Place of Attribution in Threat Intelligence

Nikolay Akatyev*, Fyodor Yarochkin
Vladimir Kropotov**

About speaker(s)

Agenda

Why Attribution?

Generic Principles of Attribution

Attribution Case Studies

Conclusions

Why Attribution?

What are the common questions people try to answer with attribution?

- Am I a targeted victim or was hit by a random chance?
- What should I do to address the situation?

Disclaimer

- We try not to attribute any of the activity to any Nation State
- When we say “attribution” - we try to give answers to the following questions:
  - Are we dealing with any known threat actor?
  - Is the actor commonly targeting specific targets?
  - Learn more about the threat actor: working hours, possible geographic location, association with other peers
  - Targets of interest, tools and techniques commonly used by the threat actor
  - And more..

Attribution is Difficult: WHY?

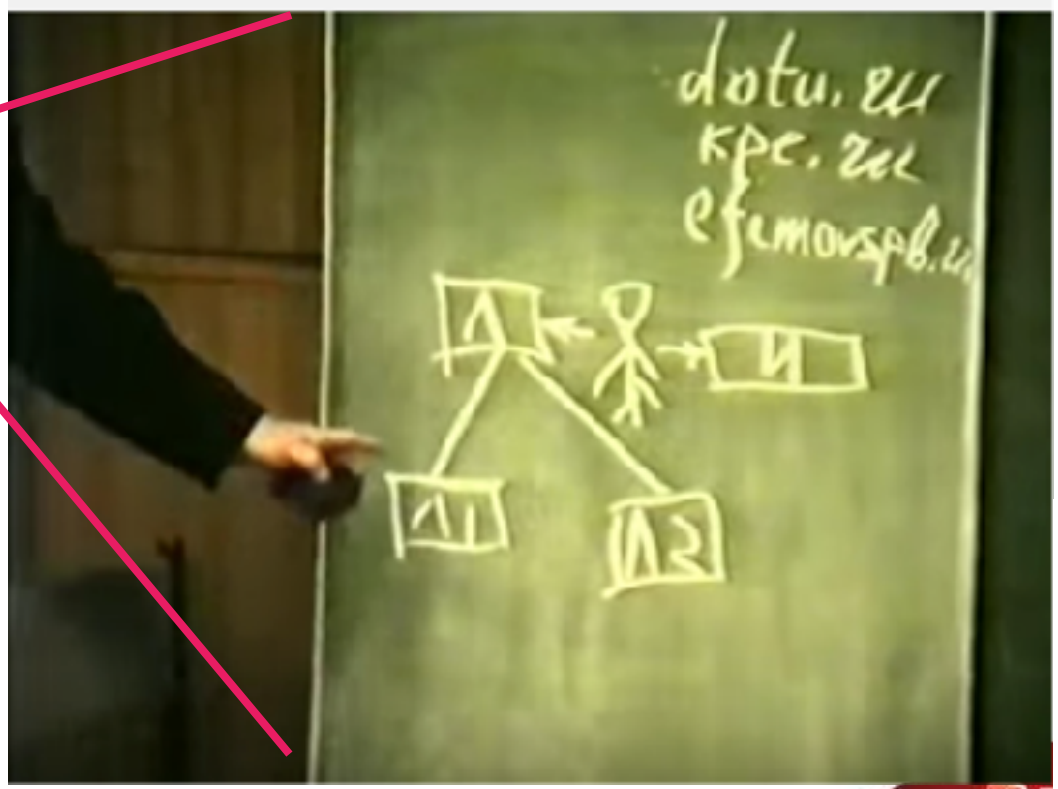
Attribution of targeted attacks is often similar to Intelligence/Counter-Intelligence

operations where for every question **multiple answers** could be found and you need to make an educated decision which answers are right.

Battle for Inchon

JUST LIKE WITH REAL SPIES, RIGHT? :)

There are multiple versions of Truth



https://www.youtube.com/watch?v=uTXs-XKA4pI

Economical Metrics TO Attribution

Scientists like quantifiable results (show me the numbers!)

Some artifacts are harder to fake than others.

Consistently faking certain artifacts to match a particular threat actor is expensive.

Examining validity/truthfulness of certain artifacts from the point of cost-evaluation can be effective.

Common Approaches in Attribution

- Use known data and metadata: IP, Domain, Character Encoding, Strings, Time-Zones
- Based on Humint (human intelligence)
- Based on Known/Visible Actor Targets
- Based on Known/Visible Actor Objectives
- Binary structure and anomalies in binary structures or implementation of algorithms
- Call back/Hack back/Interact with attacker
- Attacker Errors
- Average dwelling time (how long actor stays undetected)
- Data leaks, like Wiki Leaks (Often Reliable)

Cost?

"Mistakenly" leaking language encoding in binaries is cheaper.

Consistently leaking the same encoding, as mistake, across multiple campaigns, is expensive and requires perfect OPSEC discipline.

Cost(of falsifying an Attribution Artifact)

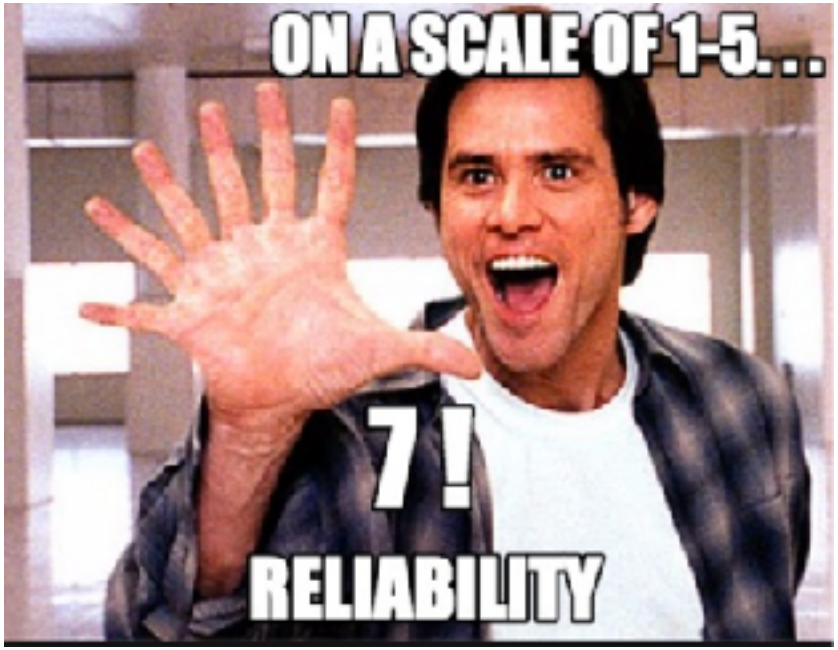
Cost(Attribution Artifact) = Expense required to fake given artifact over period of time

Awesome talk on cost of IOCs by pinkflawd and blackswanburst: IOCannon: Blasting back on Attackers with Economics

https://github.com/pinkflawd/IoCannon

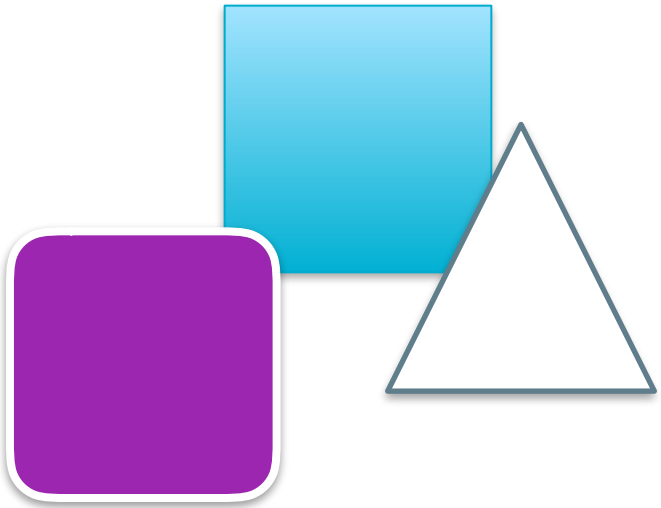
Reliability

Reliability Level of Attribution Artifacts has direct impact on incurring cost of faking them.

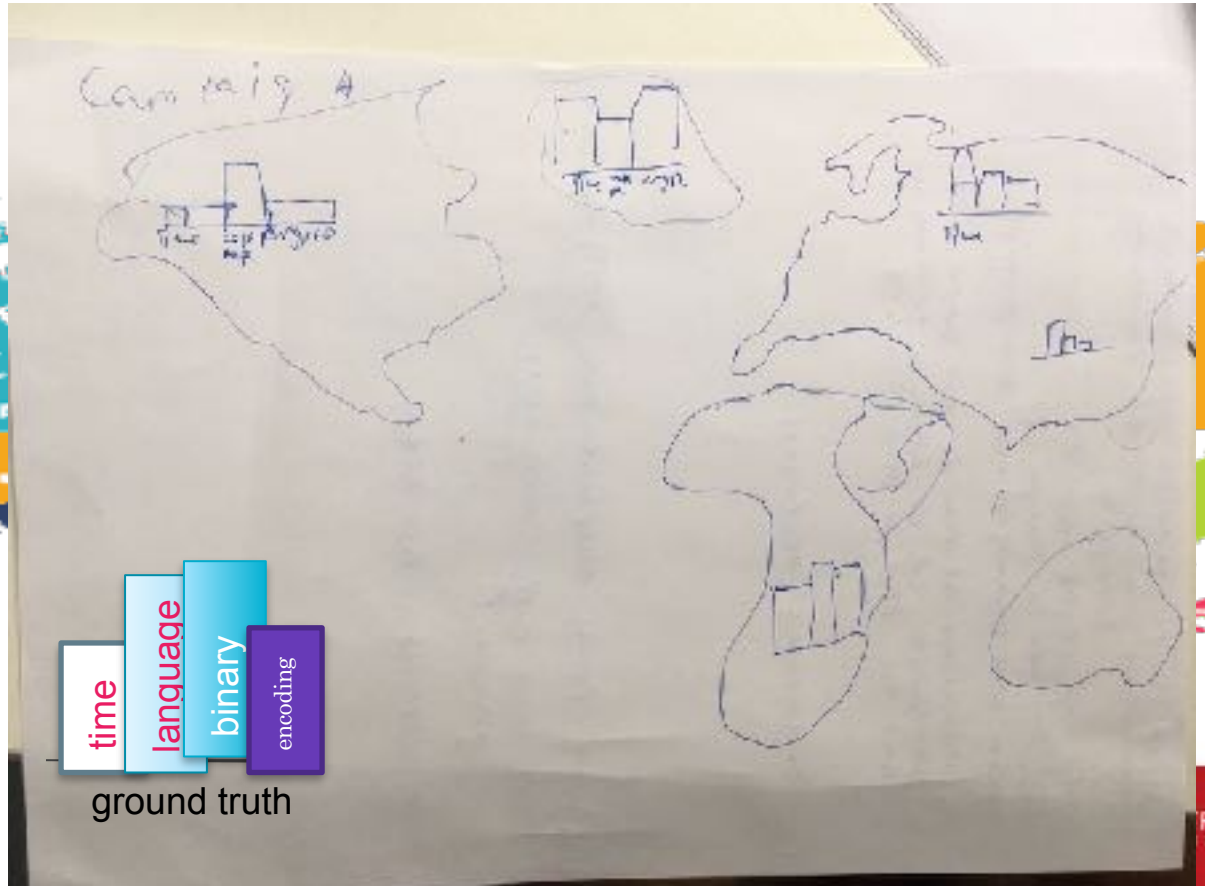


Composition

When we verify our hypothesis, we must consider a set of artifacts, and more is better.



Composition of Artifacts




uniqueness
Don’t stand out!
TREND MICRO
Securing Your Journey to the Cloud

Equation Group

What did Equation do wrong, and how can we avoid doing the same?

...

https://wikileaks.org/ciav7p1/cms/page_14588809.html

ISSUE: Use of customized crypto:

If using a custom crypto algorithm limit its use to a specific tool set

Use publicly available crypto (Microsoft's Encryption Libraries, OpenSSL, PolarSSL)

ISSUE: Unique MUTEX in privlib

If a mutex like this is needed, a compiler warning should be generated and the mutex used shoul

ISSUE: Pdb string in the binary:

We need to create a string scanner that queries active directory for user names, and such

ISSUE: Reuse of exploits

Example of equation group mistakes

Source: https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

The RC5/6 implementation from Equation group's malware is particularly interesting and deserves special attention because of its specifics.

```
.10010119: C745F884000000      mov     d,[ebp][-8],000000084 ;'    ä'
.10010120: C7006351E1B7        mov     d,[eax],0B7E15163 ;'▒ßQc'
.10010126: 41                  inc     ecx
.10010127: 8B5488FC           2mov     edx,[eax][ecx]*4[-4]
.1001012B: 81EA4786C861        sub     edx,061C88647 ;'a╠╠G'
.10010131: 891488              mov     [eax][ecx]*4,edx
.10010134: 41                  inc     ecx
.10010135: 83F92C              cmp     ecx,02C ;','
.10010138: 7CED                jl      .010010127 --↑2
.1001013A: 33D2                xor     edx,edx
.1001013C: 33DB                xor     ebx,ebx
.1001013E: 8955FC              mov     [ebp][-4],edx
.10010141: 33FF                xor     edi,edi
.10010143: EB03                jmps    .010010148 --↓3
.10010145: 8B4508              mov     eax,[ebp][8]
.10010148: 8B75FC             3mov     esi,[ebp][-4]
```

Encryption-related code in a DoubleFantasy sample

In the screenshot above, one can observe the main loop of a RC6 key setup subroutine extracted from one of the Equation group samples

Difficulty of faking artifacts

C2 calling pattern: easy - just cut-n-paste

Domain name - harder, requires ability of taking over a domain name

IP address - even harder. May need to be able to compromise the hosting system.

Let’s think about different approaches

# of Attribution

TREND MICRO

Securing Your Journey to the Cloud

How reliable approaches based on data and metadata

- IP, Domain, Encoding, Strings, Time-Zones
  - Have you seen rental contract for hosting? How long it typically lasts? Never heard about proxies? Innocent victims, when c2 hosted on EDU, Gov resources or News outlets?
- Code snippets
  - Could it be just public library?
  - Have you seen it at the first time? Along one campaign? Inside legit code?
  - Rarely used programming languages? Crypto algorithms? Encoding?

How reliable approaches based on Anomalies in Binary structure

- Host indicators and file dependencies
- How maps to killchain stages
- Anomalies in Binary structure (anti-forensics tricks)
  - Coders and packers?
  - Uniq compilation and optimization tools?
  - Execution paths
  - Code protection methods

Fuzzy Hashing algorithms can help to find related binaries:

https://github.com/trendmicro/tlsh - Locality Sensitive Hashing (opensource)

Ex. Lazarus binaries

The Enigma Protector

Защита программного обеспечения

imphash:5e5ac8ab7be27ac2d1c548e5589378b6

FileVersionInfo properties

Copyright	(c) Izex Lab. All rights reserved.
Product	NetHelper V7.0
Original name	NHEnrollMon.exe

How reliable approaches based on non technical indicators

- Based on Humint
  - How reliable the source? Does the source have enough capabilities to make a judgement on this topic? Does the source have hidden agenda?
- Based on Visible actor Targets
  - Actor targets particular industry? Particular countries?
  - Almost everyone? Almost every country **exept...**?
- Based on Visible actor Objectives
  - Money focused
  - Tactical tasks
  - Strategic tasks
- Based on Visible actor Objectives over angle
  - Enhance actor capabilities
  - Reduce victim capabilities

How reliable approaches based on Statistics and Long term campaign analysis

- Attacker errors (faults - Hangover), especially crypto
- Average dwelling time (how long actor stays undetected)
  - Detected in days and weeks
  - Detected in Months
  - Detected in Years
- Data leaks, like Wiki Leaks (Often Reliable)
  - Leaked source code of the binaries
  - Leaked unique exploits
  - Dumps of the (De)Classified documents

How reliable approaches based on Active actions

- Call back
  - Feed attacker with something, that do passive or silent fingerprinting
- Hack Back
  - Mostly the field of LE agencies, but there are a number of public examples
- Interact with attacker
  - Force the attacker to make a mistake during the interaction and win your time and try to reveal the attacker identity

Campaigns

Attributing binaries is difficult. No context. Binaries are often shared between the groups.

Attribution activity campaigns can be a little bit more simpler, because of presence of additional components: a victim, attacker TTPs and so on, time, compromised hosts, time zone of attacker activity and so on

So lets look into some case studies

TREND MICRO
Securing Your Journey to the Cloud

Hack back - control c2 server

https://malware.lu/assets/files/articles/

malware.lu/assets/files/articles/RAP002_APT1_Technical_backstage.1.0.pdf

3.4 Exploitation

With the information we previously described, we were able to get access to the attackers servers.

```
msf  exploit(poisonivy_bof_v2) > show options

Module options (exploit/windows/misc/poisonivy_bof_v2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   Password     pswpsw           yes       Client password
```

Hummint attribution

Human intelligence: always reliable!

Errors and mistakes by attacker

Use of crypto : forgotten certificates, keys oops..

Proxy/VPN use errors

```
95.[redacted]- - [09/Sep/2014:18:37:23 +0400] "GET
/cl[redacted]on/atext/fonts/verdana.ttf HTTP/1.1" 200 171792
95.[redacted]- - [09/Sep/2014:18:37:24 +0400] "GET
/cl[redacted]on/atext/fonts/times.ttf HTTP/1.1" 200 469280
95.[redacted]- - [09/Sep/2014:18:37:25 +0400] "GET
/cl[redacted]on/atext/fonts/arial.ttf HTTP/1.1" 200 367112
95.[redacted]- - [09/Sep/2014:18:37:27 +0400] "GET /files/main.swf
HTT[redacted] 570358
46.[redacted] - [09/Sep/2014:18:43:03 +0400] "GET /classes/classes.zip
HTT[redacted] 225
46.[redacted] - [09/Sep/2014:18:43:04 +0400] "GET /favicon.ico HTTP/1.1"
200
46.[redacted] - [09/Sep/2014:18:43:09 +0400] "GET /classes.zip HTTP/1.1"
200
46.[redacted] - [09/Sep/2014:18:44:24 +0400] "GET /classes/ HTTP/1.1" 200
0
46.[redacted] - [09/Sep/2014:18:44:46 +0400] "GET /classes/common/mpanel/
HTT[redacted] 1820
```

Stolen Certificates

http://m.ytn.co.kr/news_view.php?s_mcd=0102&key=201602220213189044&pos=

Lazarus

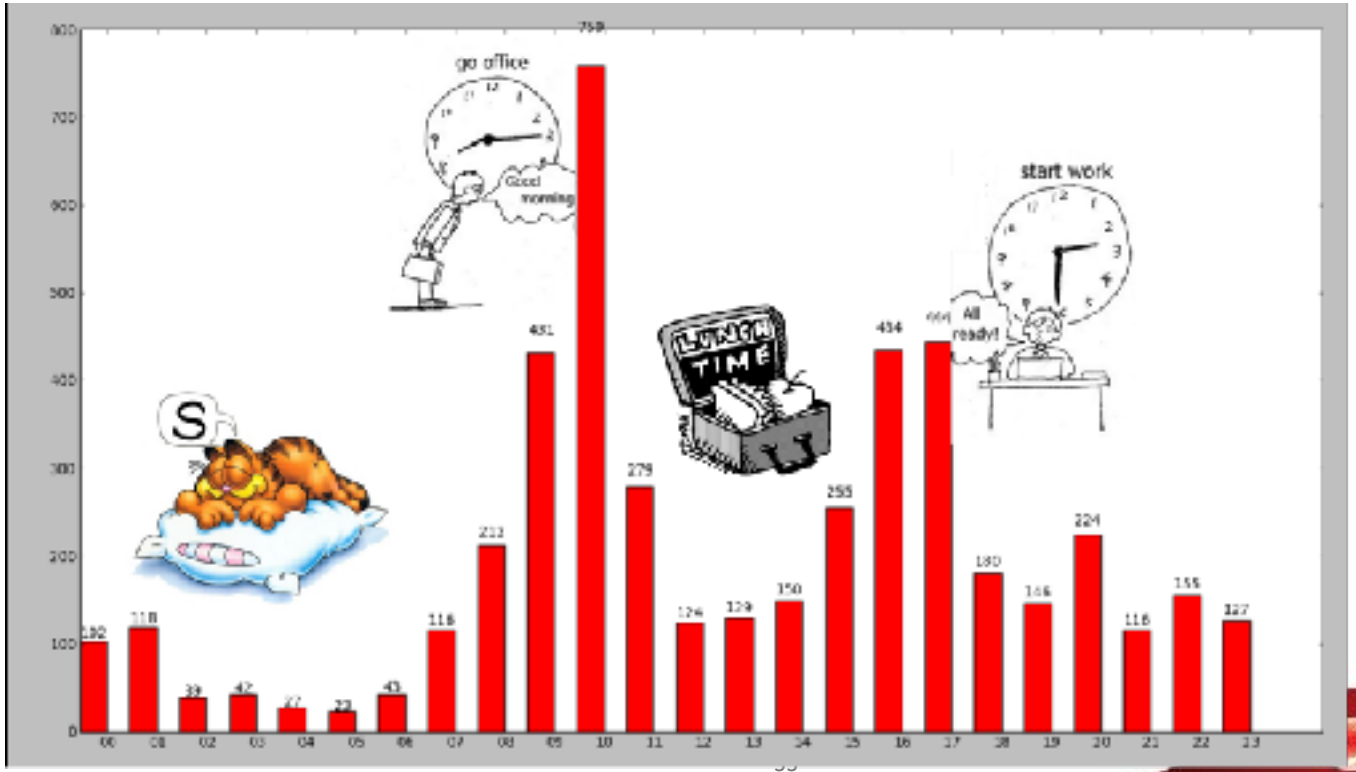
에서 제공하는 보안프로그램을 설치합니

Copyright	Copyright (C) 2017
Product	Remote
Original name	NHEnrollMon.exe
Internal name	NHEnrollMon.exe
File version	1.0.0.1
Description	RemoteMonitor
Signature verification	Certificate out of its validity period
Signers	[+] Everyzone Inc.

7c77ec259162872bf9ab18f6754e0e844157b31b32b4a746484f444b9f9a3836

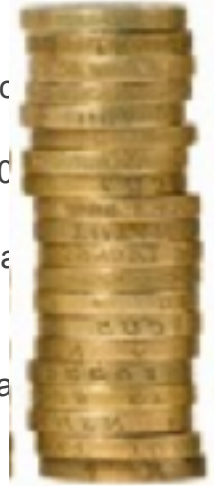
Time attributions

Source: Blackhat 2013 US: [HUNTING THE SHADOWS: IN DEPTH ANALYSIS OF ESCALATED APT ATTACKS]



Timestamps: Lazarus (timestamps in UTC)

Time Stamp : 2016:10:17 21:01:44+08:00 09a9ce7b2f443f9192007000c3cceed481be0e80
Time Stamp : 2016:10:20 14:30:05+08:00 52de4a4a2bdc7dc5c64bb5b6032df6ffd37c512c694993c337d6913eab316d78
Time Stamp : 2016:10:20 14:30:05+08:00 53da95da2842fb3a84aba16a4d2b346b2308e832d69dd4034f9b98880f7c51c2
Time Stamp : 2016:10:20 14:30:05+08:00 fbc9e003690727f3bff6957beabad58b018c00b7
Time Stamp : 2016:10:21 12:07:39+08:00 2c6c244b3858ce06a0b646ae386f65e69ae5c046
Time Stamp : 2016:10:21 12:07:39+08:00 95c8ffe03547bcb0afd4d025fb14908f5230c6dc6fdd16686609681c7f40ac
Time Stamp : 2016:10:27 10:31:55+08:00 09c1756064f15fcdd29ff8f239b3d5dcc22ac492
Time Stamp : 2016:10:27 10:31:55+08:00 825624d8a93c88a811262bd32cc51e19538c5d65f6f9137e30e72c5de4f0
Time Stamp : 2016:10:27 11:55:43+08:00 178994ab2d4fc0a32a328e97d7d220c8bbb9150c
Time Stamp : 2016:10:27 11:55:43+08:00 99017270f0af0e499cfeb19409020bfa0c2de741e5b32b9f6a01c34fe13fda
Time Stamp : 2016:11:04 09:29:03+08:00 97a3698ffffdb63df79faeaf58169f9755db1f90
Time Stamp : 2017:01:19 03:24:20+08:00 2c2fb1149c819456a51a75fe310a3a24b28a98d8
Time Stamp : 2017:01:19 03:24:20+08:00 7c77ec259162872bf9ab18f6754e0e844157b31b32b4a746484f444b9f9a
Time Stamp : 2017:01:19 03:24:20+08:00 884e06c3ff0781fcd9fb995cd746051c6f8293d3
Time Stamp : 2017:01:19 03:24:20+08:00 da967dc59a7b61aeaeaee380b2c147c5bb1b3bc5
Time Stamp : 2017:01:22 23:40:03+08:00 4d1f7e9405e4129134856a9d535bd5bc369a80ca



Language encodings: Lazarus PE binaries

```
ID 3, ID 1          RT_ICON          0x1ffc4     0x468    KOREAN, KOREAN          Thu Jan  1 00:00:00 1970
ID 3, ID 2          RT_ICON          0x204Zc     0x10a8   KOREAN, KOREAN          Thu Jan  1 00:00:00 1970
ID 11, ID 1         RT_MESSAGETABLE  0x22d08     0x3c     KOREAN, KOREAN          Thu Jan  1 00:00:00 1970
ID 14, ID 128       RT_GROUP_ICON    0x22e80     0x22     KOREAN, KOREAN          Thu Jan  1 00:00:00 1970
ID 16, ID 1         RT_VERSION       0x23160     0x2fc    KOREAN, KOREAN          Thu Jan  1 00:00:00 1970
```

Number of PE resources by language

ENGLISH US	49
KOREAN	5

hash: b84ce7a73e02e9069a9a9e6b91608bdd5450226b

Attribution to Russophone actors in Lazarus

Do you speak russian? ;)

```
vaddr=0x0045e620 paddr=0x0005d220 ordinal=1046 sz=20 len=19 section=.rdata type=a string=kliyent2podkly
vaddr=0x0045e634 paddr=0x0005d234 ordinal=1047 sz=7 len=6 section=.rdata type=a string=ssylka
vaddr=0x0045e63c paddr=0x0005d23c ordinal=1048 sz=13 len=12 section=.rdata type=a string=ustanavlivat
vaddr=0x0045e64c paddr=0x0005d24c ordinal=1049 sz=9 len=8 section=.rdata type=a string=poluchit
vaddr=0x0045e658 paddr=0x0005d258 ordinal=1050 sz=9 len=8 section=.rdata type=a string=pereslat
vaddr=0x0045e664 paddr=0x0005d264 ordinal=1051 sz=8 len=7 section=.rdata type=a string=derzhat
vaddr=0x0045e66c paddr=0x0005d26c ordinal=1052 sz=9 len=8 section=.rdata type=a string=vykhodit
vaddr=0x0045e678 paddr=0x0005d278 ordinal=1053 sz=8 len=7 section=.rdata type=a string=Nachalo
```


Lazarus: Hints to Korea

Interesting encoding error was discovered by Kaspersky Labs:
c05329f101979fa75ca297c4f77c8cd69fe8eb499d4f693550b734beb9f564b9

```
Language Code                   : English (U.S.)
Character Set                   : Unicode
Comments                        :
Company Name                    : Microsoft Corporc
File Description                : File Compress Uti
File Version                    : 5.1.2600.0 (xpcli
Internal Name                   : COMPACT.EXE
Legal Copyright                 : ¨Ï Microsoft Corp
```

FileVersionInfo properties

Copyright	¨Ï Microsoft Corporation.
Product	Microsoftçç Windows¢ç
Internal name	COMPACT.EXE
File version	5.1.2600.0 (xpclient.010817-1148)
Description	File Compress Utility

Unicode Encoding error..

```
000182a0  70 00 79 00 72 00 69 00  67 00 68 00 74 00 00 00  |p.y.r.i.g.h.t...|
000182b0  a8 00 cf 00 20 00 4d 00  69 00 63 00 72 00 6f 00  |.... .M.i.c.r.o.|
000182c0  73 00 6f 00 66 00 74 00  20 00 43 00 6f 00 72 00  |s.o.f.t. .C.o.r.|
000182d0  70 00 6f 00 72 00 61 00  74 00 69 00 6f 00 6e 00  |p.o.r.a.t.i.o.n.|
```

EUC-KR Encoding table: A8CF is .. ©

A8C0	㉮	㉯	㉰	㉱	㉲	㉳	㉴	㉵	㉶	㉷	㉸	㉹	㉺	ⓐ	ⓑ	ⓒ
A8D0	ⓓ	ⓔ	ⓕ	ⓖ	ⓗ	ⓘ	ⓙ	ⓚ	ⓛ	ⓜ	ⓝ	ⓞ	ⓟ	ⓠ	ⓡ	ⓢ
A8E0	ⓣ	ⓤ	ⓥ	ⓦ	ⓧ	ⓨ	ⓩ	①	②	③	④	⑤	⑥	⑦	⑧	⑨
A8F0	⑩	⑪	⑫	⑬	⑭	⑮	½	⅓	⅔	¼	¾	⅛	⅜	⅝	⅞	

Bad Opsec: Operation Hangover

```
HACKERSCOUNCIL.COM

Registrant:
     Appin Technologies
     Rakesh Gupta          (rakesh.gupta@appinonline.com)
     9th Floor, Metro Heights,NSP, PitamPura,
     Delhi
     Delhi,110034
     IN
     Tel. +91.1147063300


Creation Date: 17-Sep-2009
Expiration Date: 17-Sep-2011
```

R:\payloads**lta nagar**\Uploader\HangOver 1.5.7 (Startup)\HangOver 1.5.7 (Startup)\Release\Http
C:\Users**neeru rana**\Desktop\Klogger - 30 may\Klogger - 30 may\Release\Klogger.pdb
C:\Users**Yash**\Desktop\New folder\HangOver 1.5.7 (Startup) uploader\Release\Http_r.pdb

www.**noavi.org**/cl_editorial_13/hang_over_report_appin.pdf

« Older: Cyberattack against Israeli and Palestinian targets for a year

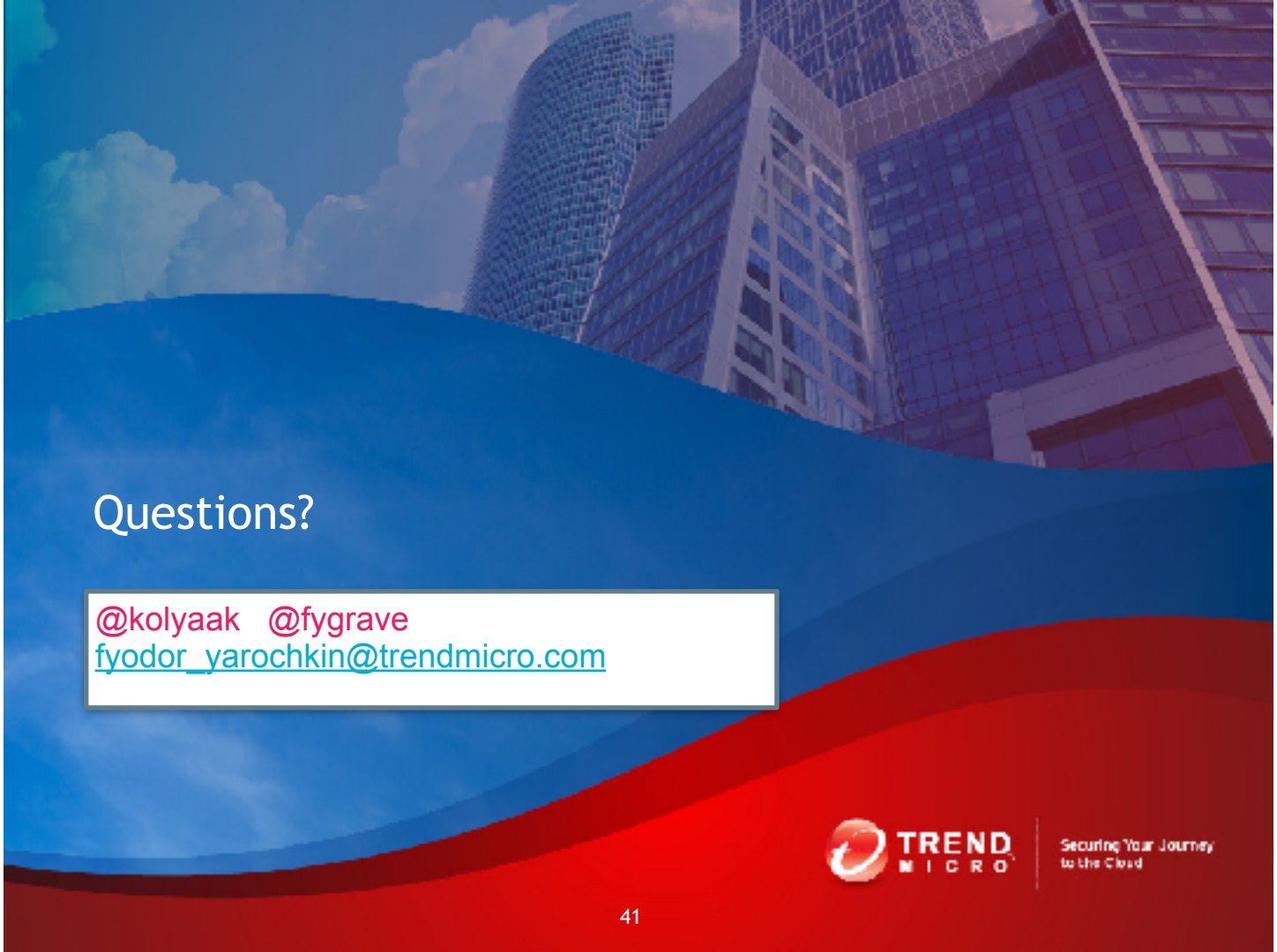
THE HANGOVER REPORT

May 20, 2013 by Snorre Fagerland - 2 Comments

Unveiling an Indian Cyberattack Infrastructure

whowas #badrabbit

```
http://www.publicdomainregistry.com
Registrant Name: Choliev Aleksandr
Registrant Organization:
Registrant Street: Stroitelnaya d. 14 korp. 4 kv. 5
Registrant City: Jukovskij
Registrant State/Province: Moskovskaya oblast
Registrant Postal Code: 140180
Registrant Country: RU
Registrant Phone: +7.9875135246
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email:
```


Questions?
@kolyaak @fygrave
fyodor_yarochkin@trendmicro.com
TREND MICRO
Securing Your Journey to the Cloud