65:09:d1:9d:7b:da:30:1d:69:cd:ef:c1:87:05 (ECDSA)
|_  256 a9:4f:b3:60:b3:fd:4b:89:09:4c:6d:c3:3c:f2:c3:f3 (EdDSA)
517/tcp   filtered talk
48882/tcp open     unknown
48883/tcp open     unknown
| fingerprint-strings:
|   GenericLines, HTTPOptions:
|     HTTP/1.1 403 Forbidden
|     Date: Wed, 07 Feb 2018 16:24:01 +0000
|     Connection: close
|     Content-Length: 9
|     Content-Type: text/plain
|     Server: crave-json-rpc/v2.5.0.1-8ebe25c-dirty
|     Forbidden
|   Kerberos:
|     HTTP/1.1 403 Forbidden
|     Date: Wed, 07 Feb 2018 16:24:05 +0000
|     Connection: close
|     Content-Length: 9
|     Content-Type: text/plain
|     Server: crave-json-rpc/v2.5.0.1-8ebe25c-dirty
|     Forbidden
|   NULL:
|     HTTP/1.1 403 Forbidden
|     Date: Wed, 07 Feb 2018 16:24:00 +0000
|     Connection: close
|     Content-Length: 9
|     Content-Type: text/plain
|     Server: crave-json-rpc/v2.5.0.1-8ebe25c-dirty
|     Forbidden
|   SIPOptions:
|     HTTP/1.1 403 Forbidden
|     Date: Wed, 07 Feb 2018 16:24:08 +0000
|     Connection: close
|     Content-Length: 9
|     Content-Type: text/plain
|     Server: crave-json-rpc/v2.5.0.1-8ebe25c-dirty
|     Forbidden
|   afp:
|     HTTP/1.1 403 Forbidden
|     Date: Wed, 07 Feb 2018 16:24:12 +0000
|     Connection: close
|     Content-Length: 9
|     Content-Type: text/plain
|     Server: crave-json-rpc/v2.5.0.1-8ebe25c-dirty
|_    Forbidden
1 service unrecognized despite returning data. If you know the service/version, please submit
```

Although these domains are like a website, the server it points to does not open any regular ports for the website (80 and 443). Therefore, CyRadar believes that all three domain names are created by one person or group of Vietnamese speakers. There is currently no malicious code that connects to "phimhayhdviet" domains, but it is likely that hackers will use it in another attack.

What do users need to do to protect themselves against malicious attacks?

1. Users need to regularly update the patches for the operating system and the software running on it.
2. Equipped with antivirus software of reputable firms.
3. Organizations and businesses need to equip the network monitoring system, can perform additional network isolation steps between the computers in the network together, to avoid the possibility of internal spread.

See more:

1. Campaign to distribute spyware aimed at macOS in Vietnam
2. New malware detection has terrible spy capabilities never seen on Android
3. Acronis Ransomware Protection, a completely free anti-ransomware solution for Windows