Attribution in a world of cyberespionage

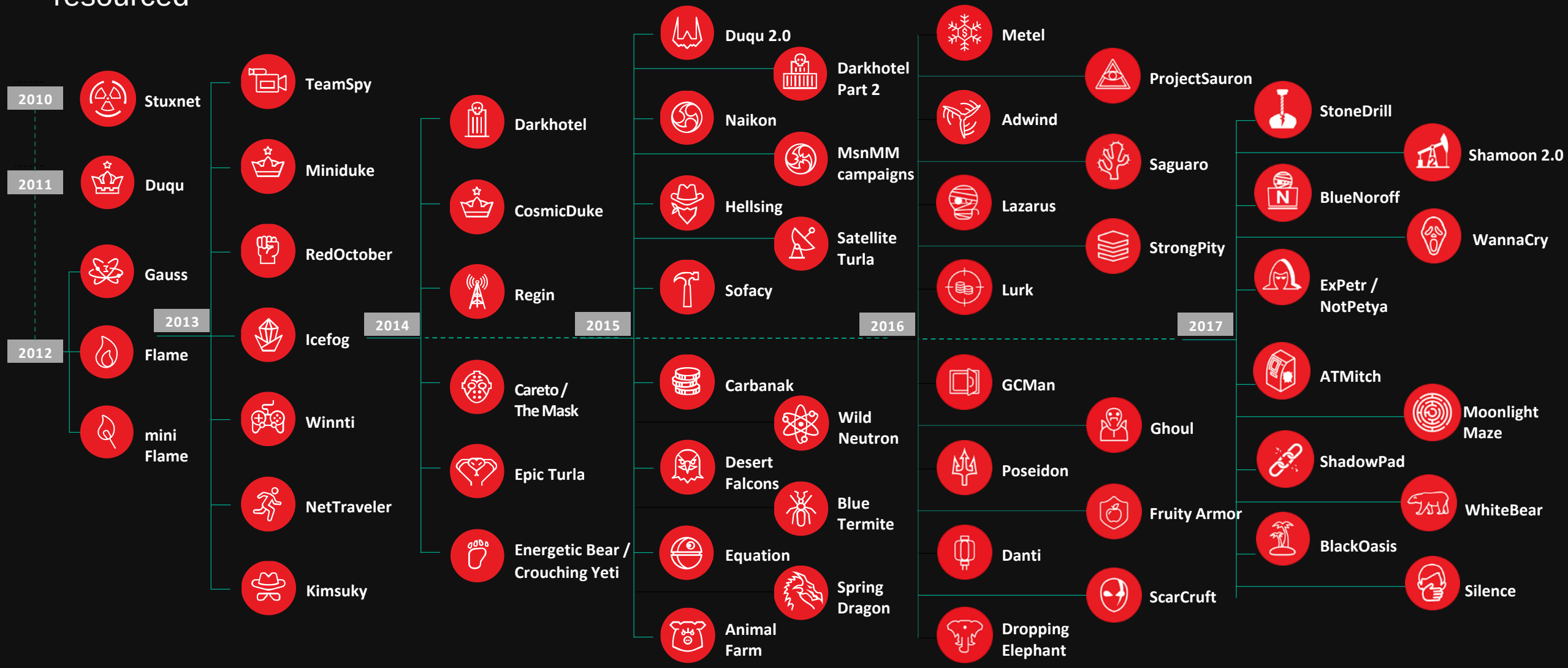
Yury Namestnikov

Head, Global Research and Analysis Team, Russia

KASPERSKY lab

Our Research

APT attacks – well planned and well resourced



Bill that would have the White House create a database of APT groups passes House vote

US hopes that a name-and-shame strategy would deter foreign nation-state hacking groups to attack US infrastructure as often as now.

By Catalin Cimpanu for Zero Day | September 8, 2018 -- 00:39 GMT (17:39 PDT) | Topic: Security

RELATED STORIES


Security
MongoDB server leaks 11 million user records from e-marketing service


Security
Bizarre botnet infects your PC to scrub away cryptocurrency mining malware


Security
GovPayNow payment portal may have exposed over 14 million customer records


Security
UK watchdog has not issued any GDPR data breach related fines yet

Okay, you know who did it and what next?

SEC. 3. ACTIONS TO ADDRESS STATE-SPONSORED CYBER ACTIVITIES AGAINST THE UNITED STATES.

(a) DESIGNATION AS A CRITICAL CYBER THREAT ACTOR.—

(1) IN GENERAL.—The President, acting through the Secretary of State, and in coordination with the heads of other relevant Federal agencies, shall designate as a critical cyber threat actor—

(A) each foreign person and each agency or instrumentality of a foreign state that the President determines to be knowingly responsible for or complicit in, or to have knowingly engaged in, directly or indirectly, state-sponsored cyber activities that are reasonably likely to result in, or have contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of—

(i) causing a significant disruption to the availability of a computer or network of computers;

115th Congress (2017-2018) | Get alerts

(b) NON-TRAVEL-RELATED SANCTIONS.—

(1) IN GENERAL.—The President shall impose one or more of the applicable sanctions described in paragraph (2) with respect to each foreign person and each agency or instrumentality of a foreign state designated as a critical cyber threat actor under subsection (a).

(2) SANCTIONS DESCRIBED.—The sanctions to be imposed under paragraph (1) with respect to a foreign person or an agency or instrumentality of a foreign state designated as a critical cyber threat actor under subsection (a) are the following:

(A) The President may provide for the withdrawal, limitation, or suspension of United States security assistance under part II of the Foreign Assistance Act of 1961 (22 U.S.C. 2301 et seq.) to or involving the foreign person or agency or instrumentality.

Introduced | Passed Senate | Passed House | To President | Became Law

KASPERSKY lab

Theory vs Practice

Right way to attribute cyberattacks:

- Catch cyber criminals in cooperation of different local police departments and industry experts

In reality:

- Slow cross-border interaction
- Tons of paper work
- Politics

False Flags

Bad Op Sec

Infrastructure Reuse

Code Reuse

Code similarity and bad OPSEC big stories


BANGLADESH BANK

LATEST OPSEC FAILURE

From the server logs of a C2 in Europe:

2017-01-18 02:54: Apache Tomcat started on port 8080
2017-01-18 04:10: HTTP GET view.jsp (via VPN in France)
2017-01-18 04:10: Testing bot (via VPN in France)
...
2017-01-18 08:12: Testing bot (via VPN in Korea)
...
2017-01-18 11:12: Testing bot (from IP in North Korea)

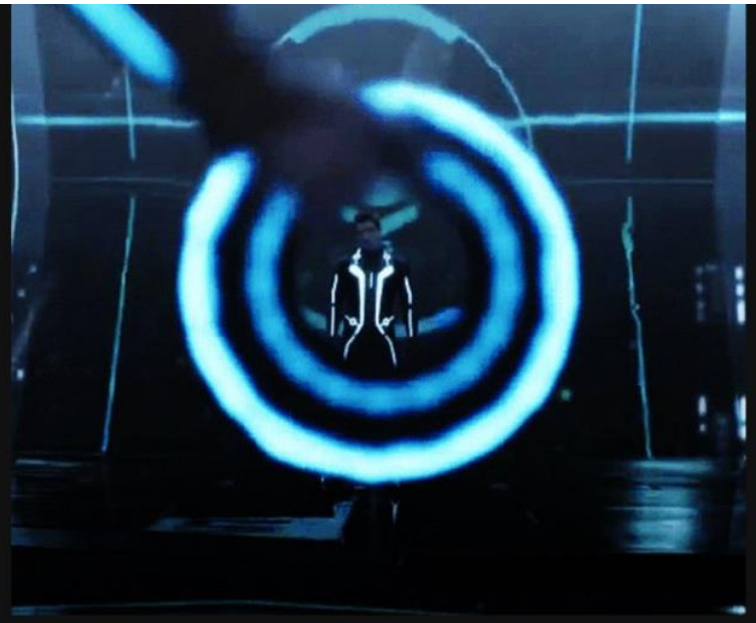
175.45.*.***

inetnum:	175.45.176.0 - 175.45.179.255
netname:	STAR-KP
descr:	Ryugyong-dong
descr:	Potong-gang District
role:	STAR JOINT VENTURE CO LTD
address:	Ryugyong-dong Potong-gang District
country:	KP

SECURELIST THREATS CATEGORIES

Lazarus Under The Hood

By GReAT on April 3, 2017. 5:57 pm



Forbes Billionaires Innovation Leadership Money Consumer Industry Lifestyle

8,754 views | Jun 22, 2017, 05:00am

Cyber Attack At Honda Stops Production After WannaCry Worm Strikes

Peter Lyon Contributor ⓘ
I focus on all things to do with cars.

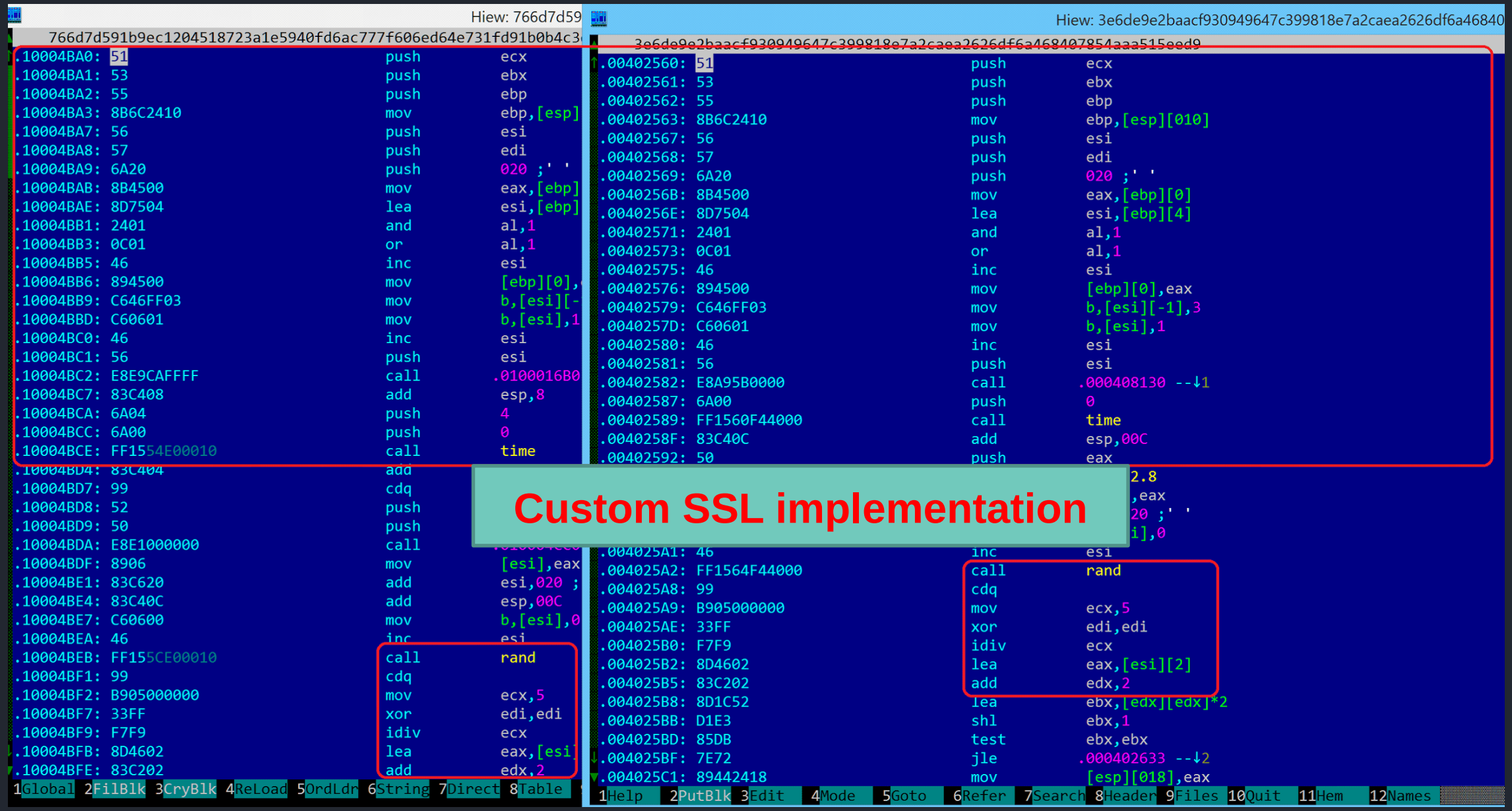
BUSINESS INSIDER

Renault-Nissan is resuming production after a global cyberattack caused stoppages at 5 plants

REUTERS

Laurence Frost and Naomi Tajitsu, Reuters
May 15, 2017, 1:25 PM

Renault-Nissan said on Monday that output had returned to normal at nearly all its plants, after a global cyber attack caused widespread disruption including stoppages at several of the auto alliance's sites.



Custom SSL implementation

GREAT Global Research & Analysis Team

KASPERSKY lab

Problem: find common code between files

- Easy approach: generate all 8-16-byte strings for all files in our collection. For new files, check overlaps.
- Problems:
  - Collection too big.
  - Capex too small. ☹
- How to solve it?

Introducing:
APT similarity hunting with Yara

Solution – multi step

- Identify relevant code in a file
- Extract _ONLY_ “interesting” strings
- Create a whitelisting databases of strings from clean files
- Extract interesting strings from new samples that are not in the whitelist db
- Make a Yara rule

Our code similarity system

- processed samples / day ~ 250 K
- known, good samples - 28 mln
- known, good strings - ~4 bln
- known, good opcode sequences - ~8 bln

Output: Yara rules and similarity profiles

Wannacry rule

```
rule ransomware_WannaCry_code {
meta:

        description = "Rule for WannaCry code, also matches other Lazarus"
        description = "campaigns: BlueNoroff, ManusCrypt, Decafett"
        hash = "808182340FB1B0B0B301C998E855A7C8"
        hash = "B9B3965D1B218C63CD317AC33EDCB942"
        author = "alice@kaspersky.com"

strings:

        $c1 = {5424FC740CC74424FC00000000015424}
        $c2 = {397424FC740CC74424FC000000000174}
        $c3 = {C74424FC00000000016C24FC83EC0439}
        $c4 = {5C24FC740CC74424FC00000000015C24}
        $c5 = {396C24FC740CC74424FC00000000016C}

condition:

        uint16(0) == 0x5A4D and filesize < 2000000 and all of them
}
```

Catches:

BlueNoroff, ManusCrypt, Decafett

Attributing APT malware by common code

CCleaner malware – custom base64 encoding

```
8f56fd14133ccd84b6395913536f5823d74737c410b829f729baaf2fe645a0a9
.003E121C: C3                  retn ; -^-^-^-^-^-^-^-^-^-^-^-^
.003E121D: 55                  push         ebp
.003E121E: 8BEC                mov          ebp,esp
.003E1220: 51                  push         ecx
.003E1221: 56                  push         esi
.003E1222: 57                  push         edi
.003E1223: 8B7D08              mov          edi,[ebp][8]
.003E1226: 85FF                test         edi,edi
.003E1228: 0F843F010000        jz           .0003E136D --↓1
.003E122E: 837D0C00            cmp          d,[ebp][00C],0
.003E1232: 0F8435010000        jz           .0003E136D --↓1
```

```
0375b42
.00401015:
.00401016:
.00401017:
.00401019:
.0040101A:
.0040101B:
.0040101C:
.0040101F:
.00401021:
.00401027:
.0040102B:
```

Costin Raiu ✓
@craiu

The malware injected into #CCleaner has shared code with several tools used by one of the APT groups from the #Axiom APT 'umbrella'.

11:34 AM - 19 Sep 2017

288 Retweets **271** Likes

7 288 271

Intezer
@IntezerLabs

Following

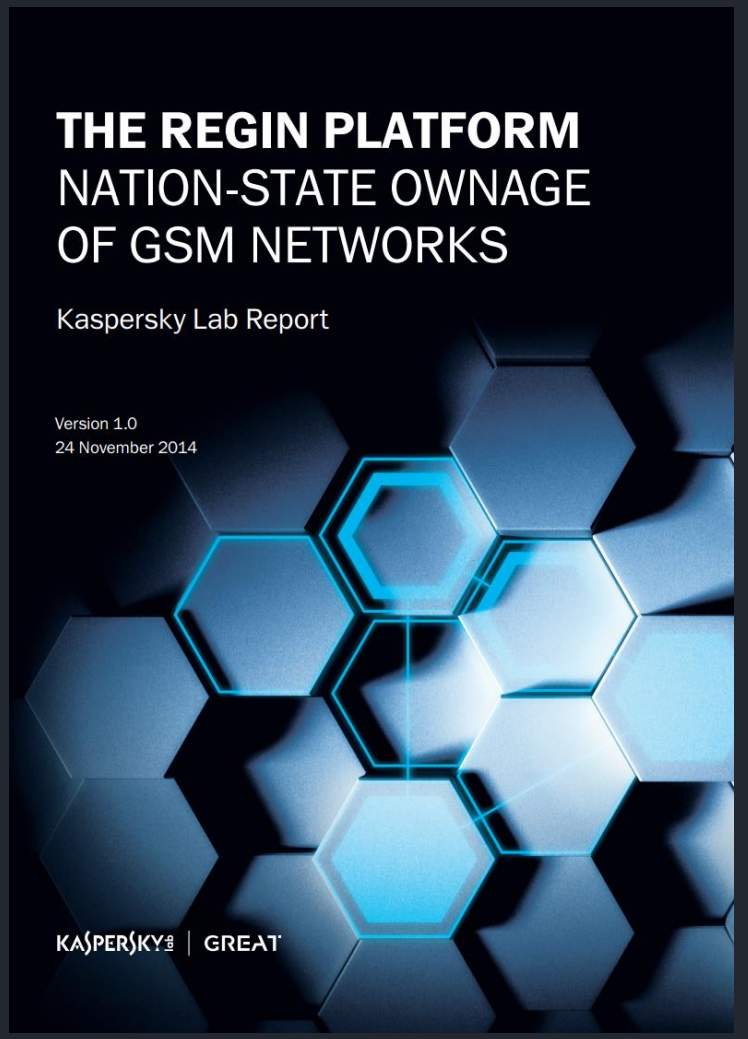
NEW BLOG POST: Evidence Aurora Operation Still Active: Supply Chain Attack Through CCleaner Read more: intezer.com/evidence-auror_...

2:29 PM - 20 Sep 2017

10 Retweets **16** Likes

10 16

Regin – GSM network pwnage



Regin rule

```
rule apt_ZZ_Regin_code2 {
meta:
 apt_ZZ_Regin_code2 C:\research\shadowbrokerss\part_banks\_unpacked_tar\windows\lib\x64-Windows\cnli-1.dll
 0xeba5:$c13: 5C 24 48 48 8B 6C 24 50 48 8B 74 24 58 8B C3 48
 0xec2d:$c13: 5C 24 48 48 8B 6C 24 50 48 8B 74 24 58 8B C3 48
 0xf356:$c46: 74 34 48 3B FB 74 2F 48 8B 0E 48 8D 54 24 40 FF
 0xeba0:$c48: 5F 08 EB 04 8B 5C 24 48 48 8B 6C 24 50 48 8B 74
 0xec28:$c48: 5F 08 EB 04 8B 5C 24 48 48 8B 6C 24 50 48 8B 74
 0xb824:$c59: 4C 89 44 24 18 4C 89 4C 24 20 48 83 EC 28 83 C8
 0xb850:$c59: 4C 89 44 24 18 4C 89 4C 24 20 48 83 EC 28 83 C8
 0xeb9b:$c71: 5C 24 48 48 01 5F 08 EB 04 8B 5C 24 48 48 8B 6C
 0xec23:$c71: 5C 24 48 48 01 5F 08 EB 04 8B 5C 24 48 48 8B 6C
 0x61a8:$c73: 48 85 C9 74 20 57 48 83 EC 20 4C 8B C1 48 8B F9
 0xeb98:$c85: 74 0A 8B 5C 24 48 48 01 5F 08 EB 04 8B 5C 24 48
 0xec20:$c85: 74 0A 8B 5C 24 48 48 01 5F 08 EB 04 8B 5C 24 48
s0x61ad:$c93: 57 48 83 EC 20 4C 8B C1 48 8B F9 33 C0 48 8B CA
 0xf37a:$c95: 75 10 8B 4C 24 40 B3 01 48 C1 E1 20 48 0B CE 48
 0x11c14:$c105: 33 C0 48 3B C8 74 14 48 39 01 74 0F 48 83 39 FF
/0x9a8e:$c110: 5C 24 08 57 48 83 EC 20 33 FF 48 3B CF 74 19 E8
 0x9a8b:$c120: CC 48 89 5C 24 08 57 48 83 EC 20 33 FF 48 3B CF
 0x9ac3:$c120: CC 48 89 5C 24 08 57 48 83 EC 20 33 FF 48 3B CF
c0x61a6:$c123: CC CC 48 85 C9 74 20 57 48 83 EC 20 4C 8B C1 48
 0x9ac6:$c138: 5C 24 08 57 48 83 EC 20 33 FF 48 3B CF 74 1A FF
 0x6df8:$c193: 32 C0 BA FF FF FF FF 41 B8 01 00 00 00 48 3B CA
}
```

Yara finds Shadowbrokers' **cnli-1.dll**

Shadowbrokers dump libraries?

cnli-1.dll exports:

```
34  .00000001`80010660 CNEFileIO_dirInstall
35  .00000001`80012130 CNEFileIO_dirInstallW
36  .00000001`8001077C CNEFileIO_dirNext
37  .00000001`80010A78 CNEFileIO_dirNextDirectory
38  .00000001`8001086C CNEFileIO_dirNextEx
39  .00000001`80012434 CNEFileIO_dirNextExW
40  .00000001`800122FC CNEFileIO_dirNextW
41  .00000001`80010498 CNEFileIO_dirOpen
42  .00000001`80011EFC CNEFileIO_dirOpenW
43  .00000001`80010754 CNEFileIO_dirRemove
44  .00000001`80012294 CNEFileIO_dirRemoveW
45  .00000001`80010B58 CNEFileIO_dirReset
46  .00000001`80012688 CNEFileIO_expendFilenameA
47  .00000001`80010C4C CNEFileIO_expendFilenameW
48  .00000001`8000F684 CNEFileIO_fileClose
49  .00000001`800100B0 CNEFileIO_fileCopy
50  .00000001`80011C40 CNEFileIO_fileCopyW
51  .00000001`8000F6C8 CNEFileIO_fileExists
52  .00000001`80011470 CNEFileIO_fileExistsW
53  .00000001`8000F6F4 CNEFileIO_fileFlush
54  .00000001`80001E40 CNEFileIO_fileGetDir
55  .00000001`80001F00 CNEFileIO_fileGetDirExW
56  .00000001`80001EA0 CNEFileIO_fileGetDirW
57  .00000001`80001F5C CNEFileIO_fileGetPos
58  .00000001`80001D78 CNEFileIO_fileGetPosEx
59  .00000001`800119EC CNEFileIO_fileGetSize
```

CNE?

C:\...npacked_tar\windows\lib\x64-Windows

n	Name		Size	Date	Time
..			Up	04/14/17	09:53
_pytrch		pyd	190976	04/14/17	09:53
adfw-2		dll	16896	04/14/17	09:53
cnli-1		dll	125440	04/14/17	09:53
coli-0		dll	17408	04/14/17	09:53
crli-0		dll	19968	04/14/17	09:53
dmgd-1		dll	36864	04/14/17	09:53
dmgd-4		dll	485376	04/14/17	09:53
exma-1		dll	10240	04/14/17	09:53
iconv		dll	26624	04/14/17	09:53
libcurl		dll	253440	04/14/17	09:53
libeay32		dll	1133 K	04/14/17	09:53
libxml2		dll	994 K	04/14/17	09:53
pcre-0		dll	174080	04/14/17	09:53
pcrecpp-0		dll	36864	04/14/17	09:53
pcreposix-0		dll	9216	04/14/17	09:53
posh-0		dll	11264	04/14/17	09:53
pytrch		py	38209	04/14/17	09:53
ssleay32		dll	230912	04/14/17	09:53
tibe-2		dll	304128	04/14/17	09:53
trch-1		dll	75264	04/14/17	09:53
trfo-2		dll	35328	04/14/17	09:53
tucl-1		dll	9728	04/14/17	09:53
ucl		dll	41472	04/14/17	09:53
xdvl-0		dll	39424	04/14/17	09:53
zlib1		dll	68608	04/14/17	09:53

Regin / cnli-1.dll shared code example:

```
__int64 __fastcall regin_sub_10018E0(__int64 a1, const void *a2, unsigned
{
  unsigned int v3; // ebx@1
  unsigned __int64 v4; // rsi@1
  const void *v5; // rbp@1
  __int64 v6; // rdi@1
  DWORD NumberOfBytesWritten; // [sp+48h] [bp+10h]@1

  v3 = 0;
  v4 = a3;
  v5 = a2;
  v6 = a1;
  NumberOfBytesWritten = 0;
  if ( a2 )
  {
    if ( (unsigned __int8)sub_1001620()
      && v4
      && *(_BYTE *)(v6 + 16) & 2
      && v4 <= 0xFFFFFFFF
      && WriteFile(*(HANDLE *)v6, v5, v4, &NumberOfBytesWritten, 0i64) )
    {
      v3 = 0;
      *(_QWORD *)(v6 + 8) = *(_QWORD *)(v6 + 8);
    }
    else
    {
      v3 = 0;
    }
```

Regin sample
66afaa303e13faa4913eaad50f7237ea

```
__int64 __fastcall CNEFileIO_fileWriteEx(__int64 a1, const void *a2, unsig
{
  unsigned int v3; // ebx@1
  unsigned __int64 v4; // rsi@1
  const void *v5; // rbp@1
  __int64 v6; // rdi@1
  DWORD NumberOfBytesWritten; // [sp+48h] [bp+10h]@1

  v3 = 0;
  v4 = a3;
  v5 = a2;
  v6 = a1;
  NumberOfBytesWritten = 0;
  if ( a2 )
  {
    if ( (unsigned __int8)CNEFileIO_fileIsOpen()
      && v4
      && *(_BYTE *)(v6 + 16) & 2
      && v4 <= 0xFFFFFFFF
      && WriteFile(*(HANDLE *)v6, v5, v4, &NumberOfBytesWritten, 0i64) )
    {
      v3 = 0;
      *(_QWORD *)(v6 + 8) = *(_QWORD *)(v6 + 8);
    }
    else
    {
      v3 = 0;
    }
```

cnli-1.dll
07cc65907642abdc8972e62c1467e83b

The Lamberts APT

Story started from a **zero-day**

Targets list includes:
Aerospace, ICS, Energy sector,
Nuclear research, engineering

3 YEARS OF RESEARCH

Operator can do anything:
60+ modules

The Lamberts APT

```
.00016D87: 6A10      push      010
.00016D89: 8811      mov       [ecx],dl
.00016D8B: 8A5001    mov       dl,[eax][1]
.00016D8E: 325301    xor       dl,[ebx][1]
.00016D91: 885101    mov       [ecx][1],dl
.00016D94: 8A5002    mov       dl,[eax][2]
.00016D97: 325302    xor       dl,[ebx][2]
.00016D9A: 885102    mov       [ecx][2],dl
.00016D9D: 8A5003    mov       dl,[eax][3]
.00016DA0: 325303    xor       dl,[ebx][3]
.00016DA3: 885103    mov       [ecx][3],dl
.00016DA6: 8A5004    mov       dl,[eax][4]
.00016DA9: 325304    xor       dl,[ebx][4]
.00016DAC: 885104    mov       [ecx][4],dl
.00016DAF: 8A5005    mov       dl,[eax][5]
.00016DB2: 325305    xor       dl,[ebx][5]
.00016DB5: 885105    mov       [ecx][5],dl
.00016DB8: 8A5006    mov       dl,[eax][6]
.00016DBB: 325306    xor       dl,[ebx][6]
.00016DBE: 885106    mov       [ecx][6],dl
.00016DC1: 8A5007    mov       dl,[eax][7]
.00016DC4: 325307    xor       dl,[ebx][7]
.00016DC7: 885107    mov       [ecx][7],dl
.00016DCA: 8A5008    mov       dl,[eax][8]
.00016DCD: 325308    xor       dl,[ebx][8]
.00016DD0: 885108    mov       [ecx][8],dl
.00016DD3: 8A5009    mov       dl,[eax][9]
.00016DD6: 325309    xor       dl,[ebx][9]
.00016DD9: 885109    mov       [ecx][9],dl
.00016DDC: 8A500A    mov       dl,[eax][00A]
.00016DDF: 32530A    xor       dl,[ebx][00A]
.00016DE2: 88510A    mov       [ecx][00A],dl
.00016DE5: 8A500B    mov       dl,[eax][00B]
.00016DE8: 32530B    xor       dl,[ebx][00B]
.00016DEB: 88510B    mov       [ecx][00B],dl
.00016DEE: 8A500C    mov       dl,[eax][00C]
.00016DF1: 32530C    xor       dl,[ebx][00C]
.00016DF4: 88510C    mov       [ecx][00C],dl
```

WhiteLambert 1.2 driver

2f60906ca535eb958389e6aed454c2a2

```
.0040D8FB: 6A10      push      010
.0040D8FD: 8811      mov       [ecx],dl
.0040D8FF: 8A5001    mov       dl,[eax][1]
.0040D902: 325301    xor       dl,[ebx][1]
.0040D905: 885101    mov       [ecx][1],dl
.0040D908: 8A5002    mov       dl,[eax][2]
.0040D90B: 325302    xor       dl,[ebx][2]
.0040D90E: 885102    mov       [ecx][2],dl
.0040D911: 8A5003    mov       dl,[eax][3]
.0040D914: 325303    xor       dl,[ebx][3]
.0040D917: 885103    mov       [ecx][3],dl
.0040D91A: 8A5004    mov       dl,[eax][4]
.0040D91D: 325304    xor       dl,[ebx][4]
.0040D920: 885104    mov       [ecx][4],dl
.0040D923: 8A5005    mov       dl,[eax][5]
.0040D926: 325305    xor       dl,[ebx][5]
.0040D929: 885105    mov       [ecx][5],dl
.0040D92C: 8A5006    mov       dl,[eax][6]
.0040D92F: 325306    xor       dl,[ebx][6]
.0040D932: 885106    mov       [ecx][6],dl
.0040D935: 8A5007    mov       dl,[eax][7]
.0040D938: 325307    xor       dl,[ebx][7]
.0040D93B: 885107    mov       [ecx][7],dl
.0040D93E: 8A5008    mov       dl,[eax][8]
.0040D941: 325308    xor       dl,[ebx][8]
.0040D944: 885108    mov       [ecx][8],dl
.0040D947: 8A5009    mov       dl,[eax][9]
.0040D94A: 325309    xor       dl,[ebx][9]
.0040D94D: 885109    mov       [ecx][9],dl
.0040D950: 8A500A    mov       dl,[eax][00A]
.0040D953: 32530A    xor       dl,[ebx][00A]
.0040D956: 88510A    mov       [ecx][00A],dl
.0040D959: 8A500B    mov       dl,[eax][00B]
.0040D95C: 32530B    xor       dl,[ebx][00B]
.0040D95F: 88510B    mov       [ecx][00B],dl
.0040D962: 8A500C    mov       dl,[eax][00C]
.0040D965: 32530C    xor       dl,[ebx][00C]
.0040D968: 88510C    mov       [ecx][00C],dl
```

BlackLambert font exploit

99ef1e473ac553cf80f6117b2e95e79b

```
.0040C76B: 6A10      push      010
.0040C76D: 8811      mov       [ecx],dl
.0040C76F: 8A5001    mov       dl,[eax][1]
.0040C772: 325301    xor       dl,[ebx][1]
.0040C775: 885101    mov       [ecx][1],dl
.0040C778: 8A5002    mov       dl,[eax][2]
.0040C77B: 325302    xor       dl,[ebx][2]
.0040C77E: 885102    mov       [ecx][2],dl
.0040C781: 8A5003    mov       dl,[eax][3]
.0040C784: 325303    xor       dl,[ebx][3]
.0040C787: 885103    mov       [ecx][3],dl
.0040C78A: 8A5004    mov       dl,[eax][4]
.0040C78D: 325304    xor       dl,[ebx][4]
.0040C790: 885104    mov       [ecx][4],dl
.0040C793: 8A5005    mov       dl,[eax][5]
.0040C796: 325305    xor       dl,[ebx][5]
.0040C799: 885105    mov       [ecx][5],dl
.0040C79C: 8A5006    mov       dl,[eax][6]
.0040C79F: 325306    xor       dl,[ebx][6]
.0040C7A2: 885106    mov       [ecx][6],dl
.0040C7A5: 8A5007    mov       dl,[eax][7]
.0040C7A8: 325307    xor       dl,[ebx][7]
.0040C7AB: 885107    mov       [ecx][7],dl
.0040C7AE: 8A5008    mov       dl,[eax][8]
.0040C7B1: 325308    xor       dl,[ebx][8]
.0040C7B4: 885108    mov       [ecx][8],dl
.0040C7B7: 8A5009    mov       dl,[eax][9]
.0040C7BA: 325309    xor       dl,[ebx][9]
.0040C7BD: 885109    mov       [ecx][9],dl
.0040C7C0: 8A500A    mov       dl,[eax][00A]
.0040C7C3: 32530A    xor       dl,[ebx][00A]
.0040C7C6: 88510A    mov       [ecx][00A],dl
.0040C7C9: 8A500B    mov       dl,[eax][00B]
.0040C7CC: 32530B    xor       dl,[ebx][00B]
.0040C7CF: 88510B    mov       [ecx][00B],dl
.0040C7D2: 8A500C    mov       dl,[eax][00C]
.0040C7D5: 32530C    xor       dl,[ebx][00C]
.0040C7D8: 88510C    mov       [ecx][00C],dl
```

BrownLambert

6c466283e7f8757973ba253aa6080d8c

False Flags

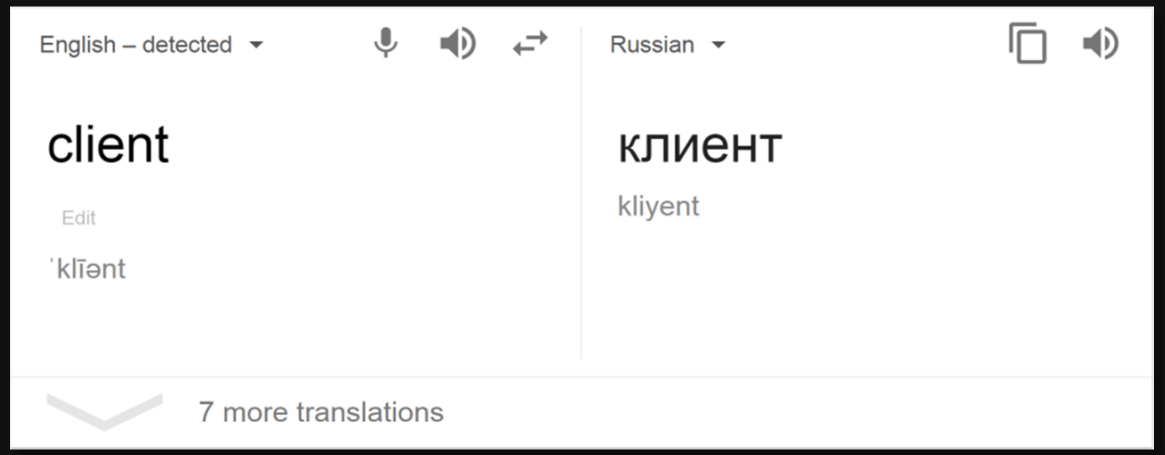
NSA Official Suggests North Korea Was Culprit in Bangladesh Bank Heist

The deputy director of the NSA says he believes states have entered the bank-robbing business.

Effect: FALSE FLAGS

```
"Nachalo" - start communication session
"ustanavlivat" - handshake state
"poluchit" - receive data
"pereslat" - send data
"derzhat" - maintain communication session
"vykhodit" - exit communication session

"kliyent2podklyuchit” - client2connect ??
```




```
private function put_dummy_args(param1:*) : *
      {
         return chainik.call.apply(null,param1);
      }
```


PyeongChang 2018™

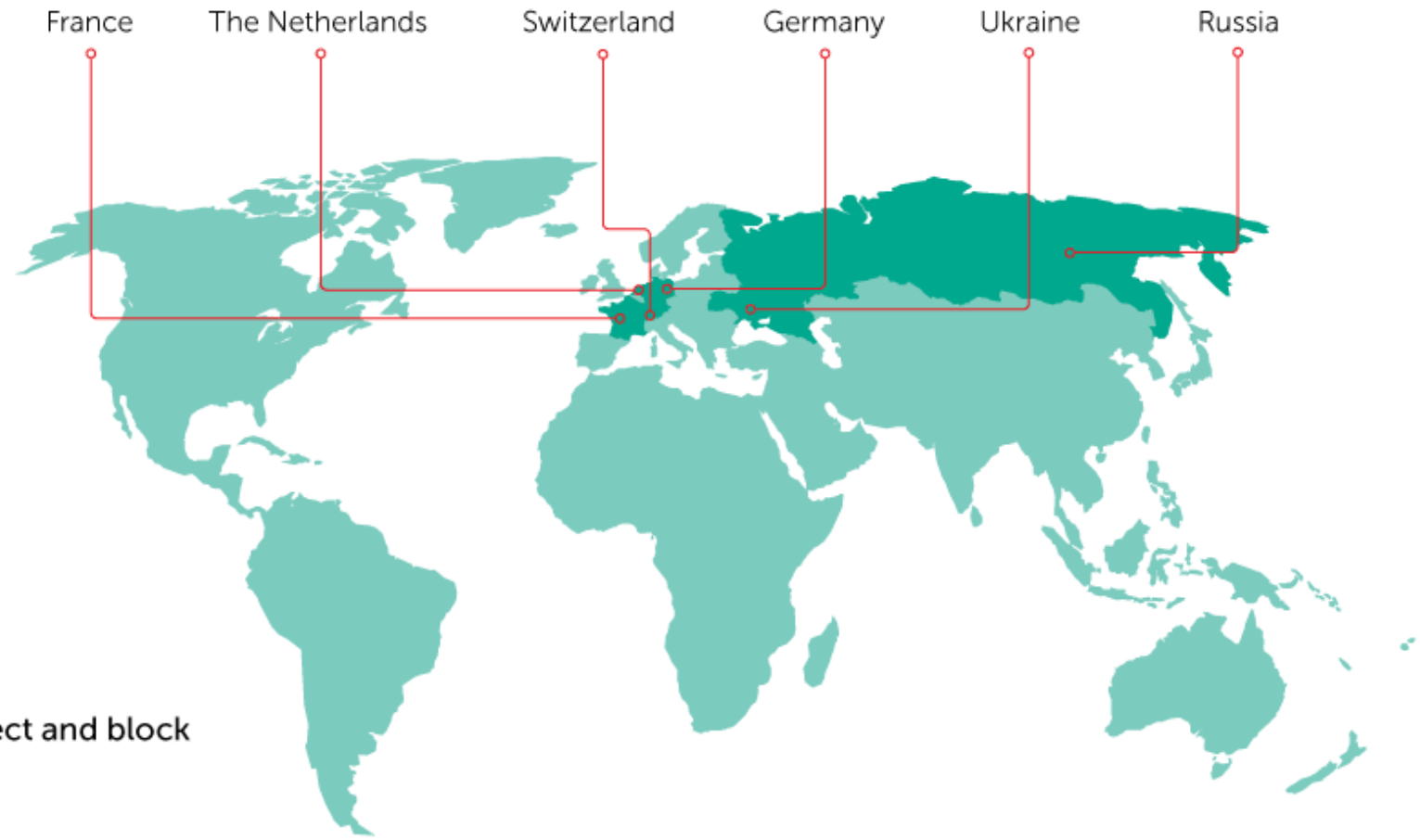
Targets of recent Olympic Destroyer attacks

In May-June 2018 Kaspersky Lab discovered new spear-phishing documents related to Olympic Destroyer. The threat actor had previously attacked Winter Olympics infrastructure.

Targets:

Biological and chemical threat prevention organizations

Financial institutions (in Russia only)



Kaspersky Lab products successfully detect and block Olympic Destroyer-related malware.

KASPERSKY lab GREAT

Attribution 2.0?

Attribution 2.0

- Tasks which took months (years?) can now be done in minutes
- Technology will become ubiquitous in 2-3 years
- Attributing attacks can be partly automated
- Effect: more false flags
  - Think Lazarus malware with Russian keywords evolved
  - OlympicDestroyer
- Effect: more scripting, reliance on automated tools
  - PowerShell, CobaltStrike to Metasploit

Let’s find out more together

Yury Namestnikov, Kaspersky Labs