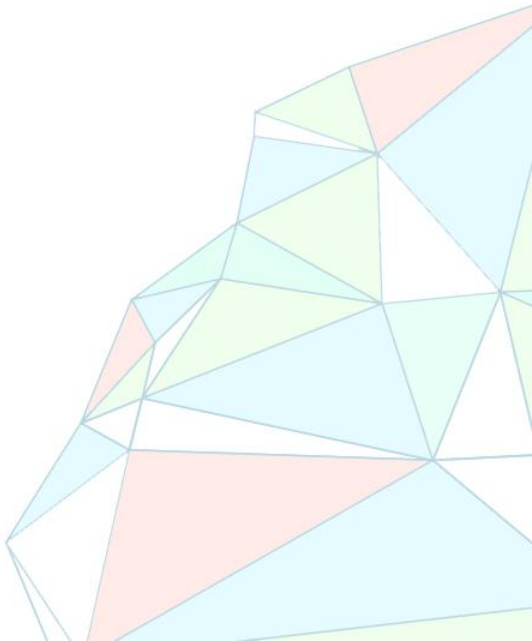
# A ‘WannaCry’ Group Therapy Session

**Juan Andres Guerrero-Saade** (@juanandres_gs)

*GReAT, Kaspersky Lab*

**Matt Suiche** (@msuiche)

*Comae Technologies*




KASPERSKY lab

comae technologies

# Agenda

What we know today

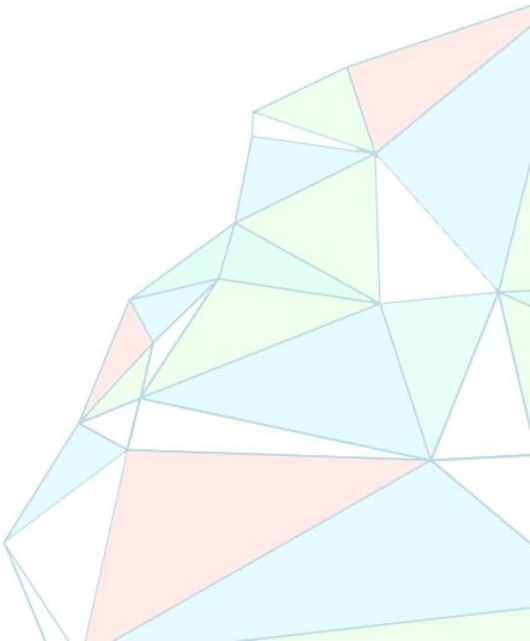
What exactly happened

Variants and Killswitches

A Lazarus connection?

Priorities & Mitigations

What’s next?



KASPERSKY lab

comae technologies

# Agenda

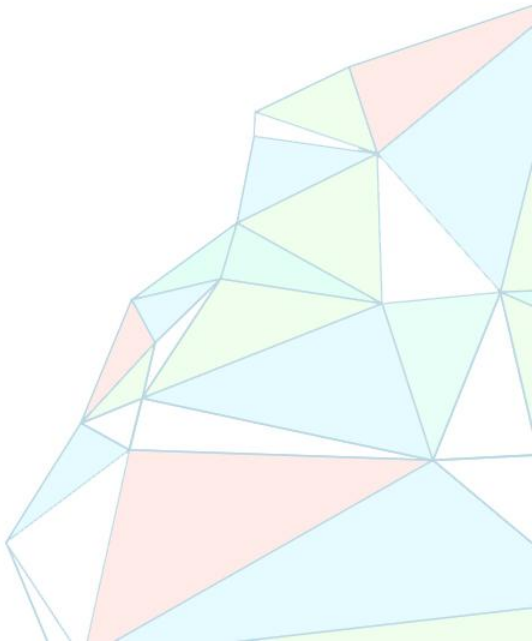
**What** happened?

**Who** is involved?

**Where** did it take place?

**When** did it take place?

**Why** did that happen?



KASPERSKY lab

comae technologies

# Largest Ransomware Infection In History

- **First** worming ransomware
- WannaCrypt incorporates leaked Equation exploit to self-spread
- Uptick of port 445 scanning stars 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)

KASPERSKY lab

comae technologies

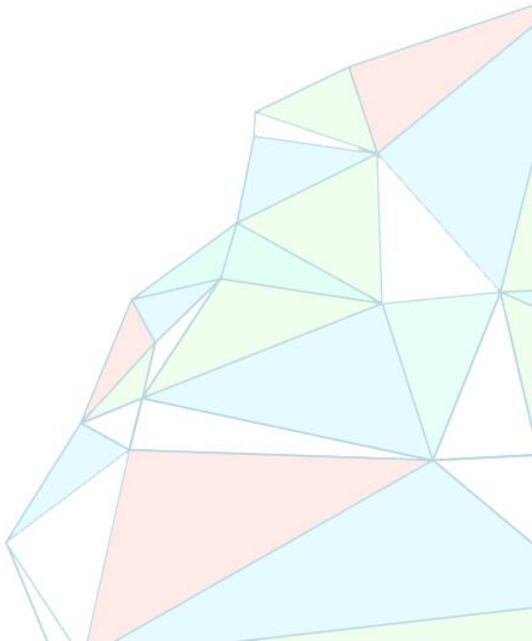
# Variants & Kill-switches

1. iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com - *@MalwareTechBlog* - 12 May
   a. *https://twitter.com/MalwareTechBlog/status/863187104716685312*

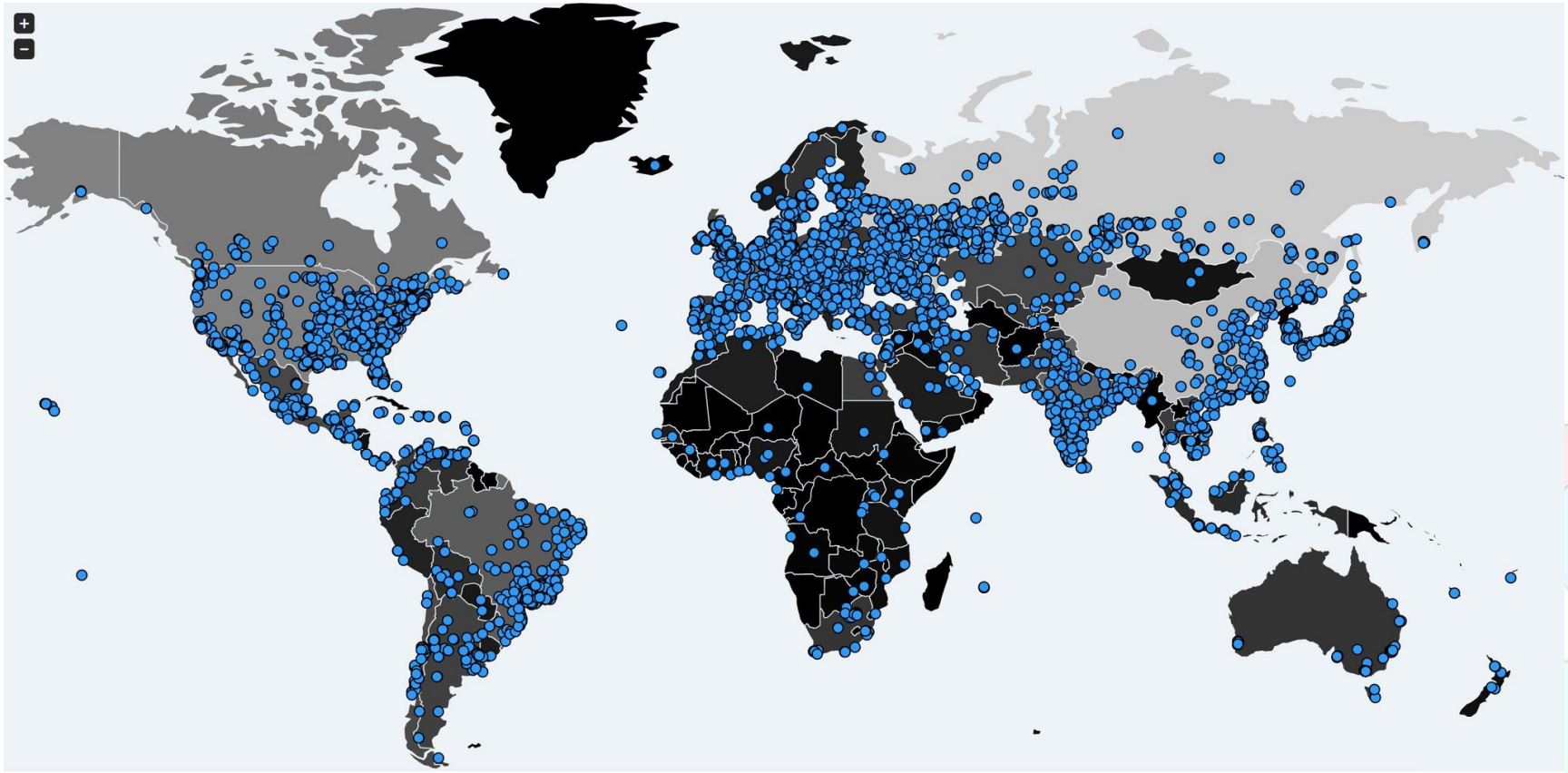
2. ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com - *@msuiche* - 14 May -
   a. *https://twitter.com/msuiche/status/863730377642442752*

3. ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com

4. A no kill switch version hasn't been detected in the wild **yet**.



KASPERSKY lab comae technologies



# MalwareTech WannaCry Live Map

KASPERSKY lab

comae technologies

# The first 6 hours...

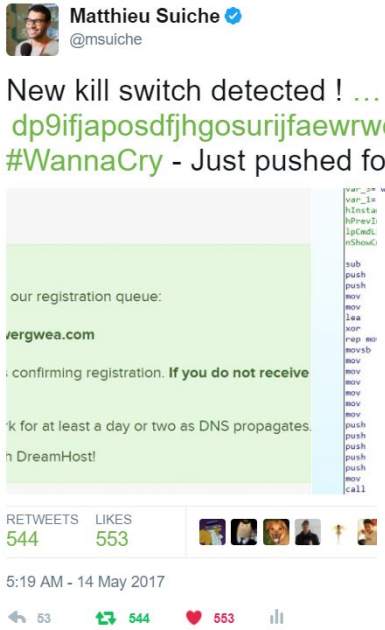
**7000+** machines

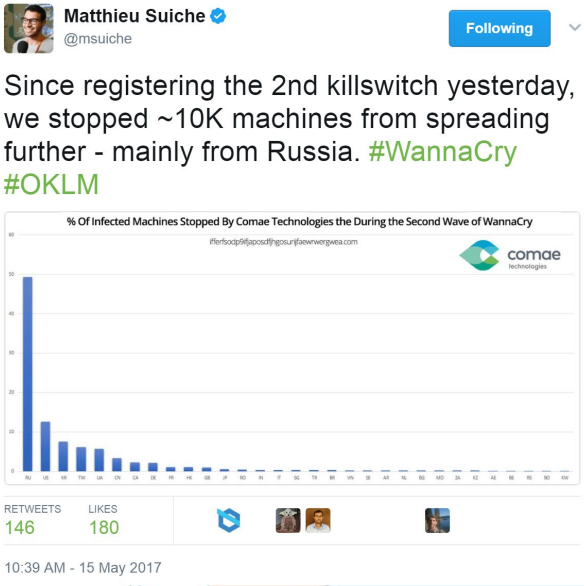
- during the 1st hour **only**

**10,000**

This is the number of machines stopped from:

- infected further machines.
- having their data destroyed.




KASPERSKY lab

comae technologies

# Kill-switch #2 today (17 May 2017)

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


KASPERSKY lab

comae technologies

**Benkow moɥuƎq** @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.ayylmaoTJHSSTasdfasdfasdfasdfasdfasdfasdf.com\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://www.ayylmaoTJHSSTasdfasdfasdfasdfasdfasdfasdf.com/]
    [HTTP request 1/1]
    [Response in frame: 239442]
```

14 81 82

KASPERSKY lab comae technologies

# Victim Stats

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

KASPERSKY lab

comae technologies

**Neel Mehta**
@neelmehta

Following

9c7c7149387a1c79679a87dd1ba755bc @ 0x402560, 0x40F598
ac21c8ad899727137c4b94458d7aa8d8 @ 0x10004ba0, 0x10012AA4
#WannaCryptAttribution

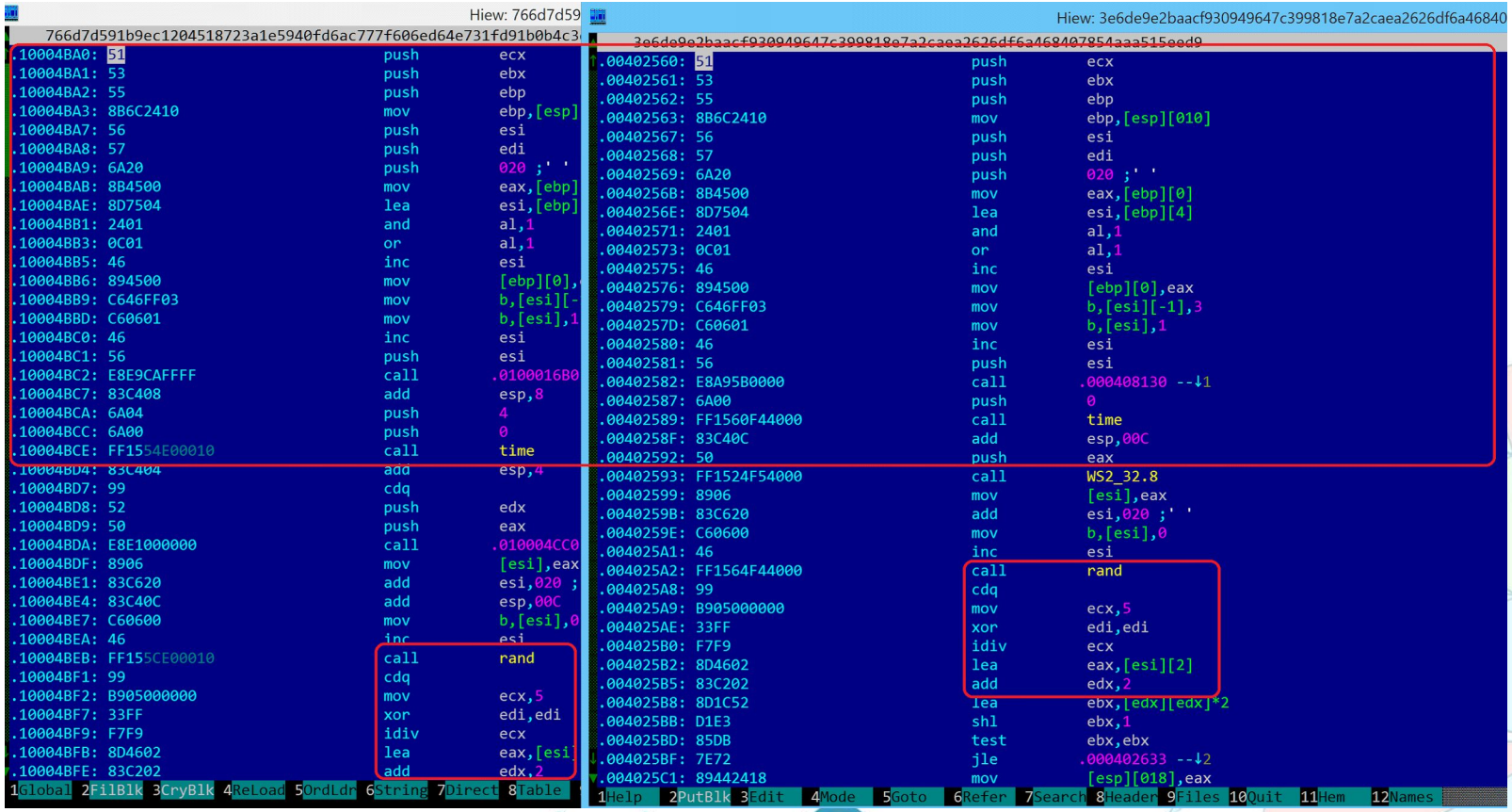
KASPERSKY lab

comae technologies

# The Lazarus Connection


KASPERSKY lab

comae technologies

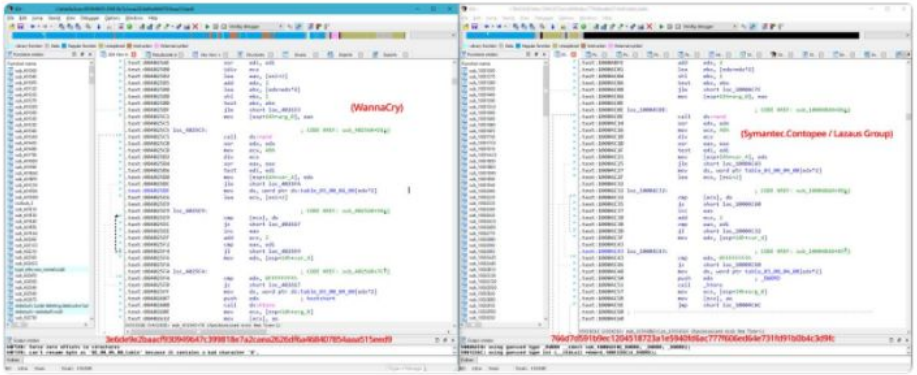



KASPERSKY lab

comae technologies

**Matthieu Suiche** 
@msuiche

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



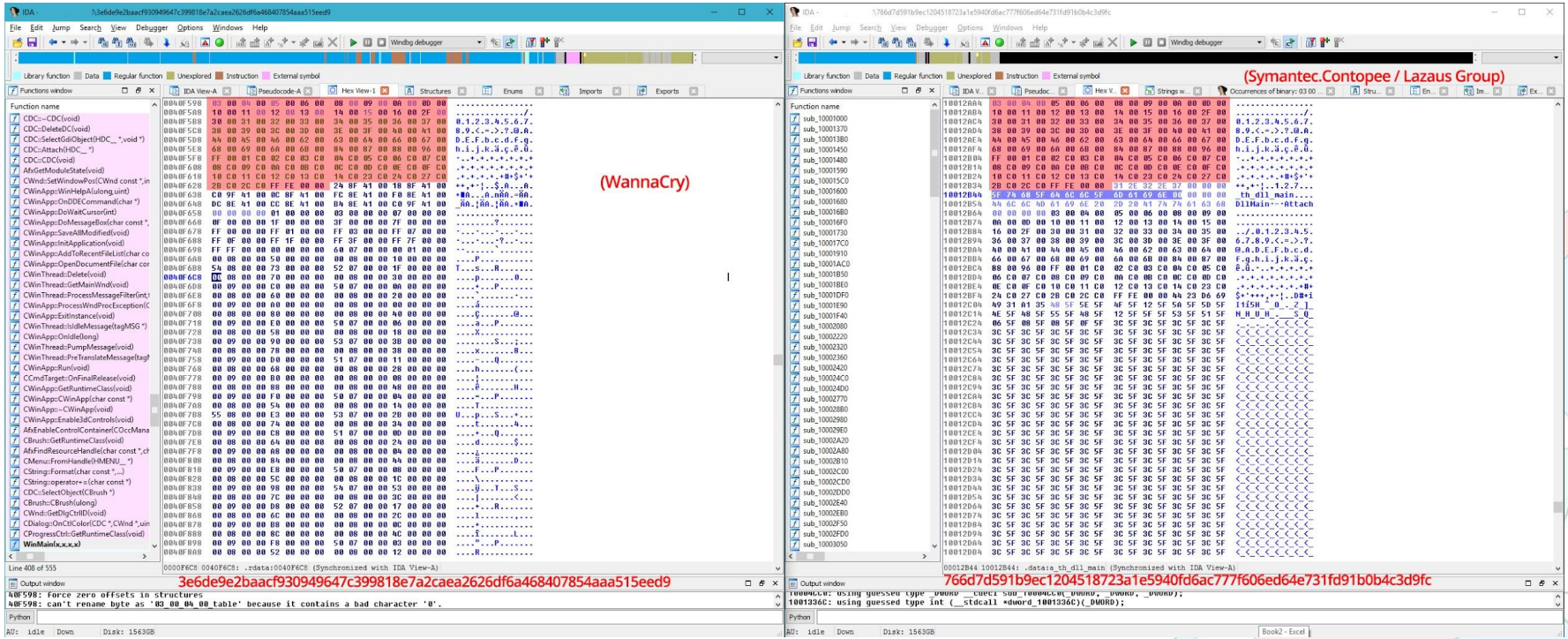

RETWEETS 522 LIKES 425

11:04 AM - 15 May 2017

35 522 425

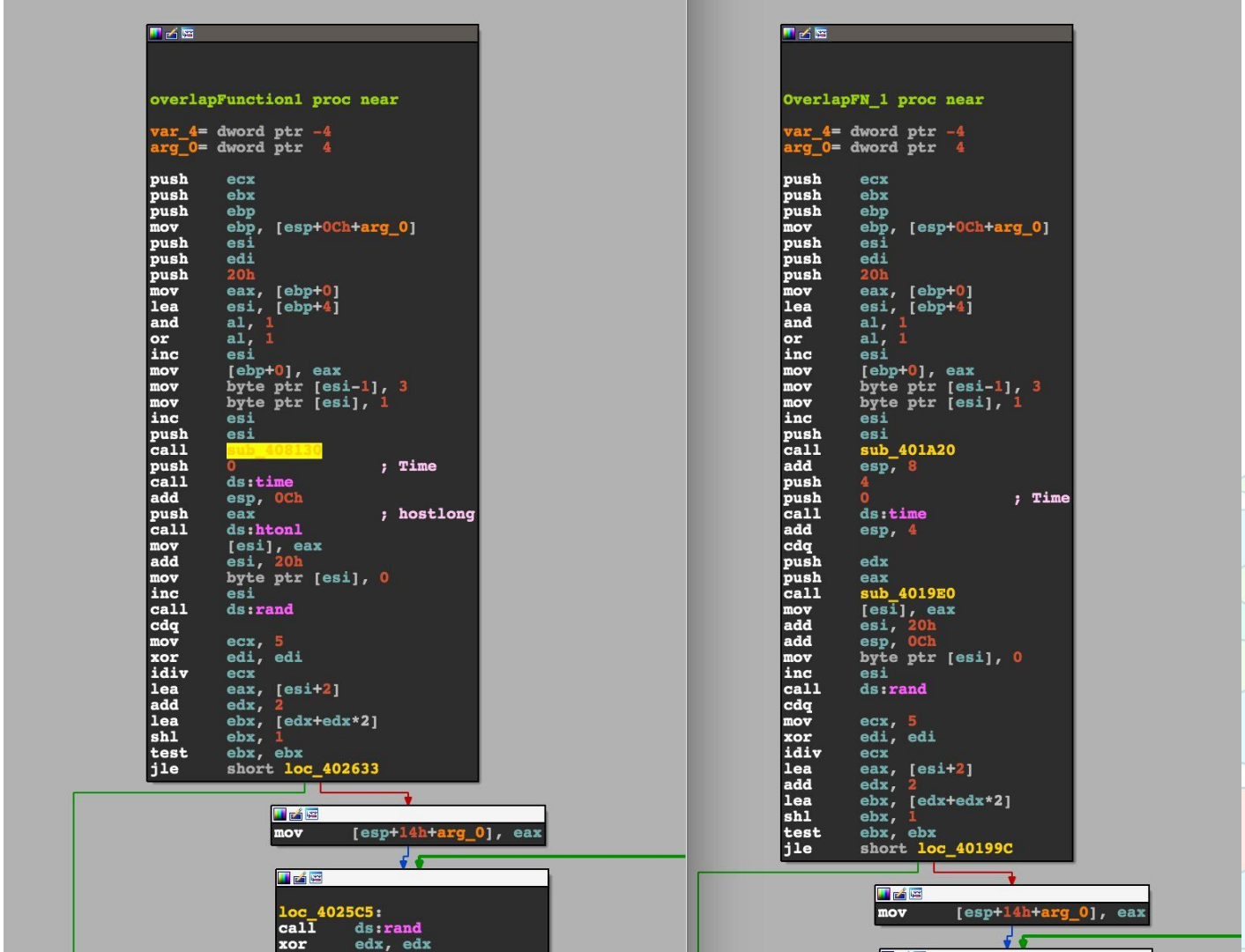
KASPERSKY lab comae technologies

# Identical Array Used by Shared Function




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_408130
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
push 0 ; Time
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)

KASPERSKY lab

comae technologies

# WannaCry Crypto

```
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        exportKeyOnDisk((int)v3, a3);
24      if ( !importPrivateKey((int)v3, lpFileName) )
25      {
26LABEL_19:
27        destroyAllKeys((int)v3);
28        return 0;
29      }
30    }
31    v5 = *((_DWORD *)v3 + 3);
32    if ( v5 )
33      CryptDestroyKey(v5);
34  }
35  else if ( !CryptImportKey(*((_DWORD *)v3 + 1), (const BYTE *)&RSA_Key_Testing, 0x114u, 0, 0, (HCRYPTKEY *)v
36  {
37    destroyAllKeys((int)v3);
38    return 0;
39  }
40  return 1;

00003AD5 sub_10003AC0:28
```

**.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)*

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

```
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_alavieala
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_alavieala
Mode(?)    : 4
Filesize   : 607
Final file: fake_alavieala

C:\security\wanadecrypt>
```

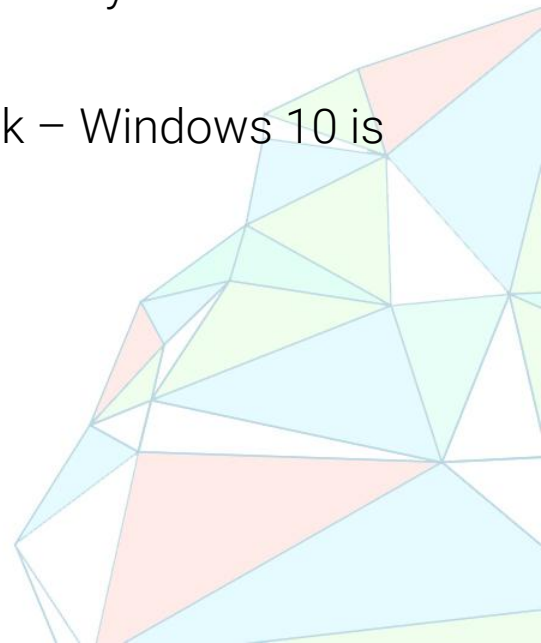
KASPERSKY lab

comae technologies

# 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



KASPERSKY lab

comae technologies

# 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**

KASPERSKY lab

comae technologies

# 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)**

KASPERSKY lab

comae technologies

# 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.

KASPERSKY lab

comae technologies

# 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-b8908fefea7e

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

KASPERSKY lab

comae technologies