

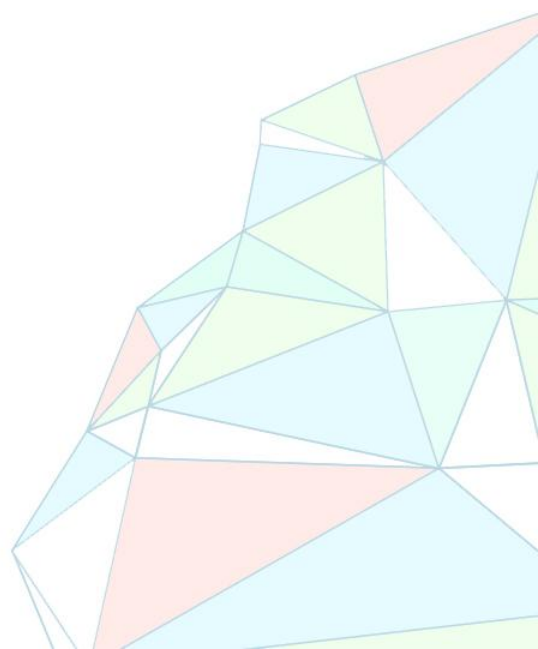
A 'WannaCry' Group Therapy Session

Juan Andres Guerrero-Saade (@juanandres_gs)

GReAT, Kaspersky Lab

Matt Suiche (@msuiche)

Comae Technologies





Agenda

What we know today

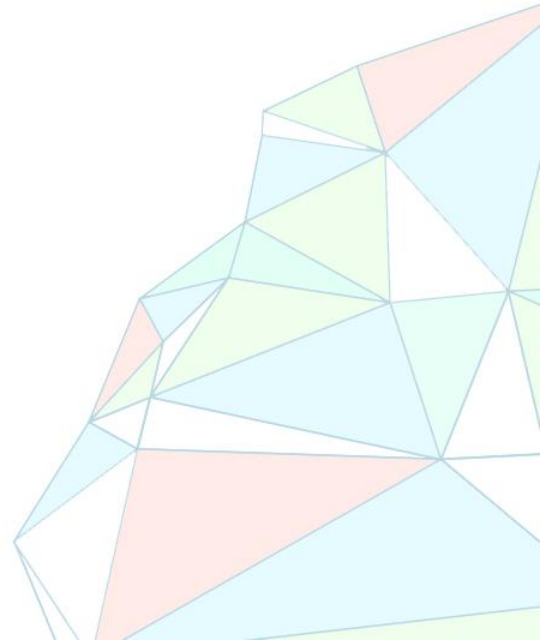
What exactly happened

Variants and Killswitches

A Lazarus connection?

Priorities & Mitigations

What's next?



Agenda

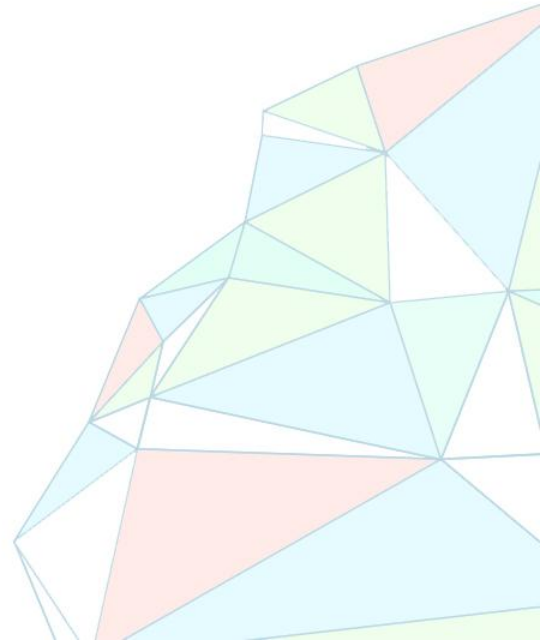
What happened?

Who is involved?

Where did it take place?

When did it take place?

Why did that happen?



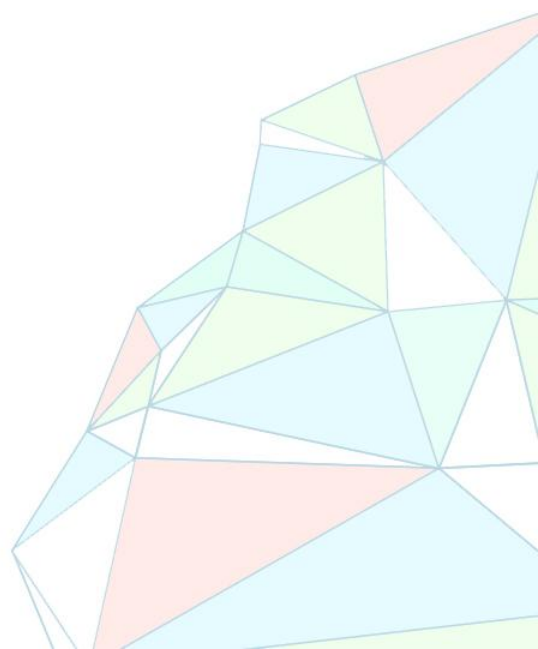
Largest Ransomware Infection In History

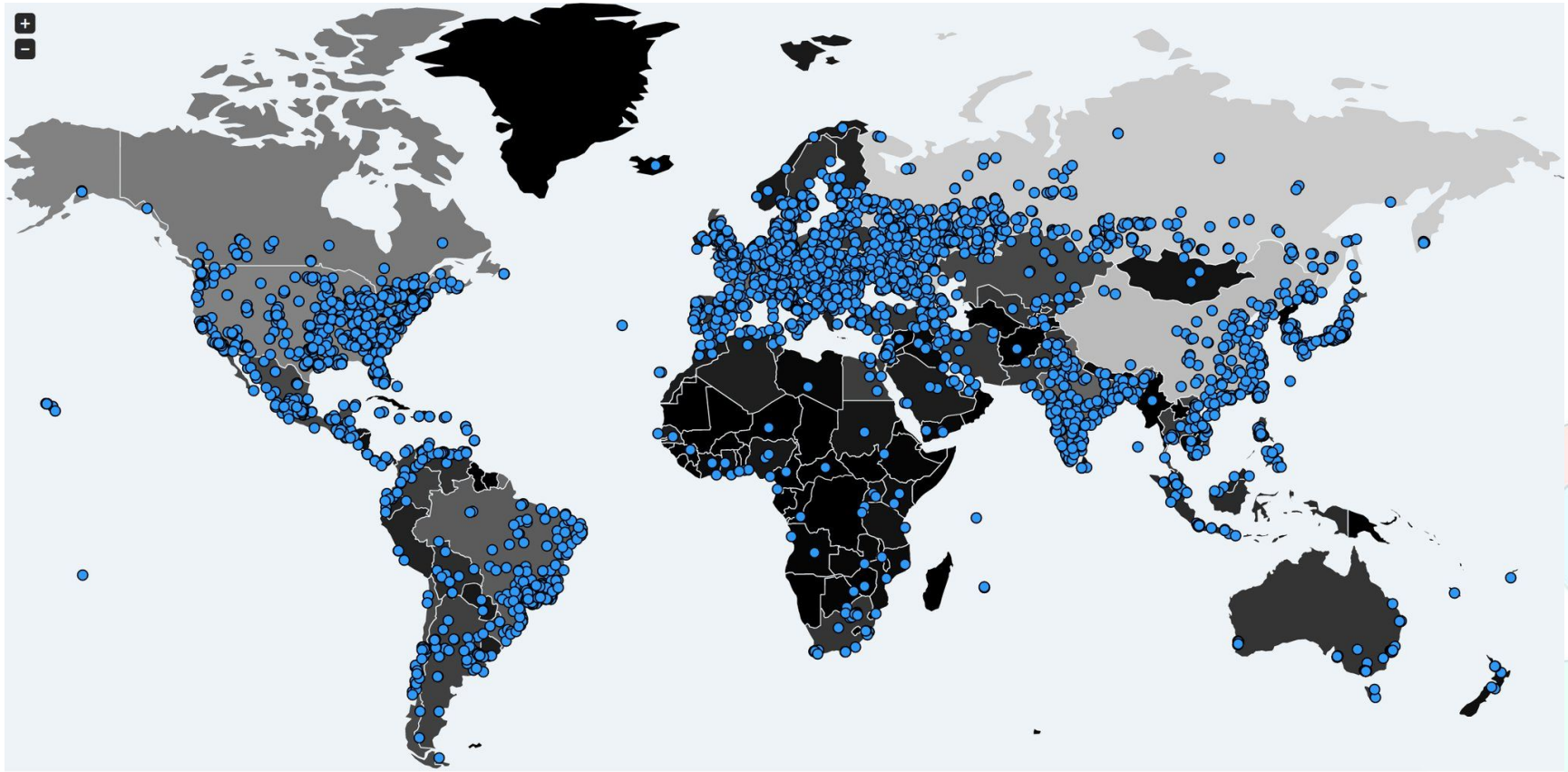
- **First** worming ransomware
- WannaCrypt incorporates leaked Equation exploit to self-spread
- Uptick of port 445 scanning starts on Thursday May 11th
- Sunday morning, variant with new killswitch appears on the scene
- Drastically decreased by Monday 15th (6x decrease)
- Killswitches **save** the day (...for now)



Variants & Kill-switches

1. iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com - *@MalwareTechBlog* - 12 May
a. <https://twitter.com/MalwareTechBlog/status/863187104716685312>
2. ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com - *@msuiche* - 14 May -
a. <https://twitter.com/msuiche/status/863730377642442752>
3. ayyлмаотјһsstasdfasdfasdfasdfasdfasdf.com
4. A no kill switch version hasn't been detected in the wild **yet**.





MalwareTech WannaCry Live Map

KASPERSKY
lab



The first 6 hours...

7000+ machines

- during the 1st hour **only**

10,000

This is the number of machines stopped from:

- infected further machines.
- having their data destroyed.

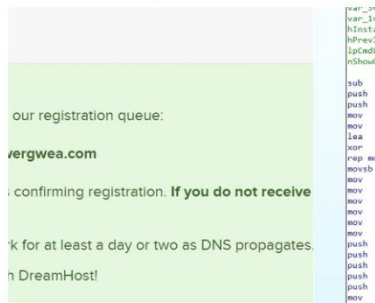


Matthieu Suiche
@msuiche

New kill switch detected ! ...

dp9ifjaposdfjhgosurijfaewrwergwea.com

#WannaCry - Just pushed for an order !



RETWEETS
544

LIKES
553

5:19 AM - 14 May 2017



53



544



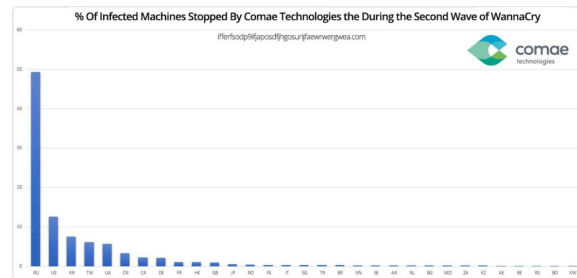
553



Matthieu Suiche
@msuiche

Following

Since registering the 2nd killswitch yesterday, we stopped ~10K machines from spreading further - mainly from Russia. #WannaCry #OKLM



RETWEETS
146

LIKES
180

10:39 AM - 15 May 2017

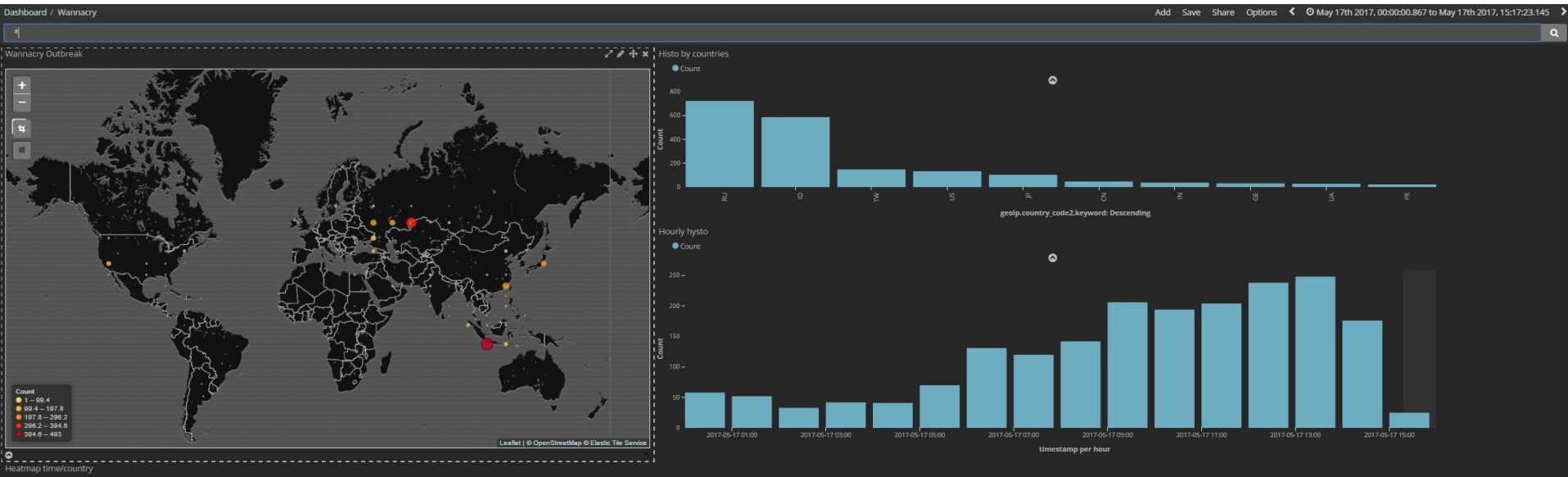
KASPERSKY



comae
technologies

Kill-switch #2 today (17 May 2017)

First half of today. Stabilizing below 300 hits per hour.





Benkow moxueg @benkow_ · 13h

#WannaCry New killswitch (already registered) again. SEEN IN THE WILD!
virustotal.com/fr/file/b9318a...

```
Frame 239437: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0
Ethernet II, Src: Microsof_32:4f:5c (98:5f:d3:32:4f:5c), Dst: Sagemcom_8d:a7:cc (24:7f:20:8d:a7:cc)
Internet Protocol Version 4, Src: 192.168.0.23, Dst: 207.154.243.152
Transmission Control Protocol, Src Port: 49252, Dst Port: 80, Seq: 1, Ack: 1, Len: 100
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Host: www.ayylmaoTJHSSasdfasdfasdfasdfasdfasdf.com\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://www.ayylmaoTJHSSasdfasdfasdfasdfasdfasdf.com/]
    [HTTP request 1/1]
    [Response in frame: 239442]
```



14



81



82

Victim Stats

- MalwareTech + Comae Sinkhole – **378,075** (*prevented*)
- KSN: 74 Countries affected
- Propagation is **exponential**
 - **The more infected machines, the faster the malware multiplies.**





Neel Mehta

@neelmehta

Following



9c7c7149387a1c79679a87dd1ba755bc @
0x402560, 0x40F598
ac21c8ad899727137c4b94458d7aa8d8 @
0x10004ba0, 0x10012AA4
[#WannaCryptAttribution](#)



comae
technologies

The Lazarus Connection

The Geography of financial attacks by Lazarus group

The malware by Lazarus group, infamous for its theft of \$81 million from Central Bank of Bangladesh, has been active since at least 2009. It has been spotted in the last couple of years in at least 18 countries.



View: 766d7d59

766d7d591b9ec1204518723a1e5940fd6ac777f606ed64e731fd91b0b4c3

.10004BA0: 51	push	ecx
.10004BA1: 53	push	ebx
.10004BA2: 55	push	ebp
.10004BA3: 8B6C2410	mov	ebp,[esp]
.10004BA7: 56	push	esi
.10004BA8: 57	push	edi
.10004BA9: 6A20	push	020 ;'
.10004BAB: 8B4500	mov	eax,[ebp]
.10004BAE: 8D7504	lea	esi,[ebp]
.10004BB1: 2401	and	al,1
.10004BB3: 0C01	or	al,1
.10004BB5: 46	inc	esi
.10004BB6: 894500	mov	[ebp][0],
.10004BB9: C646FF03	mov	b,[esi][-
.10004BBD: C60601	mov	b,[esi],1
.10004BC0: 46	inc	esi
.10004BC1: 56	push	esi
.10004BC2: E8E9CAFFFF	call	.0100016B0
.10004BC7: 83C408	add	esp,8
.10004BCA: 6A04	push	4
.10004BCC: 6A00	push	0
.10004BCE: FF1554E00010	call	time
.10004BD4: 83C404	add	esp,4
.10004BD7: 99	cdq	
.10004BD8: 52	push	edx
.10004BD9: 50	push	eax
.10004BDA: E8E1000000	call	.010004CC0
.10004BDF: 8906	mov	[esi],eax
.10004BE1: 83C620	add	esi,020 ;
.10004BE4: 83C40C	add	esp,00C
.10004BE7: C60600	mov	b,[esi],0
.10004BEA: 46	inc	esi
.10004BEB: FF155CE00010	call	rand
.10004BF1: 99	cdq	
.10004BF2: B905000000	mov	ecx,5
.10004BF7: 33FF	xor	edi,edi
.10004BF9: F7F9	idiv	ecx
.10004BF8: 8D4602	lea	eax,[esi
.10004BFE: 83C202	add	edx,2

1Global 2FileBlk 3CryBlk 4ReLoad 5Ordldr 6String 7Direct 8Table

View: 3e6de9e2baacf930949647c399818e7a2caea2626df6a468407854aaa515eed9

2e6de9e2baacf930949647c399818e7a2caea2626df6a468407854aaa515eed9

.00402560: 51	push	ecx
.00402561: 53	push	ebx
.00402562: 55	push	ebp
.00402563: 8B6C2410	mov	ebp,[esp][010]
.00402567: 56	push	esi
.00402568: 57	push	edi
.00402569: 6A20	push	020 ;'
.0040256B: 8B4500	mov	eax,[ebp][0]
.0040256E: 8D7504	lea	esi,[ebp][4]
.00402571: 2401	and	al,1
.00402573: 0C01	or	al,1
.00402575: 46	inc	esi
.00402576: 894500	mov	[ebp][0],eax
.00402579: C646FF03	mov	b,[esi][-,1],3
.0040257D: C60601	mov	b,[esi],1
.00402580: 46	inc	esi
.00402581: 56	push	esi
.00402582: E8A95B0000	call	.000408130 --1
.00402587: 6A00	push	0
.00402589: FF1560F44000	call	time
.0040258F: 83C40C	add	esp,00C
.00402592: 50	push	eax
.00402593: FF1524F54000	call	WS2_32.8
.00402599: 8906	mov	[esi],eax
.0040259B: 83C620	add	esi,020 ;'
.0040259E: C60600	mov	b,[esi],0
.004025A1: 46	inc	esi
.004025A2: FF1564F44000	call	rand
.004025A8: 99	cdq	
.004025A9: B905000000	mov	ecx,5
.004025AE: 33FF	xor	edi,edi
.004025B0: F7F9	idiv	ecx
.004025B2: 8D4602	lea	eax,[esi][2]
.004025B5: 83C202	add	edx,2
.004025B8: 8D1C52	lea	ebx,[edx][edx]*2
.004025BB: D1E3	shl	ebx,1
.004025BD: 85DB	test	ebx,ebx
.004025BF: 7E72	jle	.000402633 --12
.004025C1: 89442418	mov	[esp][018],eax

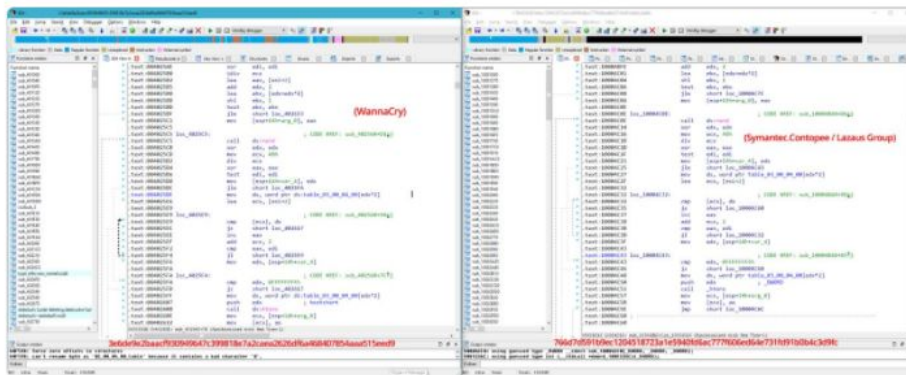
1Help 2PutBlk 3Edit 4Mode 5Goto 6Refer 7Search 8Header 9Files 10Quit 11Mem 12Names



Matthieu Suiche ✓

@msuiche

Similitude between #WannaCry and Contopee from Lazarus Group ! thx @neelmehta - Is DPRK behind #WannaCry ?



RETWEETS

522

LIKES

425



11:04 AM - 15 May 2017



35



522



425



KASPERSKY Lab



comae
technologies


```

overlapFunction1 proc near
var_4= dword ptr -4
arg_0= dword ptr 4

push    ecx
push    ebx
push    ebp
mov     ebp, [esp+0Ch+arg_0]
push    esi
push    edi
push    20h
mov     eax, [ebp+0]
lea     esi, [ebp+4]
and     al, 1
or      al, 1
inc     esi
mov     [ebp+0], eax
mov     byte ptr [esi-1], 3
mov     byte ptr [esi], 1
inc     esi
push    esi
call    sub_401A20
push    0 ; Time
call    ds:time
add     esp, 0Ch
push    eax ; hostlong
call    ds:htonl
mov     [esi], eax
add     esi, 20h
mov     byte ptr [esi], 0
inc     esi
call    ds:rand
cdq
mov     ecx, 5
xor     edi, edi
idiv    ecx
lea     eax, [esi+2]
add     edx, 2
lea     ebx, [edx+edx*2]
shl     ebx, 1
test    ebx, ebx
jle     short loc_402633

```

```

mov     [esp+14h+arg_0], eax

```

```

loc_4025C5:
call    ds:rand
xor     edx, edx

```

```

OverlapFN_1 proc near
var_4= dword ptr -4
arg_0= dword ptr 4

push    ecx
push    ebx
push    ebp
mov     ebp, [esp+0Ch+arg_0]
push    esi
push    edi
push    20h
mov     eax, [ebp+0]
lea     esi, [ebp+4]
and     al, 1
or      al, 1
inc     esi
mov     [ebp+0], eax
mov     byte ptr [esi-1], 3
mov     byte ptr [esi], 1
inc     esi
push    esi
call    sub_401A20
add     esp, 8
push    4 ; Time
push    0
call    ds:time
add     esp, 4
cdq
push    edx
push    eax
call    sub_4019E0
mov     [esi], eax
add     esi, 20h
add     esp, 0Ch
mov     byte ptr [esi], 0
inc     esi
call    ds:rand
cdq
mov     ecx, 5
xor     edi, edi
idiv    ecx
lea     eax, [esi+2]
add     edx, 2
lea     ebx, [edx+edx*2]
shl     ebx, 1
test    ebx, ebx
jle     short loc_40199C

```

```

mov     [esp+14h+arg_0], eax

```

Frequently Asked Questions

Does this require admin privileges ?

No, the infection is done via kernel exploitation which ensure total control of the machine to the attacker.

Can encrypted files be recovered ?

No viable solution to recover the encrypted files had been found yet. Private key is destroyed in memory very early.

Did Microsoft released patches for those vulnerabilities ?

Yes, [MS17-010](#) in March (Vista+), [KB4012598](#) on Friday 14 (< Vista)



WannaCry Crypto

.eky contains the user private/public key, encrypted by malware public key (embedded)

.pky is the user public key, used to encrypt AES keys (one AES key/file)

.dky should be the decrypted **.eky** sent back by the attackers once victim pays (on kiwi's screen: *fake_user_00000000.pky*)

.WNCRY, contains the AES key, encrypted by user public key, in the header, followed by the encrypted data

```
IDA View-A  Pseudocode-B  Pseudocode-A  Hex View-1  Structures
1 int __thiscall sub_10003AC0(void *this, LPCSTR lpFileName, LPCSTR a3)
2 {
3     void *v3; // esi@1
4     HCRYPTKEY v5; // esi@14
5
6     v3 = this;
7     if ( !acquireCryptContext(this) )
8     {
9         destroyAllKeys((int)v3);
10        return 0;
11    }
12    if ( lpFileName )
13    {
14        if ( !importPrivateKey((int)v3, lpFileName) )
15        {
16            if ( !CryptImportKey*((_DWORD *)v3 + 1), (const BYTE *)&RSA_Key_0, 0x114u, 0, 0, (HCRYPTKEY *)v3 + 3)
17            || !generatePrivateKey*((_DWORD *)v3 + 1), (HCRYPTKEY *)v3 + 2)
18            || !exportKeysMemoryAndFiles*((_DWORD *)v3 + 1), *((_DWORD *)v3 + 2), 6u, lpFileName )
19            {
20                goto LABEL_19;
21            }
22            if ( a3 )
23            {
24                exportKeyOnDisk((int)v3, a3);
25            }
26            if ( !importPrivateKey((int)v3, lpFileName) )
27            {
28                goto LABEL_19;
29            }
30        }
31        v5 = *((_DWORD *)v3 + 3);
32        if ( v5 )
33        {
34            CryptDestroyKey(v5);
35        }
36        else if ( !CryptImportKey*((_DWORD *)v3 + 1), (const BYTE *)&RSA_Key_Testing, 0x114u, 0, 0, (HCRYPTKEY *)v3 + 3)
37        {
38            destroyAllKeys((int)v3);
39            return 0;
40        }
41        return 1;
42    }
43    return 0;
44}
```

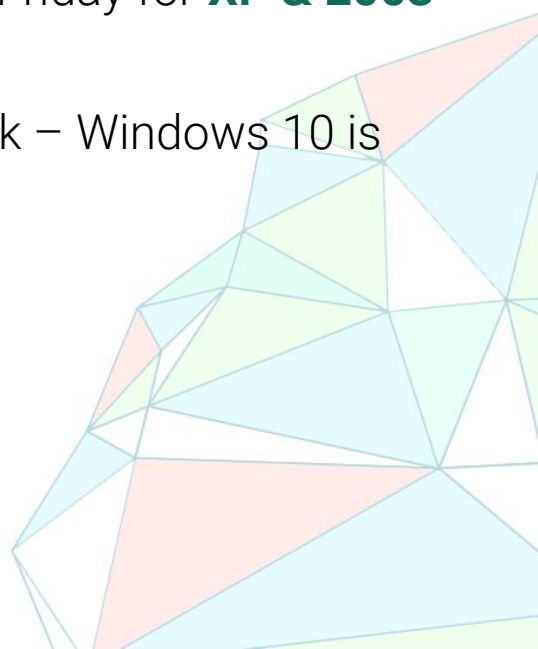
```
Invite de commandes
Microsoft Windows [version 10.0.15063]
(c) 2017 Microsoft Corporation. Tous droits réservés.

C:\Users\gentilkiwi>cd \security\wanadecrypt
C:\security\wanadecrypt>wanadecrypt fake_malware.pky fake_user_00000000.eky fake_Collines.jpg.WNCRY fake_alaviealamour.txt.WNCRY
Malware PK: fake_malware.pky
User EncPK: fake_user_00000000.eky
WARNING: user privatekey was encrypted with bad data at the end, fixed from 1225 to 1172
Save DecPK: fake_user_00000000.pky
Filename : fake_Collines.jpg.WNCRY
Mode(?) : 4
Filesize : 28521
Final file: fake_Collines.jpg
Filename : fake_alaviealamour.txt.WNCRY
Mode(?) : 4
Filesize : 607
Final file: fake_alaviealamour.txt
C:\security\wanadecrypt>
```



Priorities & Mitigations: Patch!

- **Patch, Patch, Patch!**
- Make sure **MS-17-010** is installed
- **KB4012598** - Emergency patch released by Microsoft on Friday for **XP & 2003**
- Users running Windows 10 were not targeted by the attack – Windows 10 is not vulnerable



Priorities & Mitigations: Offline Backups!

- Shadow Volumes can be deleted.
- Connected backups will be encrypted.
- Backups have to be kept disconnected
 - Insurance policy against both ransomware & wiper attacks
- **Test your backups before you need them**



Priorities & Mitigations: Block and Rollback!

- Network Level:
 - If possible, block incoming traffic to TCP Port 445
- Modern Anti-Malware Solution:
 - Strong Heuristics
- Free anti-ransom tool available for businesses
 - <https://go.kaspersky.com/Anti-ransomware-tool.html>
- Kaspersky Users:
 - **Make sure System Watcher is not disabled (on by default)**



WHAT'S NEXT?

TheShadowBrokers Monthly Data Dump could be being:

- web browser, router, handset exploits and tools
- select items from newer Ops Disks, including newer exploits for Windows 10
- compromised network data from more SWIFT providers and Central banks
- compromised network data from Russian, Chinese, Iranian, or North Korean nukes and missile programs

More details in June.



Additional resources

<https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/>

<https://securelist.com/blog/research/78431/wannacry-and-lazarus-group-the-missing-link/>

<https://blog.comae.io/the-nsa-compromised-swift-network-50ec3000b195>

<https://blog.comae.io/wannacry-the-largest-ransom-ware-infection-in-history-f37da8e30a58>

<https://blog.comae.io/wannacry-new-variants-detected-b8908fefa7e>

<https://blog.comae.io/wannacry-links-to-lazarus-group-dcea72c99d2d>

<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>

<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

<https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012>

<https://twitter.com/gentilkiwi/status/864648310371516416>

