Threat Intelligence на страже интересов государства. Как найти атаку в стоге сена?

Биль Олег Викторович –
главный архитектор (руководитель)
Лаборатории исследования вредоносного кода
РГП «Государственная техническая служба»

Обо мне.

Место работы: РГП «Государственная техническая служба»,

Основные достижения в сфере ИБ:

- Подготовил троих студентов к участию в конференции по ИБ, проводимой Лабораторией Касперского (2010-2012 годы) в г. Москва. Результат: два призера (третье и второе места) тура Россия и СНГ и участие в международных турах (Польша, Германия);
- Вошел в состав финалистов конкурса «Инновационный Казахстан» (АО «Самрук-Казына», 2011);
- Вошел в число победителей конкурса по анализу CrackMe, проводимого Лабораторией Касперского (2016);
- Консультировал работы по противодействию троянцам-шифровальщикам (Talent Lab, Лаборатория Касперского – специальный приз) (март 2017) и защите данных от потенциально опасных расширений браузера (обе работы презентовались на секции Young School конференции Positive Hack Days 2017) (апрель-май 2017);
- Выступал на конференциях PHDays (Positive Technologies, 2018, Москва), BISSummit (Infowatch, 2018, Баку) и ряде конференций в Казахстане (SOC-форум, Kazhackstan и др.).

Возможности решения

1. Отчеты о целевых угрозах (APT);
2. Песочница;
3. Информация о доменах и IP-адресах;
4. Информация об объектах и их взаимосвязях.

Отчеты о целевых угрозах

APT10 Spearphishes Japanese Policy Experts late 2016 to early 2017

Version: 1.0 (9.March.2017)

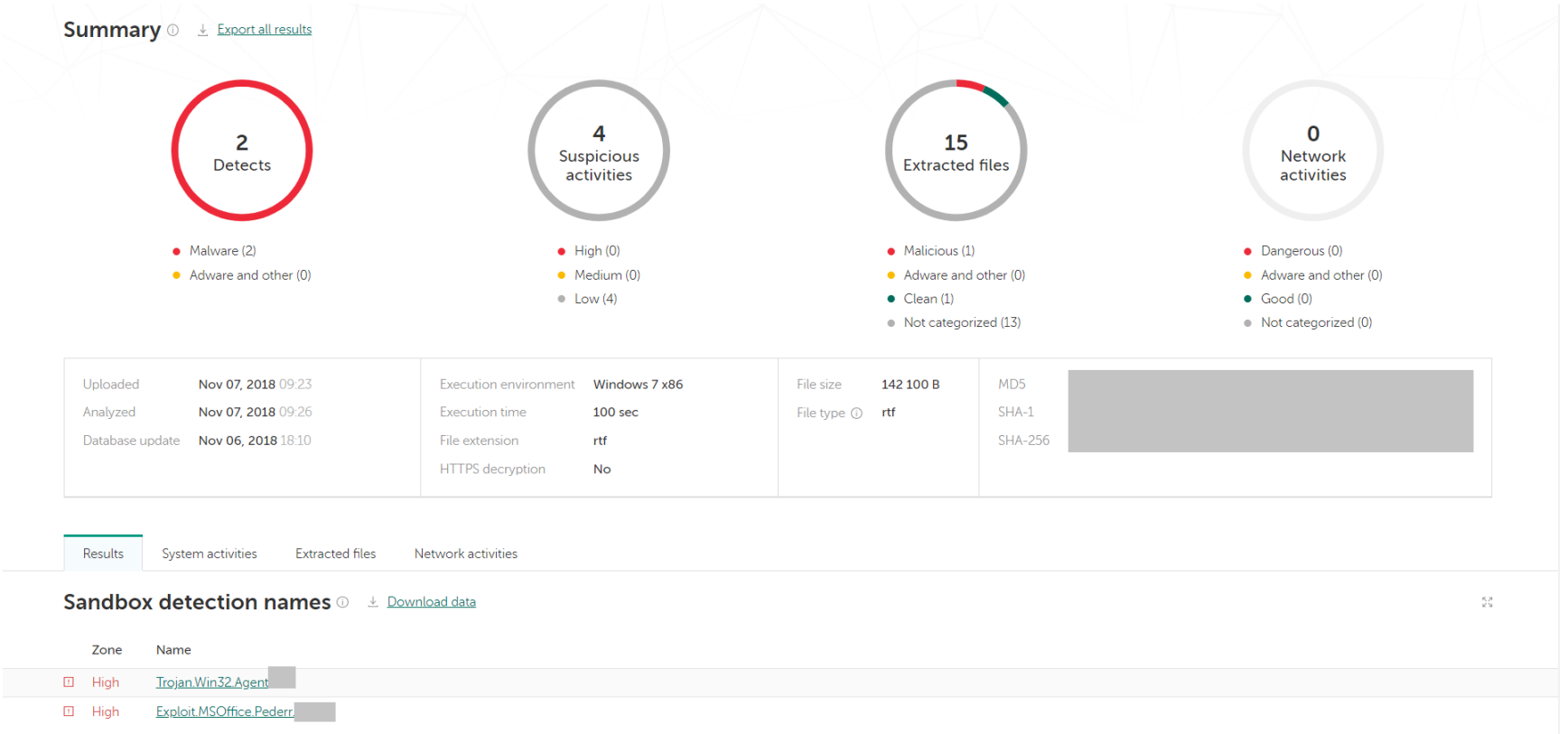
Executive summary

In late January 2017, JPCERT/CC reported a spearphishing campaign and related backdoor which they named “ChChes”. The campaign, which we have high confidence was carried out by the APT10 actor, targeted multiple Japanese organizations. Several reports on the attacks have surfaced.

The largest amount of ChChes spearphishing activity appears to have occurred in the last week of November 2016, and continues into the first week of December 2016. Following the spearphishing campaign, the group shifted toward to Powershell and other tools that will be covered in greater detail in a second part of this report.

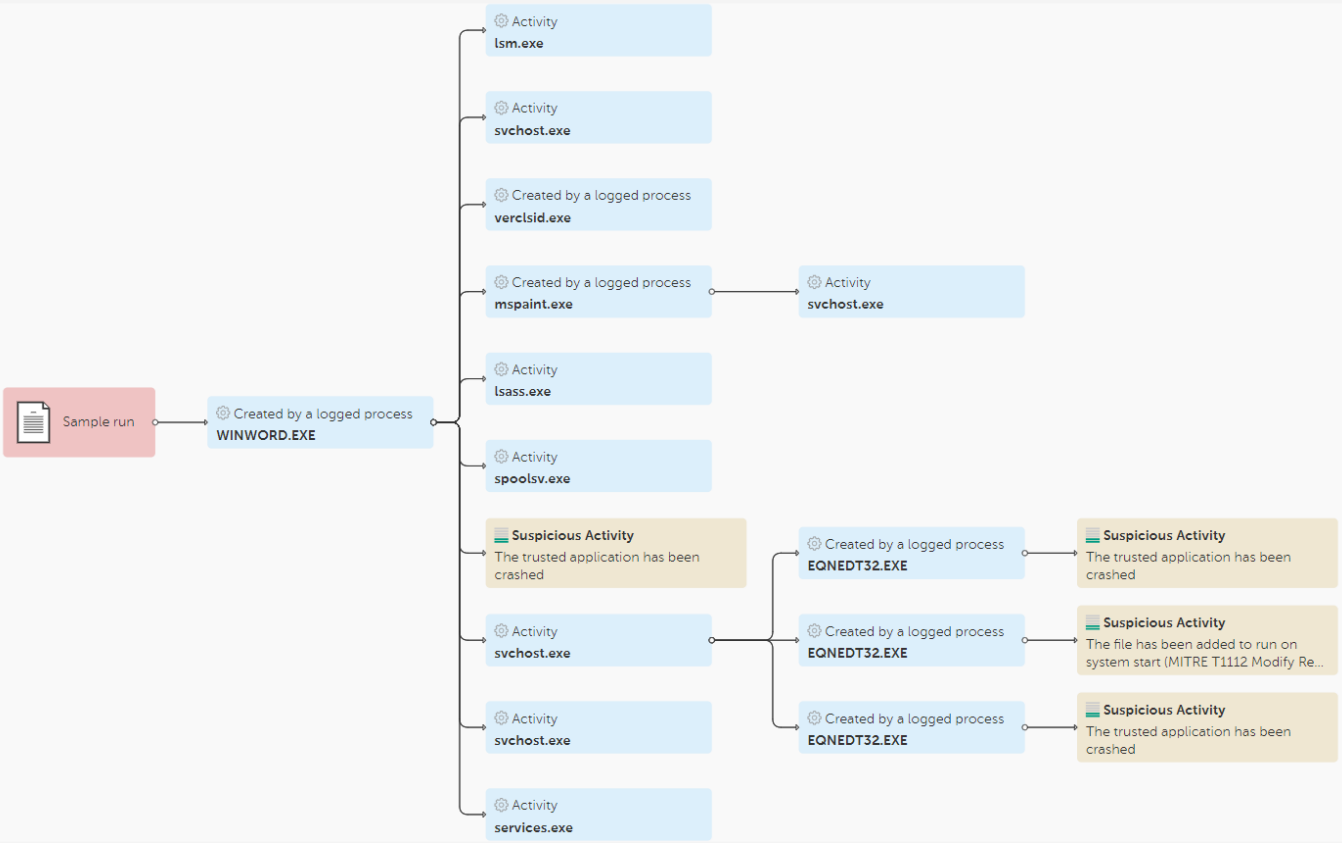
```
<IndicatorItem id="58c19f89-0220-4524-ad11-4f5cc0a85a10" condition="is">
  <Context document="RouteEntryItem" search="RouteEntryItem/Destination" type="mir" />
  <Content type="string">whale.toshste.com</Content>
</IndicatorItem>
<IndicatorItem id="58c19f89-7e98-47ac-b8f9-4f5cc0a85a10" condition="is">
  <Context document="RouteEntryItem" search="RouteEntryItem/Destination" type="mir" />
  <Content type="string">zebra.wthelpdesk.com</Content>
</IndicatorItem>
<IndicatorItem id="58c19f89-7fc4-4f90-ab0d-4f5cc0a85a10" condition="is">
  <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
  <Content type="md5">07abd6583295061eac2435ae470eff78</Content>
</IndicatorItem>
<IndicatorItem id="58c19f89-38d0-4620-9f83-4f5cc0a85a10" condition="is">
  <Context document="FileItem" search="FileItem/Sha256sum" type="mir" />
  <Content type="sha256">efa0b414a831cbf724d1c67808b7483dec22a981ae670947793d114048f88057</Content>
</IndicatorItem>
```

Песочница

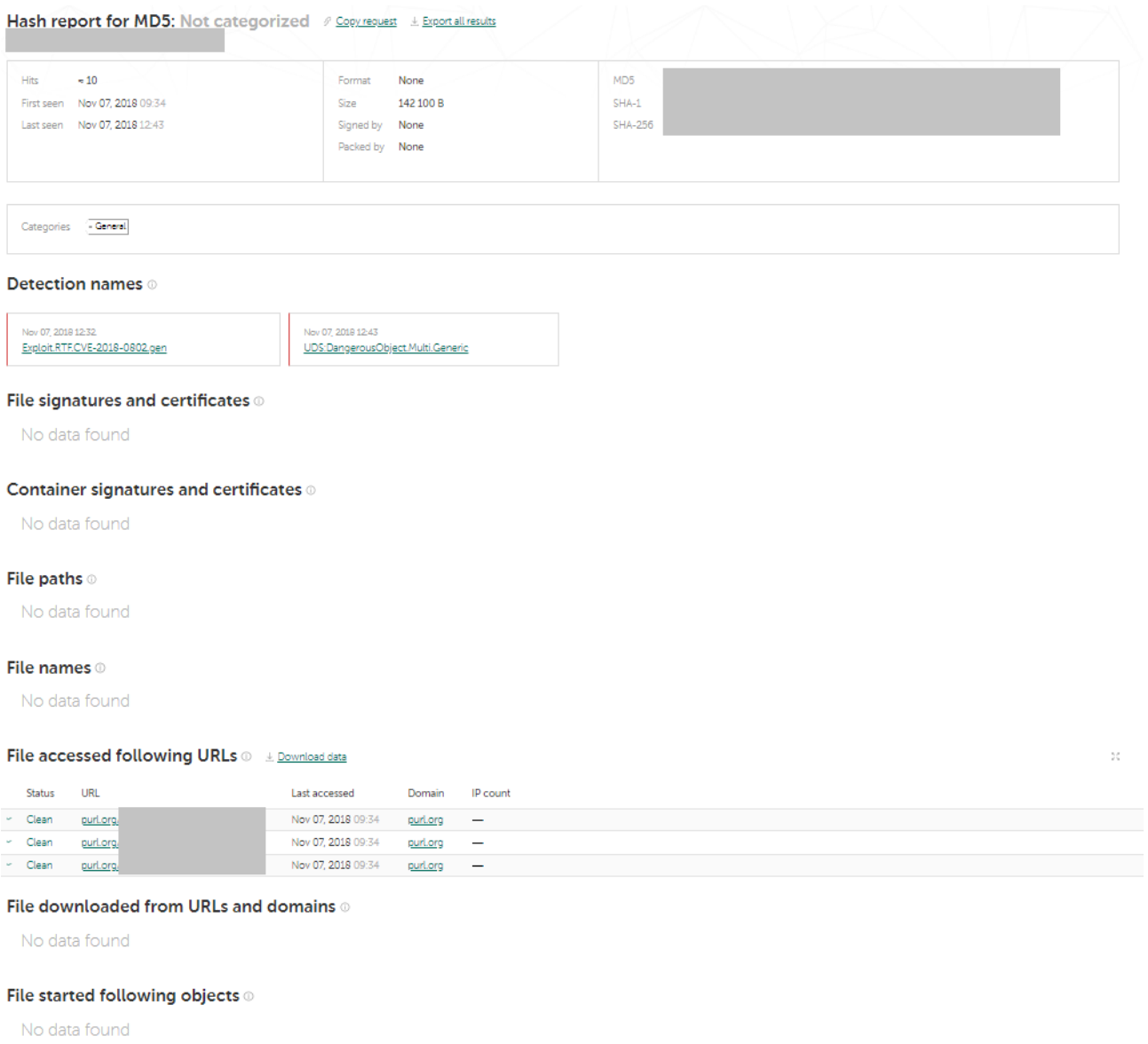

Summary
Export all results
2
Detects
Malware (2)
Adware and other (0)
4
Suspicious activities
High (0)
Medium (0)
Low (4)
15
Extracted files
Malicious (1)
Adware and other (0)
Clean (1)
Not categorized (13)
0
Network activities
Dangerous (0)
Adware and other (0)
Good (0)
Not categorized (0)
Uploaded Nov 07, 2018 09:23
Analyzed Nov 07, 2018 09:26
Database update Nov 06, 2018 18:10
Execution environment Windows 7 x86
Execution time 100 sec
File extension rtf
HTTPS decryption No
File size 142 100 B
File type rtf
MD5
SHA-1
SHA-256
Results
System activities
Extracted files
Network activities
Sandbox detection names
Download data
Zone
Name
High
Trojan.Win32.Agent
High
Exploit.MSOffice.Pederr

Песочница

Execution map



Песочница + информация об объектах



Hash report for MD5: Not categorized Copy request Export all results

[redacted]

Hits	≈ 10	Format	None	MD5	[redacted]
First seen	Nov 07, 2018 09:34	Size	142 100 B	SHA-1	
Last seen	Nov 07, 2018 12:43	Signed by	None	SHA-256	
		Packed by	None		

Categories: General

Detection names

Nov 07, 2018 12:32 Exploit.RTF.CVE-2018-0802.gen	Nov 07, 2018 12:43 UDS:DangerousObject.Multi.Generic

File signatures and certificates

No data found

Container signatures and certificates

No data found

File paths

No data found

File names

No data found

File accessed following URLs Download data

Status	URL	Last accessed	Domain	IP count
Clean	purl.org/[redacted]	Nov 07, 2018 09:34	purl.org	—
Clean	purl.org/[redacted]	Nov 07, 2018 09:34	purl.org	—
Clean	purl.org/[redacted]	Nov 07, 2018 09:34	purl.org	—

File downloaded from URLs and domains

No data found

File started following objects

No data found

Информация об объектах

Report for URL: Dangerous

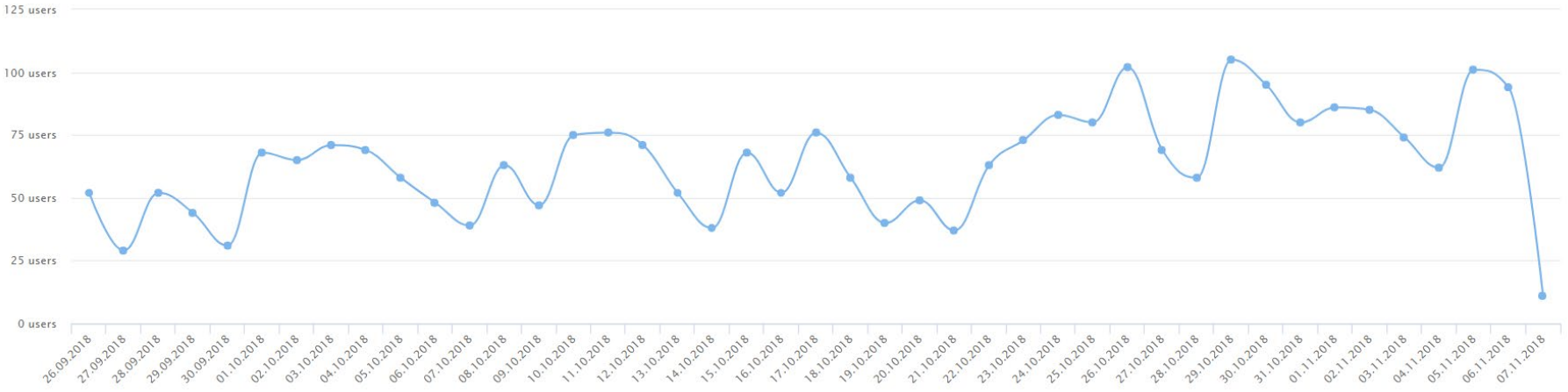
Copy request Export all results

138.[redacted]nme.gif

IPv4 count	–	Owner name	Abuse	Created	May 05, 2014
Files count	1 000	Owner ID	None	Updated	Nov 08, 2017

Categories: Botnet C&C Trojan.Win32.Lethic; Malware

Anti-Virus Statistics



Информация об объектах

Files downloaded from requested URL

Download data

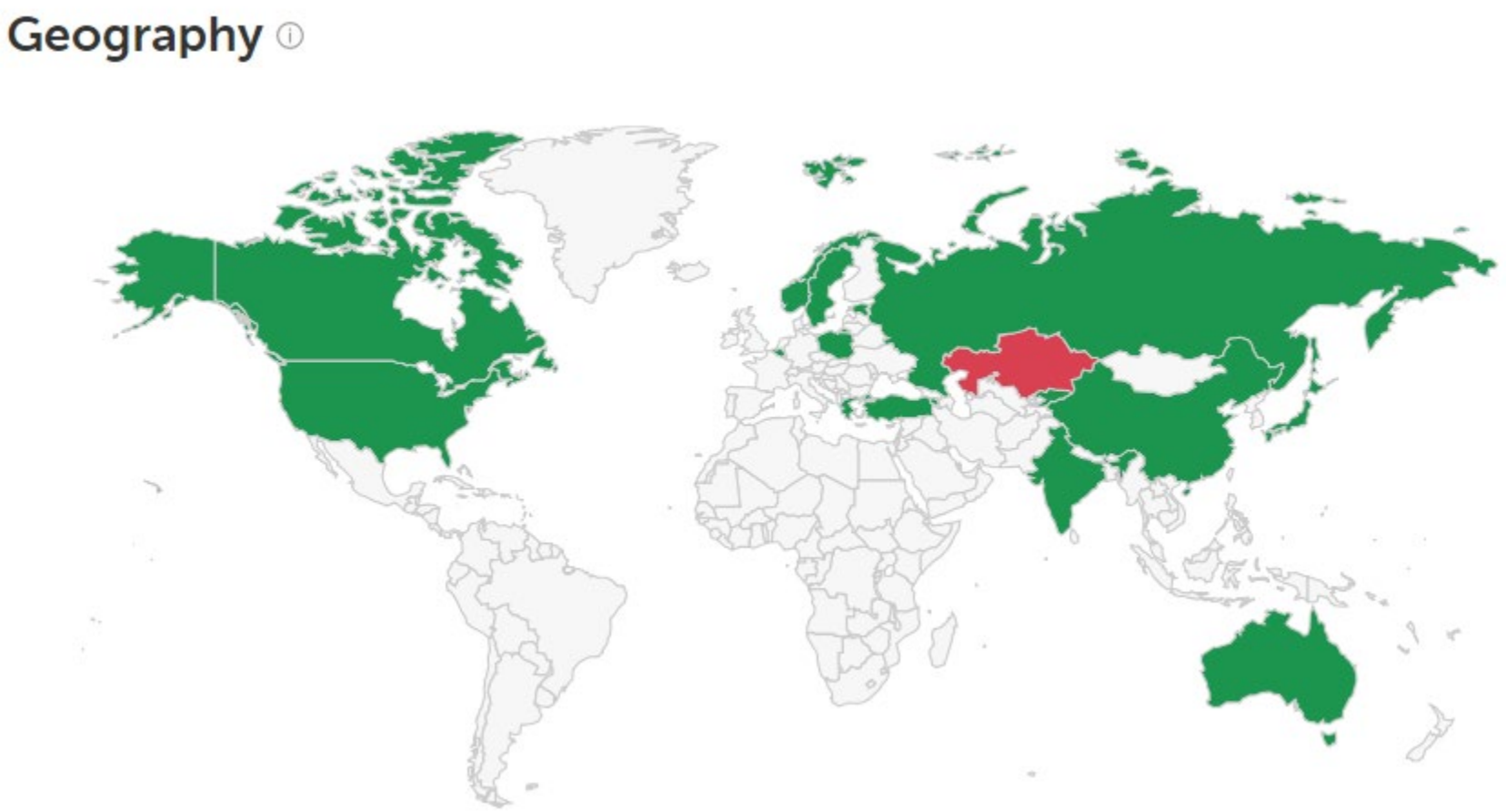
Status	Hits (≈)	File MD5	First downloaded	Last downloaded	Detection name
Malware	1000	252D7	Oct 15, 2018 02:56	Oct 24, 2018 20:24	HEUR:Trojan.Win32.Khalesi.gen
Malware	1000	8CE44	Oct 11, 2018 10:46	Nov 02, 2018 19:51	HEUR:Trojan.Win32.Khalesi.gen
Malware	1000	5F437	Oct 12, 2018 15:07	Nov 02, 2018 12:43	HEUR:Trojan.Win32.Khalesi.gen
Malware	1000	88612	Oct 21, 2018 08:36	Nov 05, 2018 02:42	HEUR:Trojan.Win32.Khalesi.gen
Malware	1000	7CEC4	Oct 16, 2018 08:32	Oct 18, 2018 20:37	HEUR:Trojan.Win32.Khalesi.gen
Malware	1000	627AD	Oct 13, 2018 20:55	Oct 18, 2018 14:52	HEUR:Trojan.Win32.Khalesi.gen
Malware	1000	489A5	Oct 18, 2018 20:37	Oct 29, 2018 21:47	HEUR:Trojan.Win32.Khalesi.gen
Malware	1000	2033F	Oct 20, 2018 02:36	Oct 21, 2018 08:11	HEUR:Trojan.Win32.Khalesi.gen
Malware	1000	3BD5A	Oct 25, 2018 03:56	Nov 05, 2018 02:42	HEUR:Trojan.Win32.Khalesi.gen
Malware	1000	24D2B	Oct 26, 2018 04:26	Oct 28, 2018 13:52	HEUR:Trojan.Win32.Khalesi.gen

Files accessed requested URL

Download data

Status	Hits (≈)	File MD5	First accessed	Last accessed	Detection name
Malware	10000	0711A	Oct 09, 2018 22:11	Nov 06, 2018 20:26	Trojan.Win32.Lethic
Malware	1000	FF464	Oct 09, 2018 22:11	Nov 06, 2018 08:11	Trojan.Win32.Lethic
Malware	1000	F5D8E	Oct 09, 2018 22:11	Nov 06, 2018 09:31	Trojan.Win32.Lethic
Malware	1000	544CF	Oct 09, 2018 21:01	Nov 06, 2018 19:21	Trojan.Win32.Lethic
Malware	1000	83436	Oct 09, 2018 22:11	Nov 06, 2018 20:21	Trojan.Win32.Lethic
Malware	1000	71AC5	Oct 09, 2018 23:46	Nov 06, 2018 08:06	Trojan.Win32.Lethic
Malware	1000	C5D72	Oct 09, 2018 22:11	Nov 06, 2018 22:41	Trojan.Win32.Lethic
Malware	1000	96FF9	Oct 09, 2018 22:11	Nov 06, 2018 08:06	Trojan.Win32.Lethic
Malware	1000	23871	Oct 09, 2018 22:11	Nov 06, 2018 13:41	Trojan.Win32.Lethic
Malware	1000	88612	Oct 25, 2018 15:23	Oct 25, 2018 15:23	HEUR:Trojan.Win32.Khalesi.gen

Информация об объектах – бывает и такое ☺



Тятя! Тятя! Наши сети (изолированные)…

Может скрывать файлы на флеш-дисках, модифицируя структуры данных файловой системы.

Может передавать данные и файлы в и из изолированных сетей.

Может получать дополнительные программные модули и исполнять их.

Количество промежуточных компьютеров в цепочке – не имеет значения!

Картинка: https://www.innovauk.com

E-mail:
o_bil@sts.kz
o_bil@kz-cert.kz

Web:
www.sts.kz
www.kz-cert.kz

Call-center:
1400