Watering hole” threat analysis in the government sector of Kazakhstan

tntsecure.kz/en/article_7.html

While studying the threat landscape of Kazakhstan as a part of the Threat Intelligence phase, T&T Security experts discovered the so-called Razy malware family. The investigated samples of the Razy family apparently were used to infect users in the form of a Trojan downloader masquerading as a regular office document (Word, Excel and Adobe PDF). Attackers usually spread Razy using a “Watering hole” attack.

The “Watering hole” is an attack where attackers locate malware on a legitimate, possibly previously hacked, site visited by a potential victim.

Thus the attacker achieves the trustworthiness effect since the link to the malicious file will likely be on a victim’s list of trusted sites.

Two of the analysed cases caught our sharp attention, in which the attackers spread the malware using the watering hole attack on the e-government portal (egov.kz).
Malicious links:

- hxxps://legalacts.egov.kz/application/downloadnpa?id=5322314
- hxxps://budget.egov.kz/budgetfile/file?fileId=1520392

At the same time, the second malicious Razy sample (at budget.egov.kz) was still available for download on the site at the time of detection.

The files are the same malicious Razy Trojan downloader. We assume that cybercriminals published the malicious software under the pretence of office documents by gaining access to uploading files to the legalacts.egov.kz and budget.egov.kz. The first document is a resolution of the district administration. The second, created in 2021, is a financial summary of the administration's budget. That implies the attacker posted the Razy malware in 2021, accordingly.

We assume that these attacks targeted specific companies that may be using these documents. And most likely, the attackers did not aim for the mass attack on the citizens of Kazakhstan, and the public exposure of the samples themselves is most likely a side effect. The rest of the Razy samples are also documents of different kinds, e.g. the resolution of the district administration. That means cybercriminals look for the documents suitable for the victim and embed them into the final malicious file.

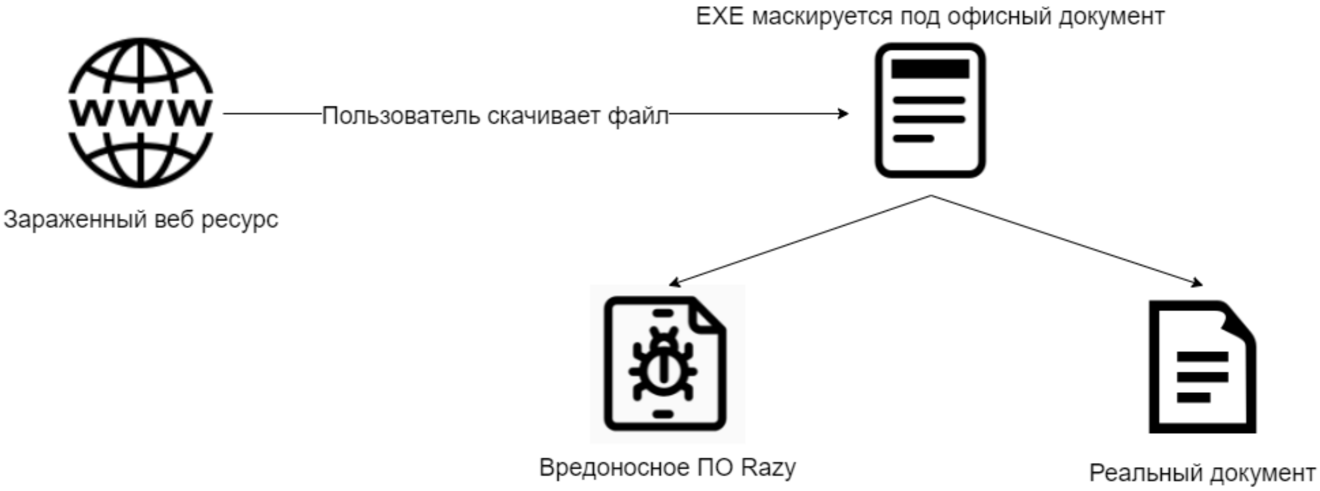
One should note, by the time of publication, the malware control server (C&C server) has already been disabled, and that is currently, these samples cannot load any additional malicious functionality.

Together with the accountable employees of Zerde National Information & Communication Holding JSC, the T&T Security team worked to detect the Razy related incidents and block the caused spreading of malicious content.

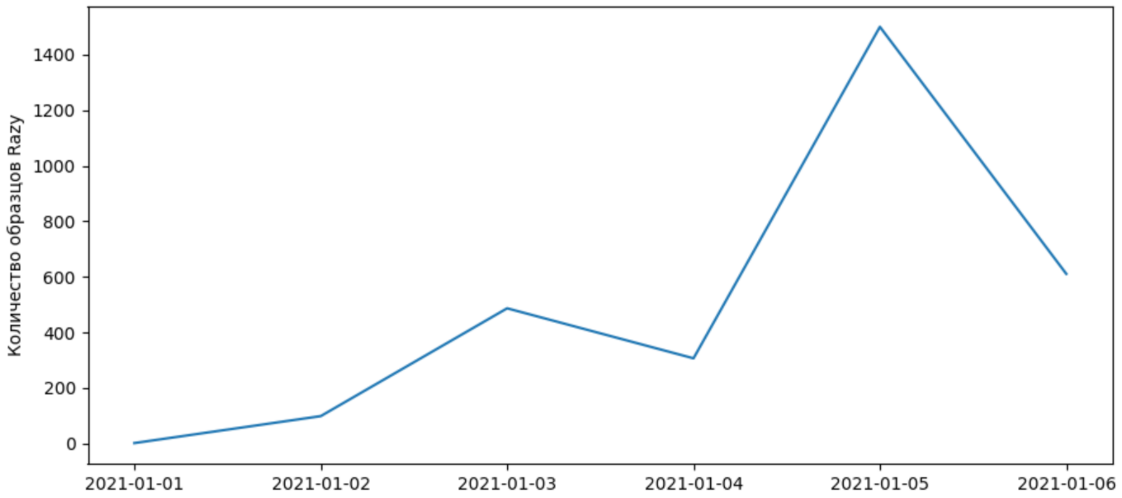
tLab successfully detects and blocks this threat, which can be seen in the video below. tLab works on the principle of zero trust based on deep behavioral analysis, and high throughput allows you to analyze tens of thousands of files per day without filters and whitelisting, then our solution effectively blocks such threats even using an attack at the watering hole. Since tLab is used as part of the Cyber Shield of the Republic of Kazakhstan, we can say that the state is ready to repel such threats.

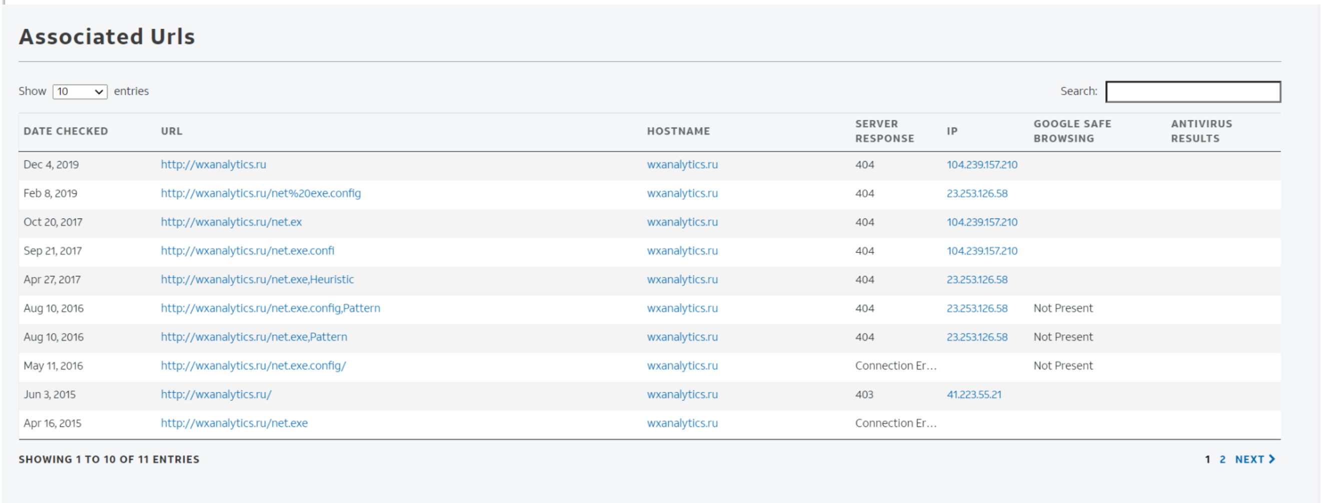
Samples technical analysis

Razy, first spotted in 2015, has been used for attacks to these days. Below is a diagram of how Razy works. One can see that when a user launches a sample, a malicious payload gets activated, and an actual legitimate document embedded in malware pops up.


EXE маскируется под офисный документ
Пользователь скачивает файл
Зараженный веб ресурс
Вредоносное ПО Razy
Реальный документ

T&T Security monitored the monthly amounts of Razy malware samples found on Virustotal and discovered a sharp increase in May 2021. Most of the detected malware samples to target Kazakhstan belong to the same period. That is, the embedded documents come from the Kazakh institutions.





Associated Urls

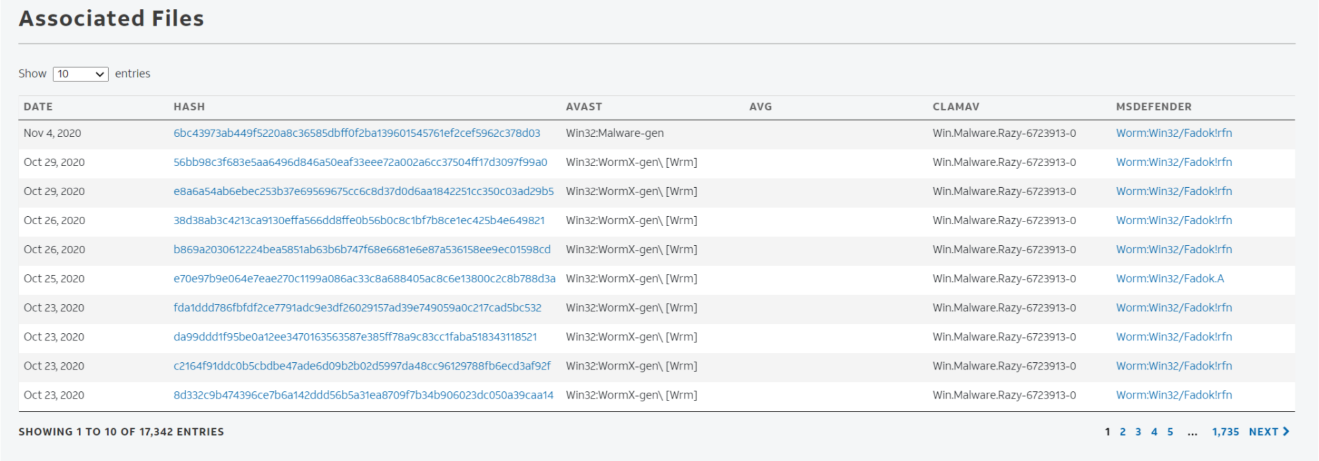
Show 10 entries

Search:

DATE CHECKED	URL	HOSTNAME	SERVER RESPONSE	IP	GOOGLE SAFE BROWSING	ANTIVIRUS RESULTS
Dec 4, 2019	http://wxanalytics.ru	wxanalytics.ru	404	104.239.157.210		
Feb 8, 2019	http://wxanalytics.ru/net%20exe.config	wxanalytics.ru	404	23.253.126.58		
Oct 20, 2017	http://wxanalytics.ru/net.ex	wxanalytics.ru	404	104.239.157.210		
Sep 21, 2017	http://wxanalytics.ru/net.exe.confi	wxanalytics.ru	404	104.239.157.210		
Apr 27, 2017	http://wxanalytics.ru/net.exe,Heuristic	wxanalytics.ru	404	23.253.126.58		
Aug 10, 2016	http://wxanalytics.ru/net.exe.config,Pattern	wxanalytics.ru	404	23.253.126.58	Not Present	
Aug 10, 2016	http://wxanalytics.ru/net.exe,Pattern	wxanalytics.ru	404	23.253.126.58	Not Present	
May 11, 2016	http://wxanalytics.ru/net.exe.config/	wxanalytics.ru	Connection Er…		Not Present	
Jun 3, 2015	http://wxanalytics.ru/	wxanalytics.ru	403	41.223.55.21		
Apr 16, 2015	http://wxanalytics.ru/net.exe	wxanalytics.ru	Connection Er…			

SHOWING 1 TO 10 OF 11 ENTRIES

Razy stats from alienvault.com
(2015 - 2019)



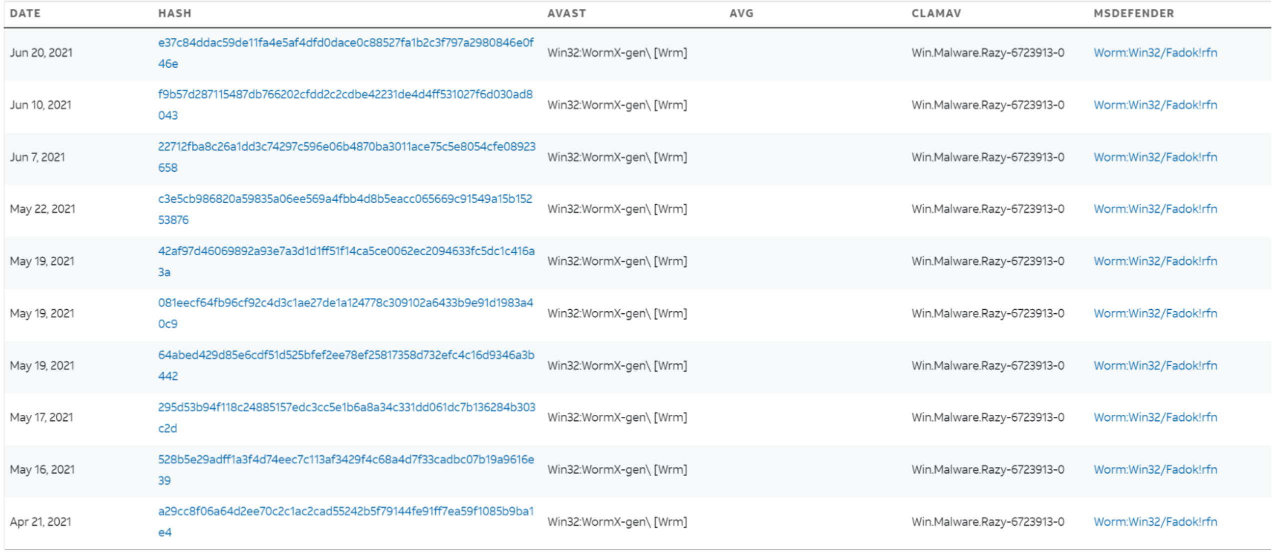
Associated Files

Show 10 entries

DATE	HASH	AVAST	AVG	CLAMAV	MSDEFENDER
Nov 4, 2020	6bc43973ab449f5220a8c36585dbff0f2ba139601545761ef2cef5962c378d03	Win32:Malware-gen		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
Oct 29, 2020	56bb98c3f683e5aa6496d846a50eaf33eee72a002a6cc37504ff17d3097f99a0	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
Oct 29, 2020	e8a6a54ab6ebec253b37e69569675cc6c8d37d0d6aa1842251cc350c03ad29b5	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
Oct 26, 2020	38d38ab3c4213ca9130effa566dd8ffe0b56b0c8c1bf7b8ce1ec425b4e649821	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
Oct 26, 2020	b869a2030612224bea5851ab63b6b747f68e6681e6e87a536158ee9ec01598cd	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
Oct 25, 2020	e70e97b9e064e7eae270c1199a086ac33c8a688405ac8c6e13800c2c8b788d3a	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok.A
Oct 23, 2020	fda1ddd786fbfdf2ce7791adc9e3df26029157ad39e749059a0c217cad5bc532	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
Oct 23, 2020	da99ddd1f95be0a12ee3470163563587e385ff78a9c83cc1faba518343118521	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
Oct 23, 2020	c2164f91ddc0b5cbdbe47ade6d09b2b02d5997da48cc96129788fb6ecd3af92f	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
Oct 23, 2020	8d332c9b474396ce7b6a142ddd56b5a31ea8709f7b34b906023dc050a39caa14	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn

SHOWING 1 TO 10 OF 17,342 ENTRIES

Razy stats from alienvault.com
(2020)



DATE	HASH	AVAST	AVG	CLAMAV	MSDEFENDER
Jun 20, 2021	e37c84ddac59de11fa4e5af4dfd0dace0c88527fa1b2c3f797a2980846e0f46e	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
Jun 10, 2021	f9b57d287115487db766202cfdd2c2cdbe42231de4d4ff531027f6d030ad8043	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
Jun 7, 2021	22712fba8c26a1dd3c74297c596e06b4870ba3011ace75c5e8054cfe08923658	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
May 22, 2021	c3e5cb986820a59835a06ee569a4fbb4d8b5eacc065669c91549a15b15253876	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
May 19, 2021	42af97d46069892a93e7a3d1d1ff51f14ca5ce0062ec2094633fc5dc1c416a3a	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
May 19, 2021	081eecf64fb96cf92c4d3c1ae27de1a124778c309102a6433b9e91d1983a40c9	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
May 19, 2021	64abed429d85e6cdf51d525bfef2ee78ef25817358d732efc4c16d9346a3b442	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
May 17, 2021	295d53b94f118c24885157edc3cc5e1b6a8a34c331dd061dc7b136284b303c2d	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
May 16, 2021	528b5e29adff1a3f4d74eec7c113af3429f4c68a4d7f33cadbc07b19a9616e39	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn
Apr 21, 2021	a29cc8f06a64d2ee70c2c1ac2cad55242b5f79144fe91ff7ea59f1085b9ba1e4	Win32:WormX-gen\ [Wrm]		Win.Malware.Razy-6723913-0	Worm:Win32/Fadok!rfn

Razy stats from alienvault.com
(2021)

We researched the following files.

- 2 6>10 @CA.exe

  SHA256: 20f7a8258f83862ae6638a6bd1ad0bc83d40928a89eb40c720934db9b65f4bec

- эльвира отчет.exe

  SHA256:
  b06e65a0009ae771566db075c0f5850799977b4a982d7d6a63565a184be60796

- Отчёт по практике.exe

  SHA256: 219c44420a95370a22ef806244033c2a21e94b7500fc780fc8e4f25183f745bc

- 24160712_ExSteppeEagle_INTSUM_S2_160X_E_O.exe

  SHA256:
  2F6C1C2C4043CA6D19ADDD60FA85A5AD6D347075E73AE1E1DCB76D5CC5224573

- eastmere vil.exe

  SHA256:
  7615E69D6FA11FC851C4CD10DDEE3820ACFC6170578C61AE74B6D4FD8EA71E10

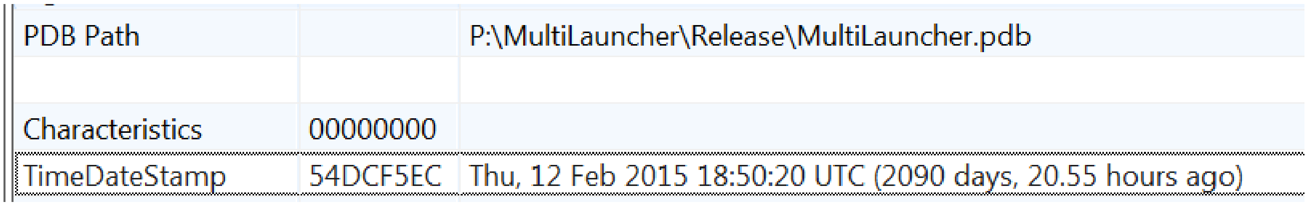
- OWNSITREP 241700AJUL16 G3.exe

  SHA256:
  8FA473C03850B22C2C6AADCFE69268BE4E4C7A33881581FEA83789755AF8F22A

- 61c98d12-06b1-4f5d-9c12-ace5630dcc07

  SHA256:
  3ED1B88C9AE34BA4FFBF8AED737F2DC9A0AEDEEDF8D2A4A69555518845E16264

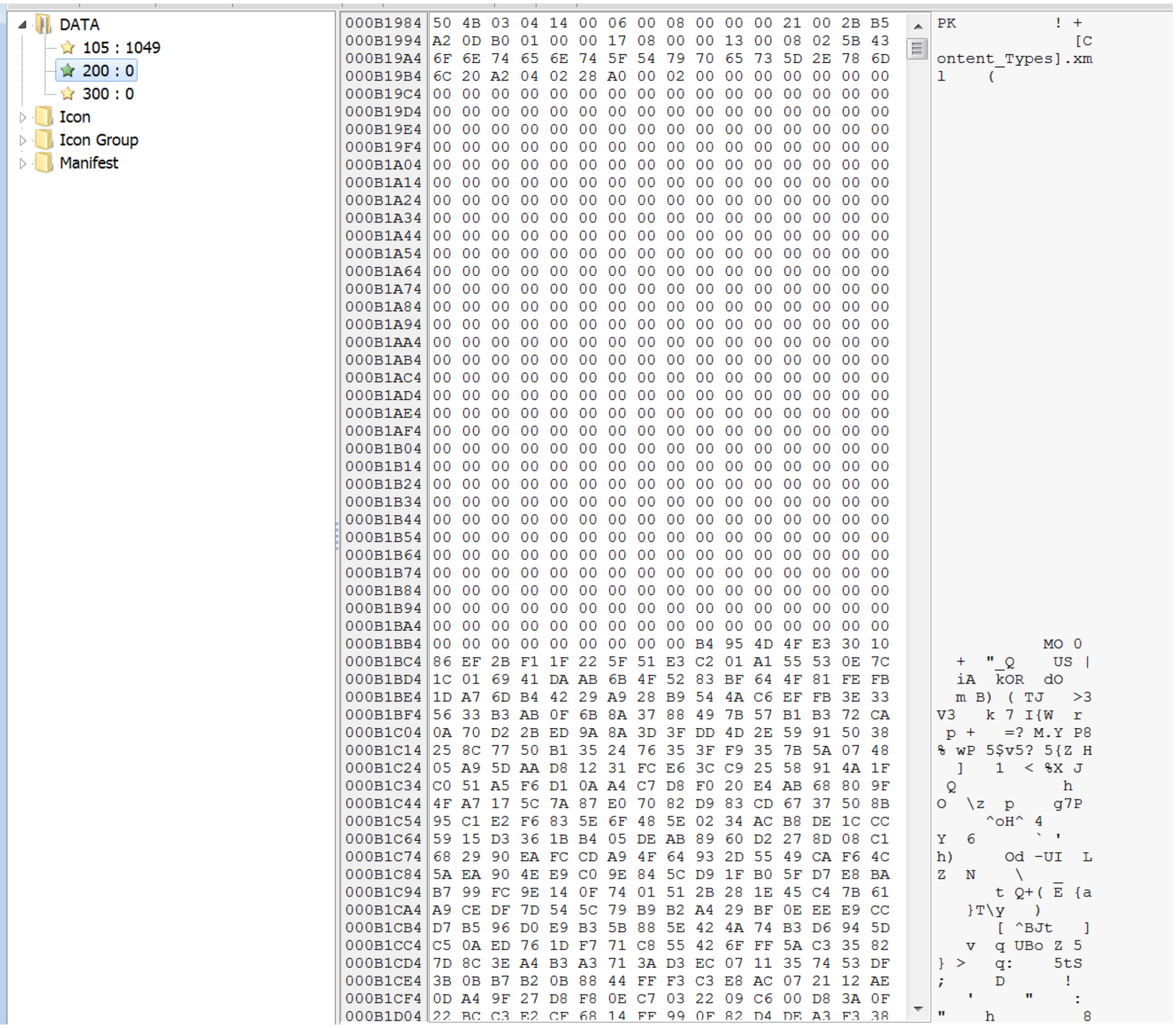
The identical PDB file paths and the timestamps found in all six samples indicate they were all created by a single “MultiLauncher” tool.



PDB Path		P:\MultiLauncher\Release\MultiLauncher.pdb
Characteristics	00000000	
TimeDateStamp	54DCF5EC	Thu, 12 Feb 2015 18:50:20 UTC (2090 days, 20.55 hours ago)

PE file characteristics:

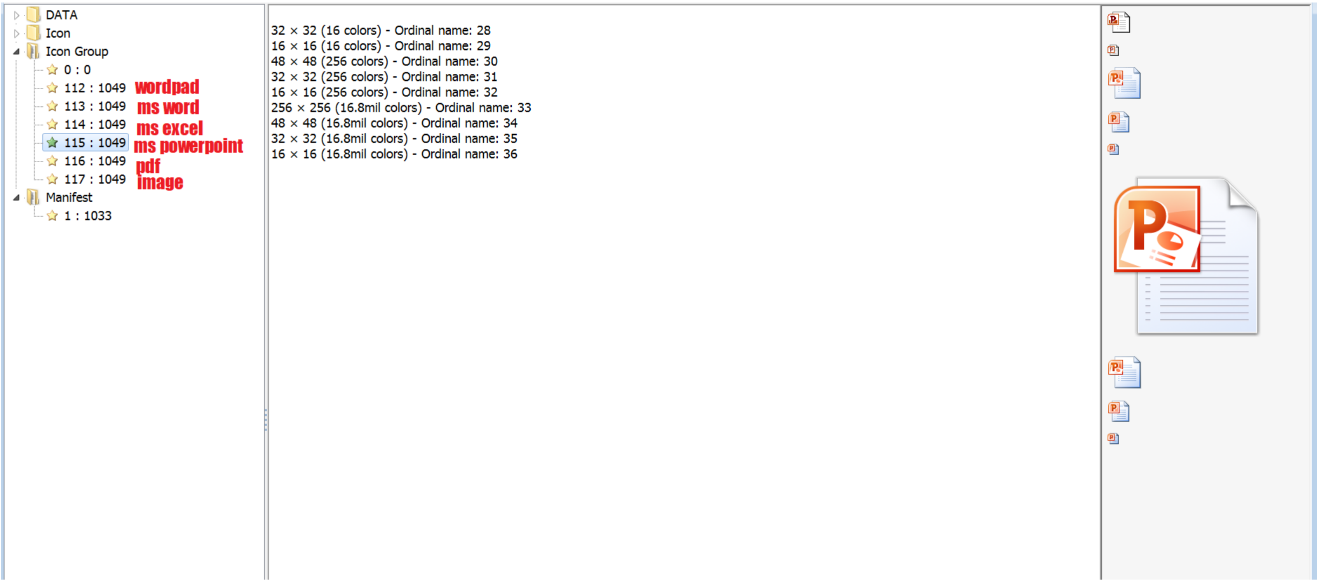
Most of the samples contain a document displayed to the user in resource number 200.



- DATA
  - 105 : 1049
  - 200 : 0
  - 300 : 0
- Icon
- Icon Group
- Manifest

```
000B1984 50 4B 03 04 14 00 06 00 08 00 00 00 21 00 2B B5  PK          ! +
000B1994 A2 0D B0 01 00 00 17 08 00 00 13 00 08 02 5B 43                [C
000B19A4 6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D  ontent_Types].xm
000B19B4 6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00  l    (
000B19C4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B19D4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B19E4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B19F4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AA4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AB4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AC4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AD4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AE4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AF4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1BA4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1BB4 00 00 00 00 00 00 00 00 00 B4 95 4D 4F E3 30 10             MO 0
000B1BC4 86 EF 2B F1 1F 22 5F 51 E3 C2 01 A1 55 53 0E 7C    +  "_Q    US |
000B1BD4 1C 01 69 41 DA AB 6B 4F 52 83 BF 64 4F 81 FE FB    iA  kOR  dO
000B1BE4 1D A7 6D B4 42 29 A9 28 B9 54 4A C6 EF FB 3E 33    m B) ( TJ   >3
000B1BF4 56 33 B3 AB 0F 6B 8A 37 88 49 7B 57 B1 B3 72 CA  V3   k 7 I{W  r
000B1C04 0A 70 D2 2B ED 9A 8A 3D 3F DD 4D 2E 59 91 50 38   p +   =? M.Y P8
000B1C14 25 8C 77 50 B1 35 24 76 35 3F F9 35 7B 5A 07 48  % wP 5$v5? 5{Z H
000B1C24 05 A9 5D AA D8 12 31 FC E6 3C C9 25 58 91 4A 1F    ]   1  < %X J
000B1C34 C0 51 A5 F6 D1 0A A4 C7 D8 F0 20 E4 AB 68 80 9F   Q            h
000B1C44 4F A7 17 5C 7A 87 E0 70 82 D9 83 CD 67 37 50 8B  O  \z  p    g7P
000B1C54 95 C1 E2 F6 83 5E 6F 48 5E 02 34 AC B8 DE 1C CC       ^oH^ 4
000B1C64 59 15 D3 36 1B B4 05 DE AB 89 60 D2 27 8D 08 C1  Y  6       ` '
000B1C74 68 29 90 EA FC CD A9 4F 64 93 2D 55 49 CA F6 4C  h)      Od -UI  L
000B1C84 5A EA 90 4E E9 C0 9E 84 5C D9 1F B0 5F D7 E8 BA  Z  N    \   _
000B1C94 B7 99 FC 9E 14 0F 74 01 51 2B 28 1E 45 C4 7B 61        t Q+( E {a
000B1CA4 A9 CE DF 7D 54 5C 79 B9 B2 A4 29 BF 0E EE E9 CC     }T\y    )
000B1CB4 D7 B5 96 D0 E9 B3 5B 88 5E 42 4A 74 B3 D6 94 5D        [ ^BJt   ]
000B1CC4 C5 0A ED 76 1D F7 71 C8 55 42 6F FF 5A C3 35 82     v  q UBo Z 5
000B1CD4 7D 8C 3E A4 B3 A3 71 3A D3 EC 07 11 35 74 53 DF  } >   q:    5tS
000B1CE4 3B 0B B7 B2 0B 88 44 FF F3 C3 E8 AC 07 21 12 AE  ;     D     !
000B1CF4 0D A4 9F 27 D8 F8 0E C7 03 22 09 C6 00 D8 3A 0F     '    "    :
000B1D04 22 BC C3 E2 CF 68 14 FF 99 0F 82 D4 DE A3 F3 38  "    h         8
```

The samples contain icon sets for all types of documents. The final file uses one of the types. That leaves us with a conclusion the creators were using one tool and were choosing the required document type in the final build.



```
DATA
Icon
Icon Group
  0 : 0
  112 : 1049  wordpad
  113 : 1049  ms word
  114 : 1049  ms excel
  115 : 1049  ms powerpoint
  116 : 1049  pdf
  117 : 1049  image
Manifest
  1 : 1033
```

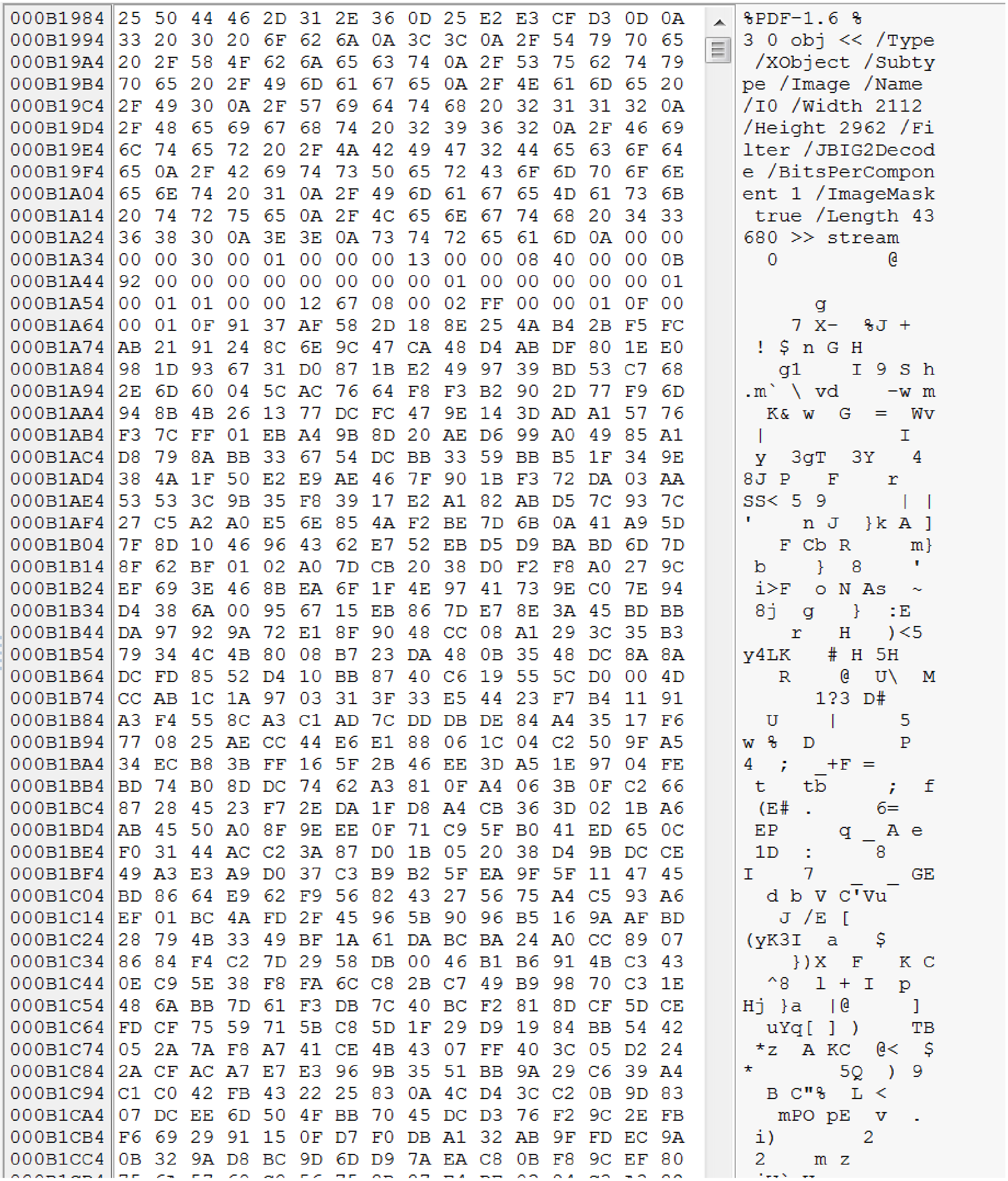
```
32 × 32 (16 colors) - Ordinal name: 28
16 × 16 (16 colors) - Ordinal name: 29
48 × 48 (256 colors) - Ordinal name: 30
32 × 32 (256 colors) - Ordinal name: 31
16 × 16 (256 colors) - Ordinal name: 32
256 × 256 (16.8mil colors) - Ordinal name: 33
48 × 48 (16.8mil colors) - Ordinal name: 34
32 × 32 (16.8mil colors) - Ordinal name: 35
16 × 16 (16.8mil colors) - Ordinal name: 36
```

There are Razy builds that do not contain malicious documents:

- 1f35ce5d620f4eddbfbff5fd1b6142b002bb6a537b864d7745d96ddfd8424bd6
- 3a050db9c571eafd5b1dccb412991434bd0a0fc52c4771274018420a08af4c00

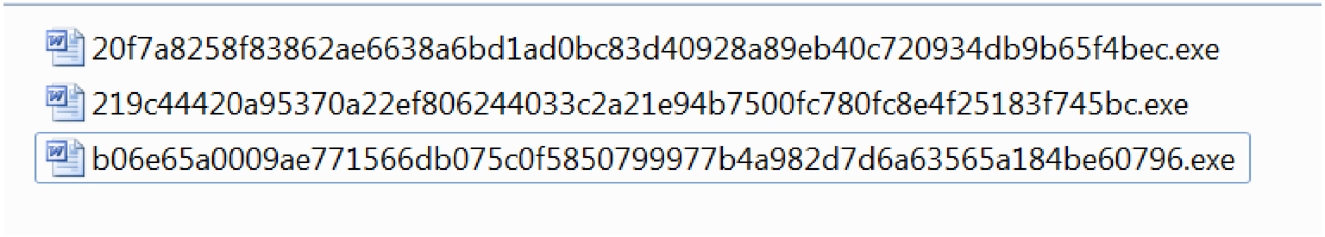
That explains that the attacker always looks for the “right” documents before embedding them into the final file.

The resource can be a PDF file also.



```
000B1984 25 50 44 46 2D 31 2E 36 0D 25 E2 E3 CF D3 0D 0A  %PDF-1.6 %
000B1994 33 20 30 20 6F 62 6A 0A 3C 3C 0A 2F 54 79 70 65  3 0 obj << /Type
000B19A4 20 2F 58 4F 62 6A 65 63 74 0A 2F 53 75 62 74 79   /XObject /Subty
000B19B4 70 65 20 2F 49 6D 61 67 65 0A 2F 4E 61 6D 65 20  pe /Image /Name
000B19C4 2F 49 30 0A 2F 57 69 64 74 68 20 32 31 31 32 0A  /I0 /Width 2112
000B19D4 2F 48 65 69 67 68 74 20 32 39 36 32 0A 2F 46 69  /Height 2962 /Fi
000B19E4 6C 74 65 72 20 2F 4A 42 49 47 32 44 65 63 6F 64  lter /JBIG2Decod
000B19F4 65 0A 2F 42 69 74 73 50 65 72 43 6F 6D 70 6F 6E  e /BitsPerCompon
000B1A04 65 6E 74 20 31 0A 2F 49 6D 61 67 65 4D 61 73 6B  ent 1 /ImageMask
000B1A14 20 74 72 75 65 0A 2F 4C 65 6E 67 74 68 20 34 33   true /Length 43
000B1A24 36 38 30 0A 3E 3E 0A 73 74 72 65 61 6D 0A 00 00  680 >> stream
000B1A34 00 00 30 00 01 00 00 00 13 00 00 08 40 00 00 0B    0         @
000B1A44 92 00 00 00 00 00 00 00 01 00 00 00 00 00 00 01
000B1A54 00 01 01 00 00 12 67 08 00 02 FF 00 00 01 0F 00        g
000B1A64 00 01 0F 91 37 AF 58 2D 18 8E 25 4A B4 2B F5 FC      7 X-  %J +
000B1A74 AB 21 91 24 8C 6E 9C 47 CA 48 D4 AB DF 80 1E E0   ! $ n G H
000B1A84 98 1D 93 67 31 D0 87 1B E2 49 97 39 BD 53 C7 68     g1    I 9 S h
000B1A94 2E 6D 60 04 5C AC 76 64 F8 F3 B2 90 2D 77 F9 6D  .m` \ vd    -w m
000B1AA4 94 8B 4B 26 13 77 DC FC 47 9E 14 3D AD A1 57 76    K& w  G  =  Wv
000B1AB4 F3 7C FF 01 EB A4 9B 8D 20 AE D6 99 A0 49 85 A1   |           I
000B1AC4 D8 79 8A BB 33 67 54 DC BB 33 59 BB B5 1F 34 9E   y  3gT  3Y   4
000B1AD4 38 4A 1F 50 E2 E9 AE 46 7F 90 1B F3 72 DA 03 AA  8J P   F    r
000B1AE4 53 53 3C 9B 35 F8 39 17 E2 A1 82 AB D5 7C 93 7C  SS< 5 9      | |
000B1AF4 27 C5 A2 A0 E5 6E 85 4A F2 BE 7D 6B 0A 41 A9 5D  '    n J  }k A ]
000B1B04 7F 8D 10 46 96 43 62 E7 52 EB D5 D9 BA BD 6D 7D     F Cb R     m}
000B1B14 8F 62 BF 01 02 A0 7D CB 20 38 D0 F2 F8 A0 27 9C   b    }  8    '
000B1B24 EF 69 3E 46 8B EA 6F 1F 4E 97 41 73 9E C0 7E 94   i>F  o N As  ~
000B1B34 D4 38 6A 00 95 67 15 EB 86 7D E7 8E 3A 45 BD BB   8j  g   }  :E
000B1B44 DA 97 92 9A 72 E1 8F 90 48 CC 08 A1 29 3C 35 B3      r   H   )<5
000B1B54 79 34 4C 4B 80 08 B7 23 DA 48 0B 35 48 DC 8A 8A  y4LK   # H 5H
000B1B64 DC FD 85 52 D4 10 BB 87 40 C6 19 55 5C D0 00 4D     R    @  U\  M
000B1B74 CC AB 1C 1A 97 03 31 3F 33 E5 44 23 F7 B4 11 91        1?3 D#
000B1B84 A3 F4 55 8C A3 C1 AD 7C DD DB DE 84 A4 35 17 F6    U    |     5
000B1B94 77 08 25 AE CC 44 E6 E1 88 06 1C 04 C2 50 9F A5  w %  D       P
000B1BA4 34 EC B8 3B FF 16 5F 2B 46 EE 3D A5 1E 97 04 FE  4  ;  _+F =
000B1BB4 BD 74 B0 8D DC 74 62 A3 81 0F A4 06 3B 0F C2 66   t   tb     ;  f
000B1BC4 87 28 45 23 F7 2E DA 1F D8 A4 CB 36 3D 02 1B A6   (E# .     6=
000B1BD4 AB 45 50 A0 8F 9E EE 0F 71 C9 5F B0 41 ED 65 0C   EP     q _ A e
000B1BE4 F0 31 44 AC C2 3A 87 D0 1B 05 20 38 D4 9B DC CE   1D  :     8
000B1BF4 49 A3 E3 A9 D0 37 C3 B9 B2 5F EA 9F 5F 11 47 45  I    7   _  _ GE
000B1C04 BD 86 64 E9 62 F9 56 82 43 27 56 75 A4 C5 93 A6    d b V C'Vu
000B1C14 EF 01 BC 4A FD 2F 45 96 5B 90 96 B5 16 9A AF BD     J /E [
000B1C24 28 79 4B 33 49 BF 1A 61 DA BC BA 24 A0 CC 89 07  (yK3I  a    $
000B1C34 86 84 F4 C2 7D 29 58 DB 00 46 B1 B6 91 4B C3 43      })X  F   K C
000B1C44 0E C9 5E 38 F8 FA 6C C8 2B C7 49 B9 98 70 C3 1E    ^8  l + I  p
000B1C54 48 6A BB 7D 61 F3 DB 7C 40 BC F2 81 8D CF 5D CE  Hj }a  |@    ]
000B1C64 FD CF 75 59 71 5B C8 5D 1F 29 D9 19 84 BB 54 42    uYq[ ] )    TB
000B1C74 05 2A 7A F8 A7 41 CE 4B 43 07 FF 40 3C 05 D2 24   *z  A KC  @<  $
000B1C84 2A CF AC A7 E7 E3 96 9B 35 51 BB 9A 29 C6 39 A4  *       5Q  ) 9
000B1C94 C1 C0 42 FB 43 22 25 83 0A 4C D4 3C C2 0B 9D 83    B C"%  L <
000B1CA4 07 DC EE 6D 50 4F BB 70 45 DC D3 76 F2 9C 2E FB     mPO pE  v  .
000B1CB4 F6 69 29 91 15 0F D7 F0 DB A1 32 AB 9F FD EC 9A   i)       2
000B1CC4 0B 32 9A D8 BC 9D 6D D9 7A EA C8 0B F8 9C EF 80   2    m z
```

Usually, Razy is an EXE file with an office document icon.



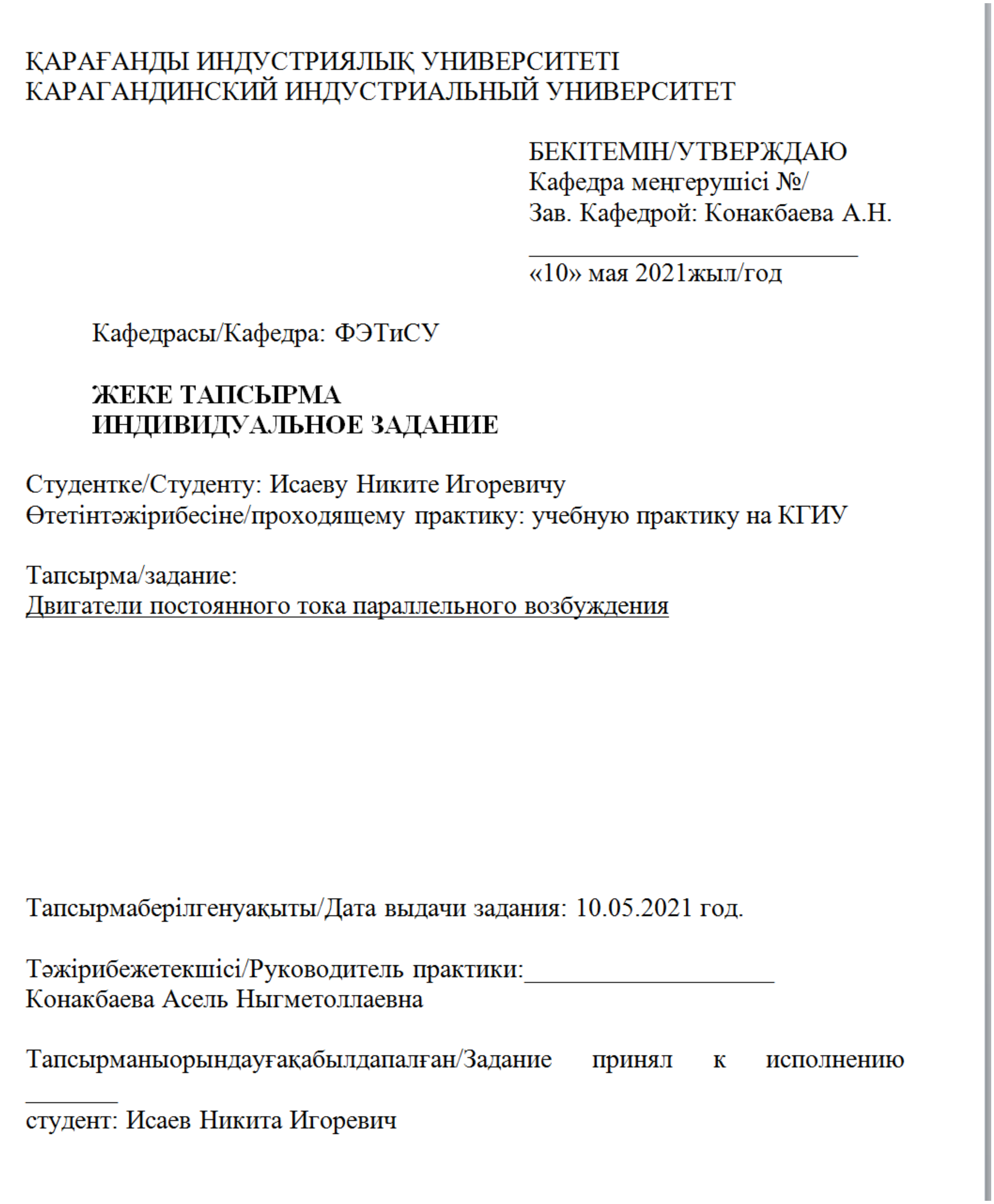
20f7a8258f83862ae6638a6bd1ad0bc83d40928a89eb40c720934db9b65f4bec.exe

219c44420a95370a22ef806244033c2a21e94b7500fc780fc8e4f25183f745bc.exe

b06e65a0009ae771566db075c0f5850799977b4a982d7d6a63565a184be60796.exe

The actual file extension

Most of the time, the attackers set up an office document icon for an executable file to mislead the user. When the user launches a file, he sees an opened office document, and a malicious EXE file will perform other operations.



ҚАРАҒАНДЫ ИНДУСТРИЯЛЫҚ УНИВЕРСИТЕТІ
КАРАГАНДИНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ

БЕКІТЕМІН/УТВЕРЖДАЮ
Кафедра меңгерушісі №/
Зав. Кафедрой: Конакбаева А.Н.
____
«10» мая 2021жыл/год

Кафедрасы/Кафедра: ФЭТиСУ

ЖЕКЕ ТАПСЫРМА
ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

Студентке/Студенту: Исаеву Никите Игоревичу
Өтетінтәжірибесіне/проходящему практику: учебную практику на КГИУ

Тапсырма/задание:
Двигатели постоянного тока параллельного возбуждения

Тапсырмаберілгенуақыты/Дата выдачи задания: 10.05.2021 год.

Тәжірибежетекшісі/Руководитель практики:____________________
Конакбаева Асель Ныгметоллаевна

Тапсырманыорындауғақабылдапалған/Задание принял к исполнению ________
студент: Исаев Никита Игоревич

SHA256:219c44420a95370a22ef806244033c2a21e94b7500fc780fc8e4f25183f745bc

Отчет о проделанной работе на 2020 – 2021 уч.год

Учитель по предмету «Коррекционная ритмика» - Абулхайрова.Э.Е., стаж работы 26 лет, высшая категория.

Прошла курс повышения квалифкации на тему «Инновациялық технологияларды қолдану арқылы педагог- хореографтардың құзреттілігін дамыту»,13.03.2021г.

Коррекционная ритмика в неделю 1 час (1 В, 3Д, 4А, 4В,5В, 6В), музыкальная коррекционная ритмика в группе детского сада.

В настоящее время работаю над темой «Развития слухового восприятия и произносительной стороны речи на уроках ритмики».

Основные направления работы по коррекционной ритмике:

- Развитие восприятия музыкальных произведений разного характера (веселого, грустного, быстрого, медленного)
- Развитие умения слушать произведение до конца, различать части произведения, определять характер музыки
- Выразительно, правильно выполнять под музыку танцевальные движения, несложные композиции.

Достижения учащихся:

Сентябрь – октябрь: онлайн конкурс – фестиваль народных танцев- «Гран – При».

Ноябрь – декабрь: Международный фестиваль- конкурс театр и студий моды

SHA256:b06e65a0009ae771566db075c0f5850799977b4a982d7d6a63565a184be60796

О внесении изменений в постановление акимата Акжаикского района от 28 мая 2018 года № 155 «Об утверждении коэффициента зонирования, учитывающего месторасположение объекта налогообложения в населенном пункте»

В соответствии с Законом Республики Казахстан от 6 апреля 2016 года «О правовых актах» акимат района **ПОСТАНОВЛЯЕТ**:

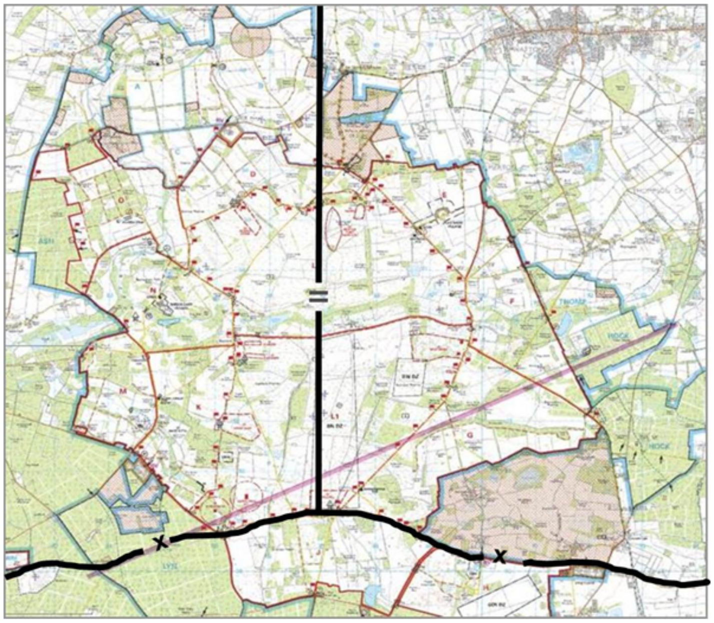
1. Внести в постановление акимата Акжаикского района от 28 мая 2018 года № 155 «Об утверждении коэффициента зонирования, учитывающего месторасположение объекта налогообложения в населенном пункте» (зарегистрированное в Реестре государственной регистрации нормативных правовых актов за №5223, опубликованное 8 июня 2018 года в Эталонном контрольном банке нормативных правовых актов Республики Казахстан) следующие изменения:

преамбулу указанного постановления изложить в следующей редакции:

«В соответствии с Кодексом Республики Казахстан от 25 декабря

SHA256:20f7a8258f83862ae6638a6bd1ad0bc83d40928a89eb40c720934db9b65f4bec

(EXAMPLE)BATTLEGROUP TITLE INTELLIGENCE SUMMARY (002)
AS AT DATE: 241800AJUL16
INTELLIGENCE CUT OFF DATE:241800AJUL16



VITAL INTELLIGENCE:

1.NSTR

SITUATION IN GENERAL:

- 2 Person visit westmere camp;
- Media visited base;
- Mine field on KazCOY AO;
- Weapon founded in civil car;
- Key persons identified in Eastmere village

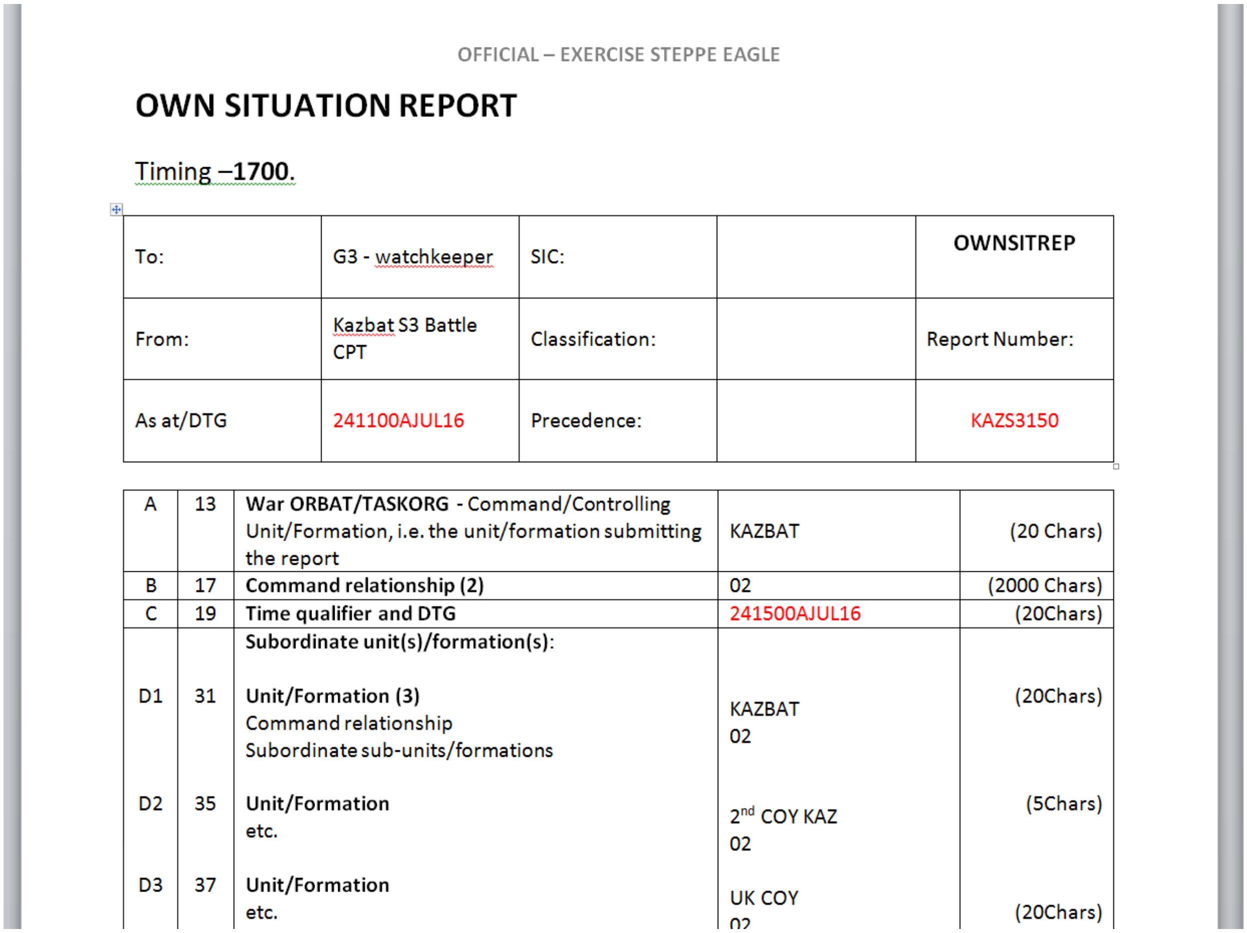
SITUATION IN DETAIL / COMPANY SUMMARY

2.NSTR

POPULATION:

1. 2 Person visited Westmere camp;

240830AJUL16 1 male and 1 female came to base and suggest their fruits and vegetables. They said that they had access to inside the camp and militaries, which were before KAZBAT always bought their staff



OFFICIAL – EXERCISE STEPPE EAGLE

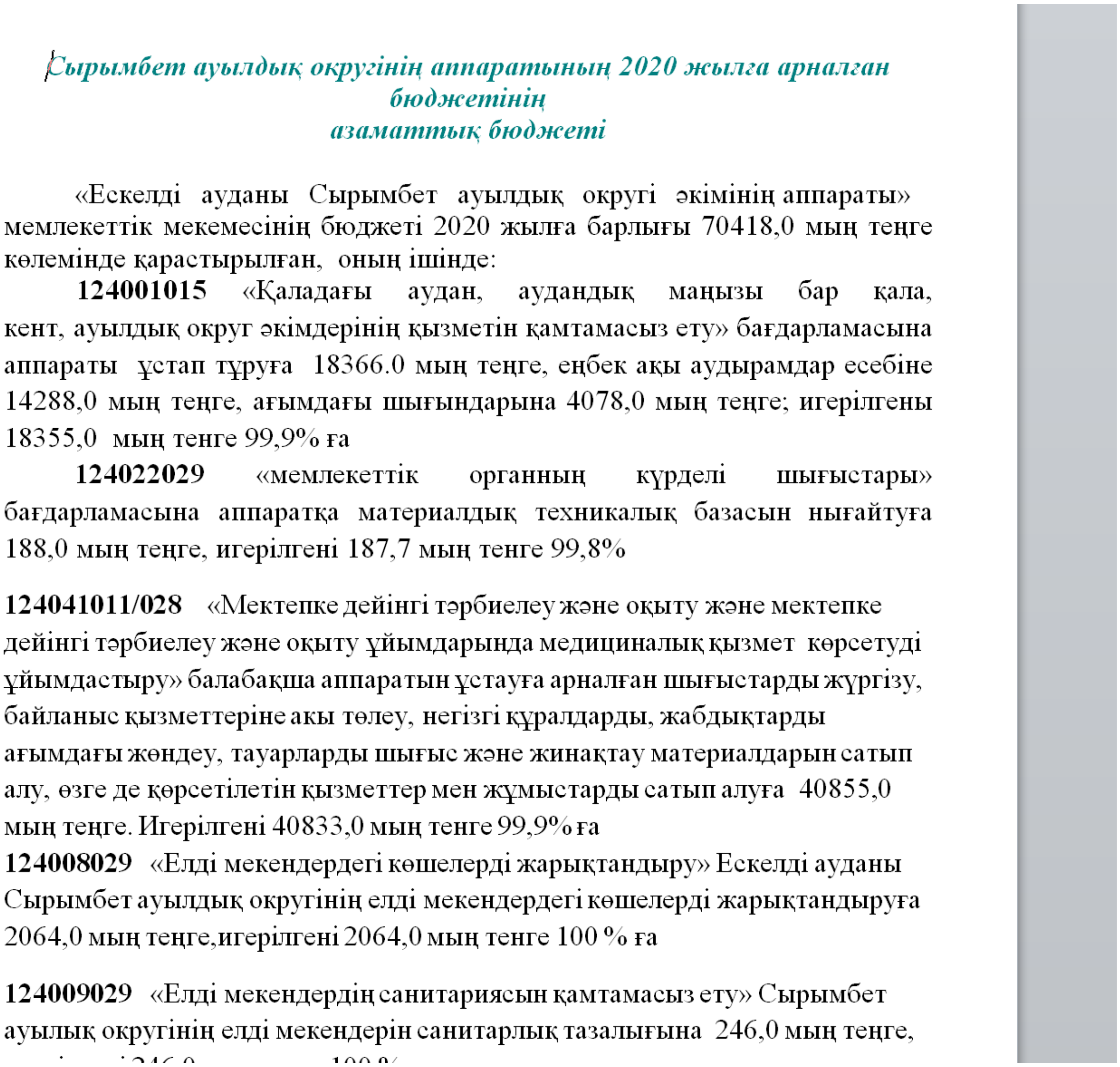
OWN SITUATION REPORT

Timing –**1700**.

To:	G3 - watchkeeper	SIC:		**OWNSITREP**
From:	Kazbat S3 Battle CPT	Classification:		Report Number:
As at/DTG	241100AJUL16	Precedence:		KAZS3150

A	13	**War ORBAT/TASKORG** - Command/Controlling Unit/Formation, i.e. the unit/formation submitting the report	KAZBAT	(20 Chars)
B	17	**Command relationship (2)**	02	(2000 Chars)
C	19	**Time qualifier and DTG**	241500AJUL16	(20Chars)
		Subordinate unit(s)/formation(s):		
D1	31	**Unit/Formation (3)** Command relationship Subordinate sub-units/formations	KAZBAT 02	(20Chars)
D2	35	**Unit/Formation** **etc.**	2nd COY KAZ 02	(5Chars)
D3	37	**Unit/Formation** **etc.**	UK COY 02	(20Chars)

SHA256:8FA473C03850B22C2C6AADCFE69268BE4E4C7A33881581FEA83789755AF8F22A



Сырымбет ауылдық округінің аппаратының 2020 жылға арналған бюджетінің
азаматтық бюджеті

«Ескелді ауданы Сырымбет ауылдық округі әкімінің аппараты» мемлекеттік мекемесінің бюджеті 2020 жылға барлығы 70418,0 мың теңге көлемінде қарастырылған, оның ішінде:

124001015 «Қаладағы аудан, аудандық маңызы бар қала, кент, ауылдық округ әкімдерінің қызметін қамтамасыз ету» бағдарламасына аппараты ұстап тұруға 18366.0 мың теңге, еңбек ақы аудырамдар есебіне 14288,0 мың теңге, ағымдағы шығындарына 4078,0 мың теңге; игерілгены 18355,0 мың тенге 99,9% ға

124022029 «мемлекеттік органның күрделі шығыстары» бағдарламасына аппаратқа материалдық техникалық базасын нығайтуға 188,0 мың теңге, игерілгені 187,7 мың тенге 99,8%

124041011/028 «Мектепке дейінгі тәрбиелеу және оқыту және мектепке дейінгі тәрбиелеу және оқыту ұйымдарында медициналық қызмет көрсетуді ұйымдастыру» балабақша аппаратын ұстауға арналған шығыстарды жүргізу, байланыс қызметтеріне акы төлеу, негізгі құралдарды, жабдықтарды ағымдағы жөндеу, тауарларды шығыс және жинақтау материалдарын сатып алу, өзге де қөрсетілетін қызметтер мен жұмыстарды сатып алуға 40855,0 мың теңге. Игерілгені 40833,0 мың тенге 99,9% ға

124008029 «Елді мекендердегі көшелерді жарықтандыру» Ескелді ауданы Сырымбет ауылдық округінің елді мекендердегі көшелерді жарықтандыруға 2064,0 мың теңге,игерілгені 2064,0 мың тенге 100 % ға

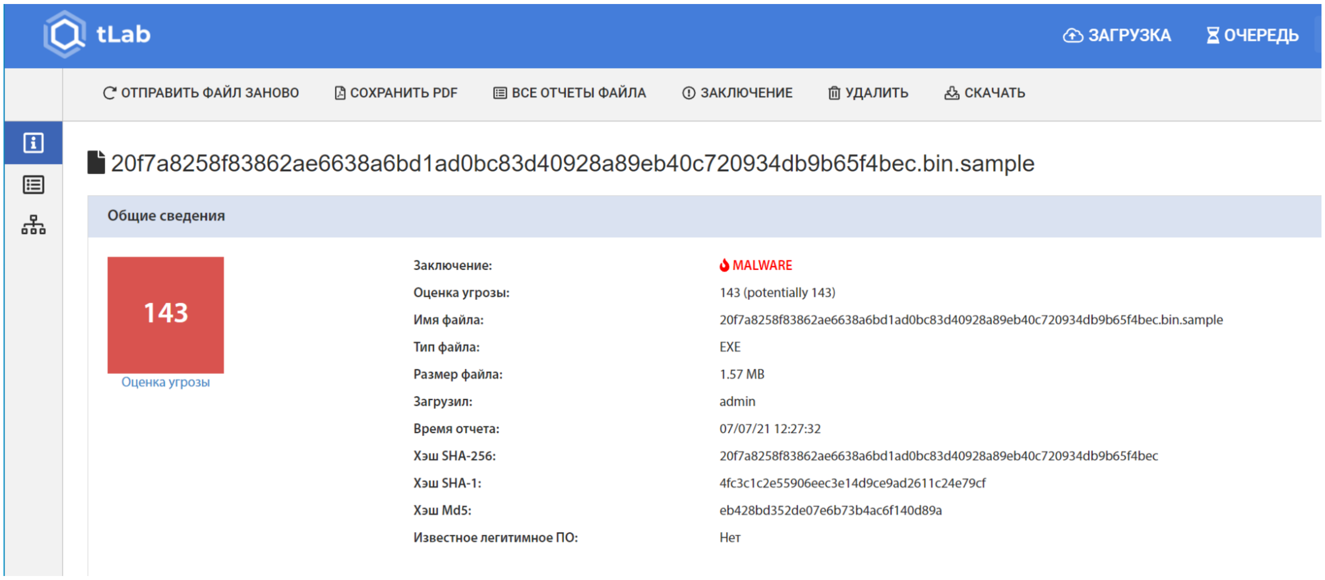
124009029 «Елді мекендердің санитариясын қамтамасыз ету» Сырымбет ауылық округінің елді мекендерін санитарлық тазалығына 246,0 мың теңге,

SHA256:3ED1B88C9AE34BA4FFBF8AED737F2DC9A0AEDEEDF8D2A4A69555518845E16264

All objects have the same functionality but different office documents. Since all of the samples are just variants of the same family, consider one of them.

20f7a8258f83862ae6638a6bd1ad0bc83d40928a89eb40c720934db9b65f4bec

This object is an EXE file with an icon of a Word document. At a closer look, one can conclude, it is a dropper for office documents.



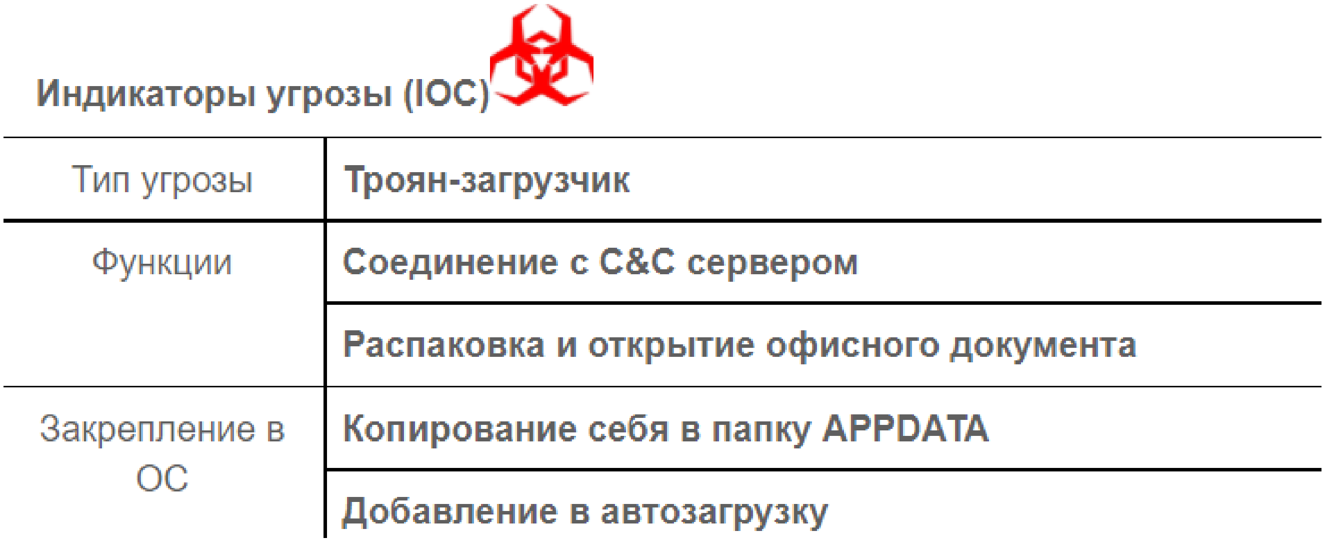
20f7a8258f83862ae6638a6bd1ad0bc83d40928a89eb40c720934db9b65f4bec.bin.sample

Общие сведения

143
Оценка угрозы

Заключение:	MALWARE
Оценка угрозы:	143 (potentially 143)
Имя файла:	20f7a8258f83862ae6638a6bd1ad0bc83d40928a89eb40c720934db9b65f4bec.bin.sample
Тип файла:	EXE
Размер файла:	1.57 MB
Загрузил:	admin
Время отчета:	07/07/21 12:27:32
Хэш SHA-256:	20f7a8258f83862ae6638a6bd1ad0bc83d40928a89eb40c720934db9b65f4bec
Хэш SHA-1:	4fc3c1c2e55906eec3e14d9ce9ad2611c24e79cf
Хэш Md5:	eb428bd352de07e6b73b4ac6f140d89a
Известное легитимное ПО:	Нет

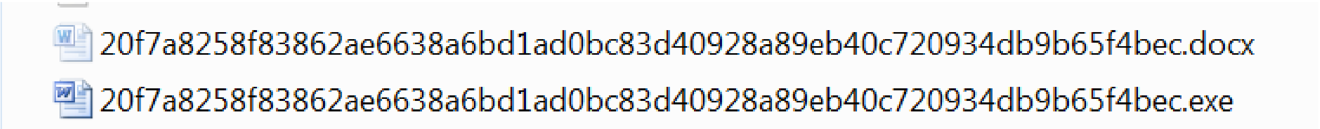
Summary of the object in the tLab system:



Индикаторы угрозы (IOC)

Тип угрозы	Троян-загрузчик
Функции	Соединение с C&C сервером
	Распаковка и открытие офисного документа
Закрепление в ОС	Копирование себя в папку APPDATA
	Добавление в автозагрузку

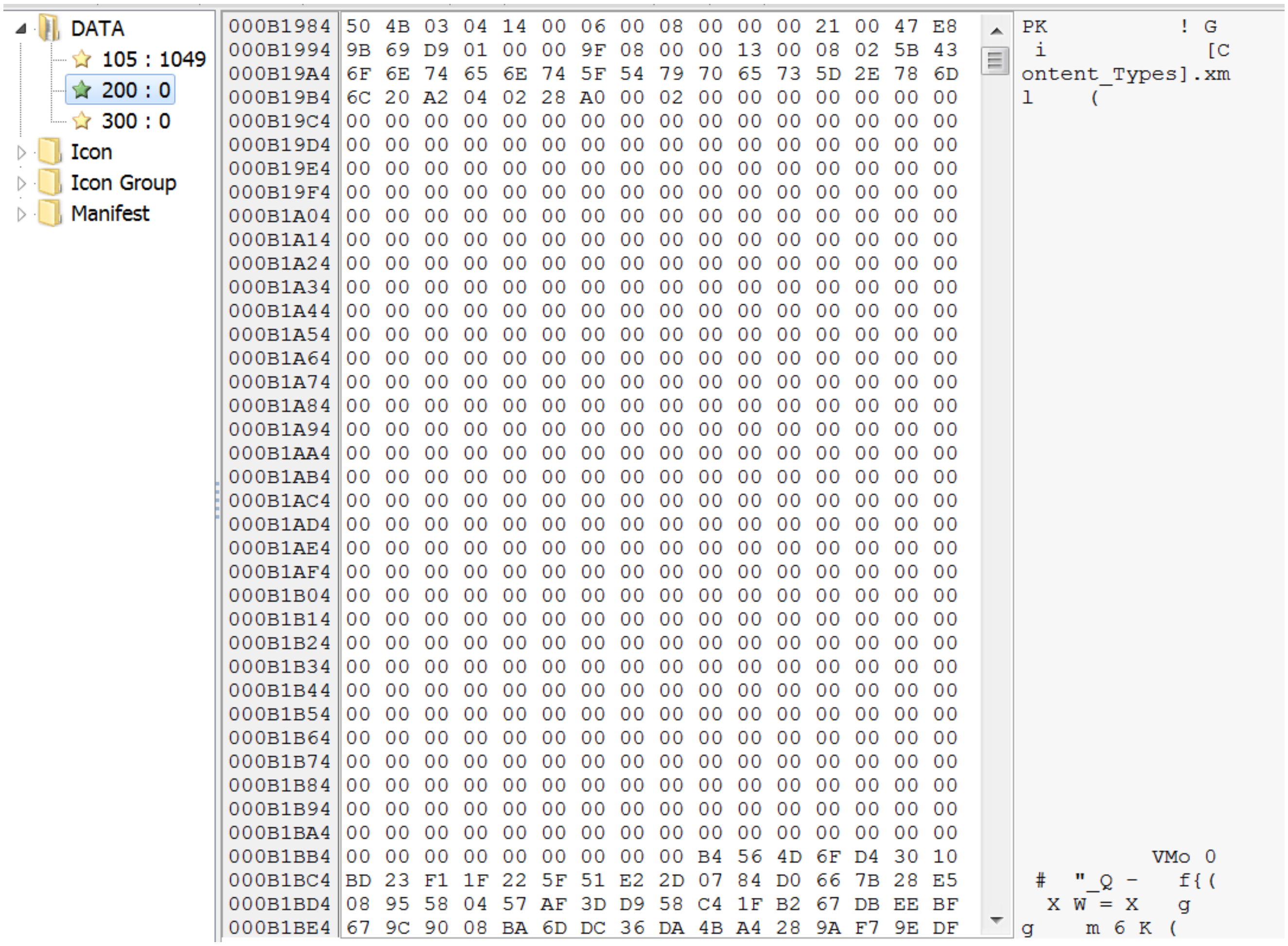
Launching the EXE file will result in a regular office document hiddenly located in the current folder.



20f7a8258f83862ae6638a6bd1ad0bc83d40928a89eb40c720934db9b65f4bec.docx
20f7a8258f83862ae6638a6bd1ad0bc83d40928a89eb40c720934db9b65f4bec.exe

Created hidden office document

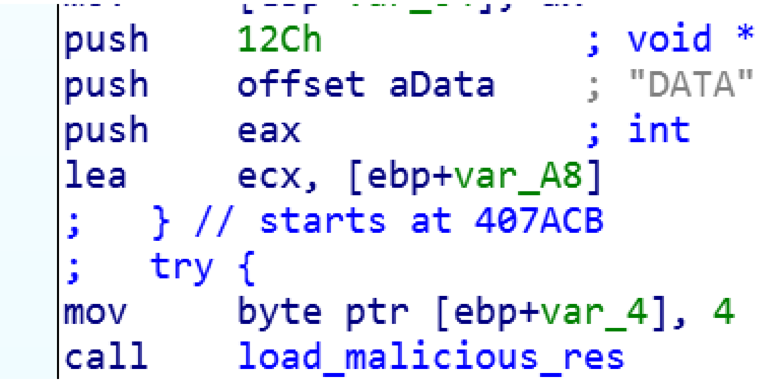
The malicious file contains office document in its resources (DATA - 200):



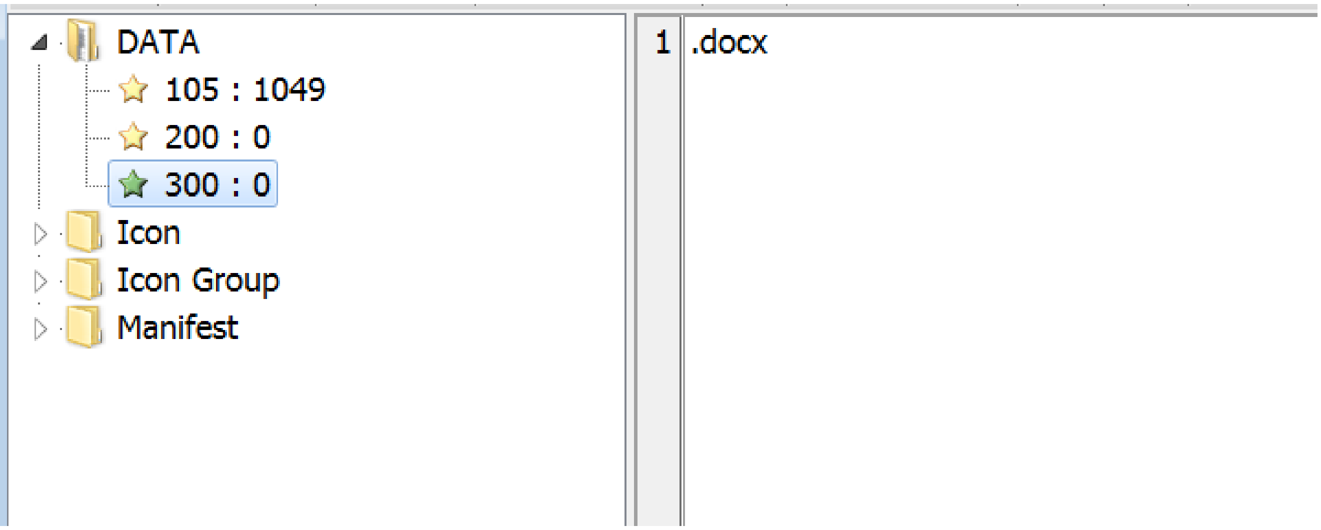
```
000B1984 50 4B 03 04 14 00 06 00 08 00 00 00 21 00 47 E8  PK          ! G
000B1994 9B 69 D9 01 00 00 9F 08 00 00 13 00 08 02 5B 43   i            [C
000B19A4 6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D  ontent_Types].xm
000B19B4 6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00  l    (
000B19C4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B19D4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B19E4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B19F4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1A94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AA4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AB4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AC4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AD4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AE4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1AF4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1B94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1BA4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000B1BB4 00 00 00 00 00 00 00 00 00 B4 56 4D 6F D4 30 10                VMo 0
000B1BC4 BD 23 F1 1F 22 5F 51 E2 2D 07 84 D0 66 7B 28 E5   #  "_Q -    f{(
000B1BD4 08 95 58 04 57 AF 3D D9 58 C4 1F B2 67 DB EE BF    X W = X    g
000B1BE4 67 9C 90 08 BA 6D DC 36 DA 4B A4 28 9A F7 9E DF  g     m 6 K (
```

The first bytes of the file in the resources determine the type of the embedded document. In this case, the “4B 03 04 14 00 06 00 08 00” signature corresponds with the Microsoft Office Open XML Format.

When launched, the Razy malware detects the type of displayed document given the information from the resource number 300 (0x12C):



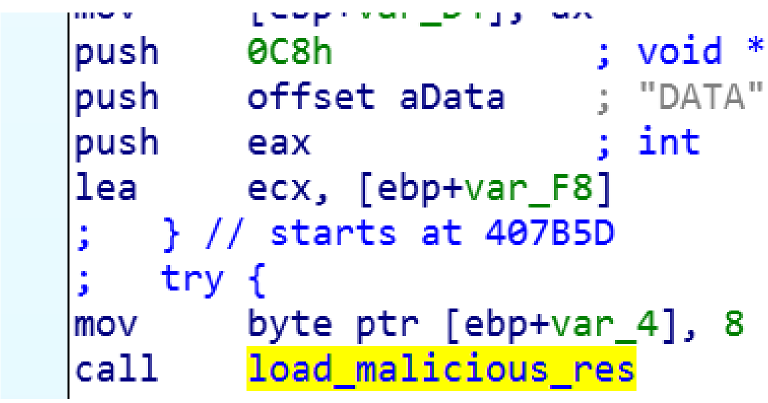
```
push    12Ch            ; void *
push    offset aData    ; "DATA"
push    eax             ; int
lea     ecx, [ebp+var_A8]
;   } // starts at 407ACB
;   try {
mov     byte ptr [ebp+var_4], 4
call    load_malicious_res
```



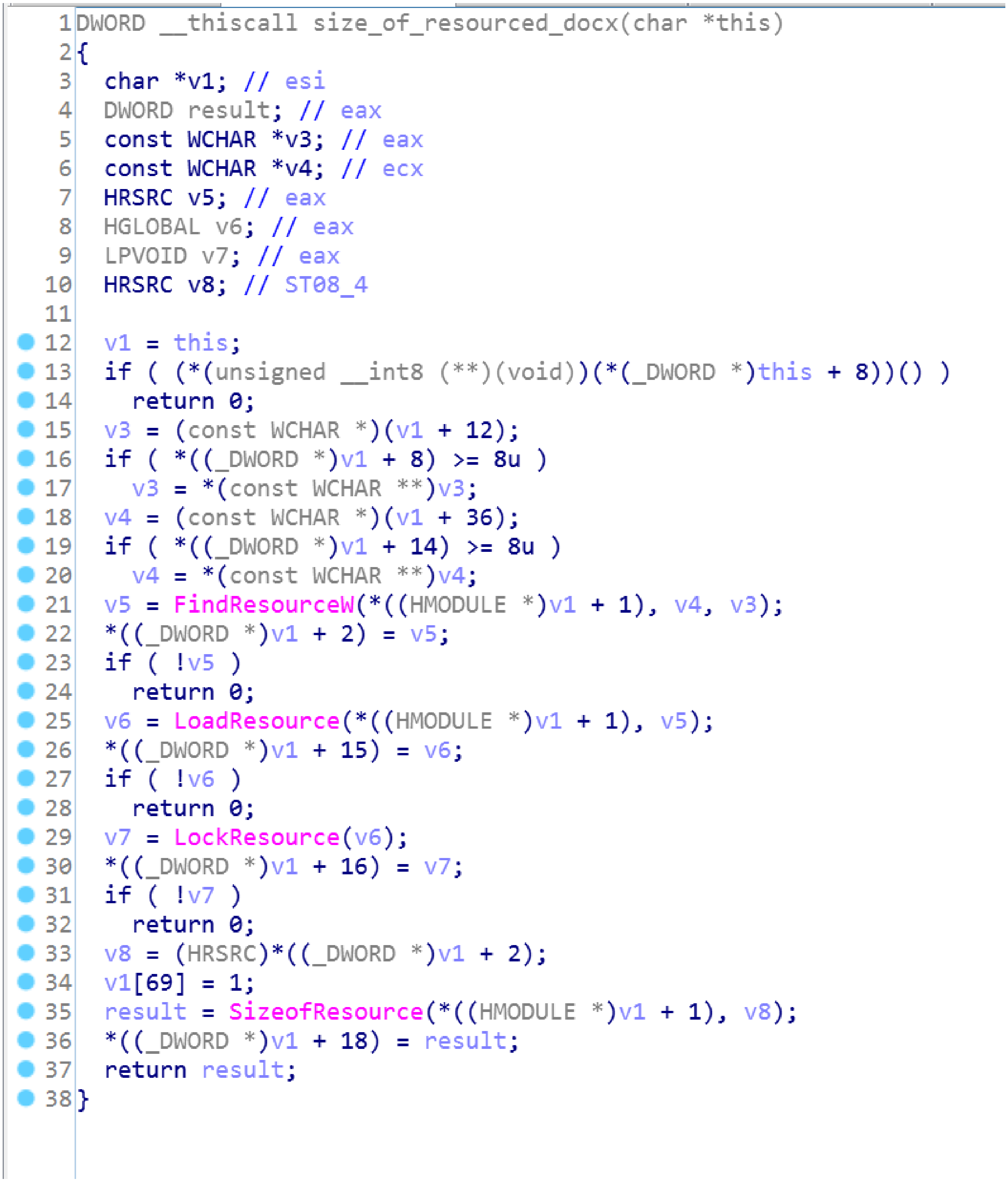
```
1 .docx
```

The resource containing real extension of the file

Next, the reading of the original office document from the resource number 200 (0x0C8) begins, using the FindResource, LoadResource, LockResource, SizeOfResource functions:



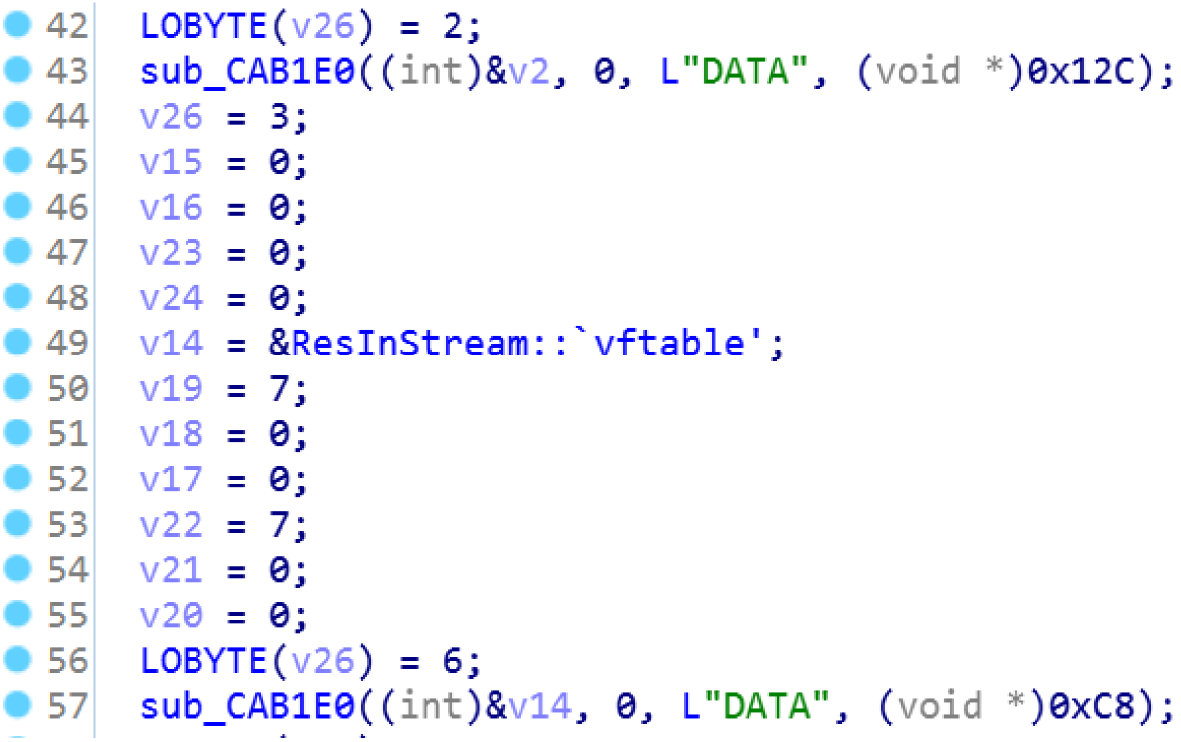
```
mov     [ebp+var_[illegible]], ax
push    0C8h                ; void *
push    offset aData        ; "DATA"
push    eax                 ; int
lea     ecx, [ebp+var_F8]
;   } // starts at 407B5D
;   try {
mov     byte ptr [ebp+var_4], 8
call    load_malicious_res
```



```
DWORD __thiscall size_of_resourced_docx(char *this)
{
  char *v1; // esi
  DWORD result; // eax
  const WCHAR *v3; // eax
  const WCHAR *v4; // ecx
  HRSRC v5; // eax
  HGLOBAL v6; // eax
  LPVOID v7; // eax
  HRSRC v8; // ST08_4

  v1 = this;
  if ( (*(unsigned __int8 (**)(void))(*(_DWORD *)this + 8))() )
    return 0;
  v3 = (const WCHAR *)(v1 + 12);
  if ( *((_DWORD *)v1 + 8) >= 8u )
    v3 = *(const WCHAR **)v3;
  v4 = (const WCHAR *)(v1 + 36);
  if ( *((_DWORD *)v1 + 14) >= 8u )
    v4 = *(const WCHAR **)v4;
  v5 = FindResourceW(*((HMODULE *)v1 + 1), v4, v3);
  *((_DWORD *)v1 + 2) = v5;
  if ( !v5 )
    return 0;
  v6 = LoadResource(*((HMODULE *)v1 + 1), v5);
  *((_DWORD *)v1 + 15) = v6;
  if ( !v6 )
    return 0;
  v7 = LockResource(v6);
  *((_DWORD *)v1 + 16) = v7;
  if ( !v7 )
    return 0;
  v8 = (HRSRC)*((_DWORD *)v1 + 2);
  v1[69] = 1;
  result = SizeofResource(*((HMODULE *)v1 + 1), v8);
  *((_DWORD *)v1 + 18) = result;
  return result;
}
```

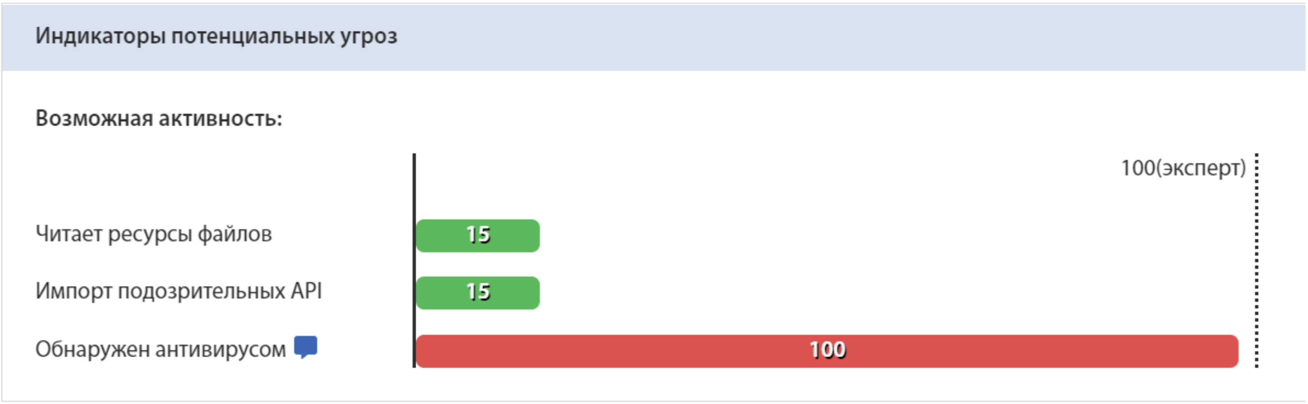
Functions for working with resources



```
LOBYTE(v26) = 2;
sub_CAB1E0((int)&v2, 0, L"DATA", (void *)0x12C);
v26 = 3;
v15 = 0;
v16 = 0;
v23 = 0;
v24 = 0;
v14 = &ResInStream::`vftable';
v19 = 7;
v18 = 0;
v17 = 0;
v22 = 7;
v21 = 0;
v20 = 0;
LOBYTE(v26) = 6;
sub_CAB1E0((int)&v14, 0, L"DATA", (void *)0xC8);
```

Code for working with resources under the DATA identifier

In the tLab sandbox, when uploading a file, one can see a potential threat indicator:



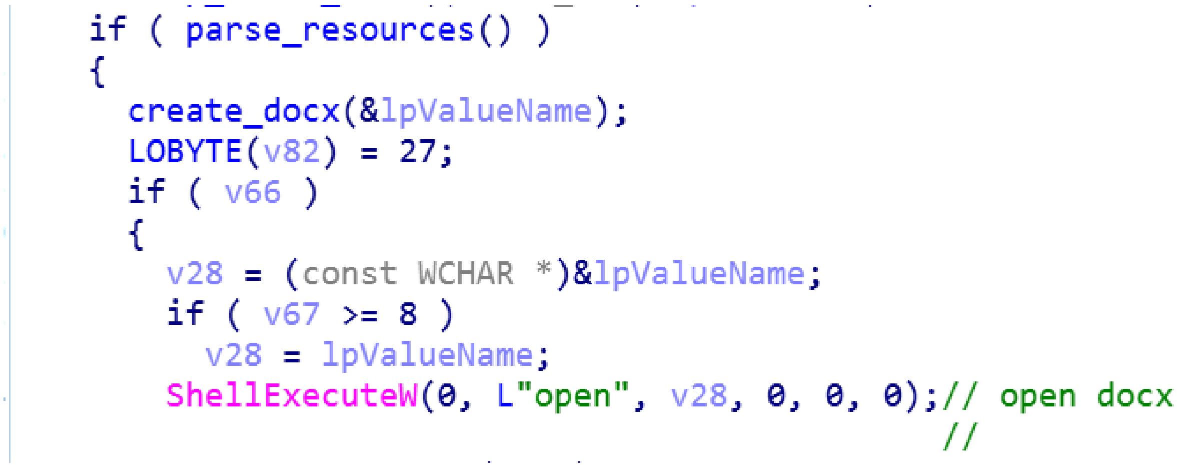
Индикаторы потенциальных угроз

Возможная активность:

	100(эксперт)
Читает ресурсы файлов	15
Импорт подозрительных API	15
Обнаружен антивирусом	100

The result of static analysis on the tLab system

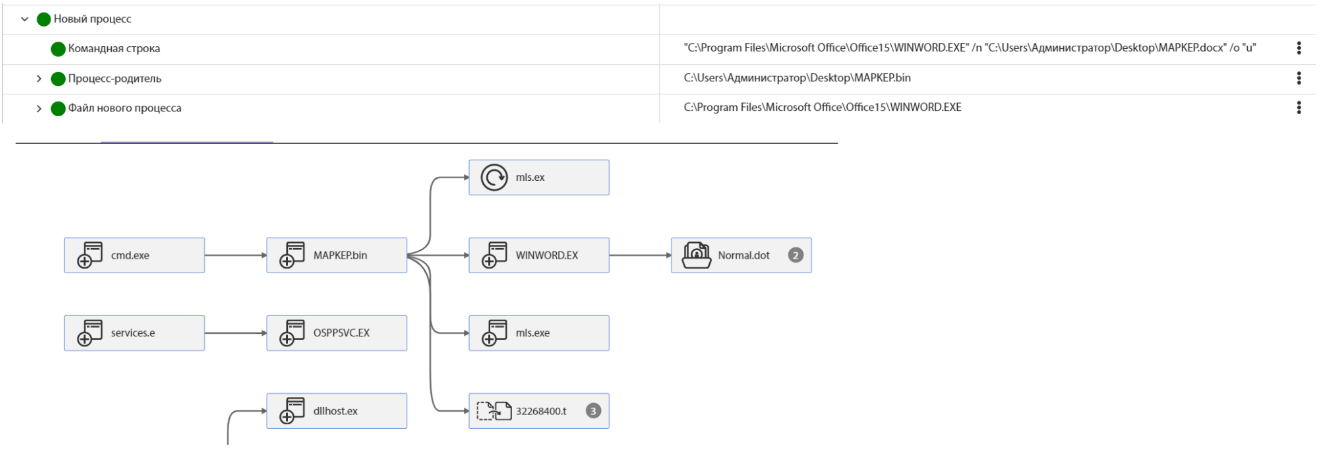
A malicious file opens a created document in Word using the ShellExecuteW function:



```
if ( parse_resources() )
{
  create_docx(&lpValueName);
  LOBYTE(v82) = 27;
  if ( v66 )
  {
    v28 = (const WCHAR *)&lpValueName;
    if ( v67 >= 8 )
      v28 = lpValueName;
    ShellExecuteW(0, L"open", v28, 0, 0, 0);// open docx
                                            //
```

The ShellExecute function opens the passed file in a program associated with specific extensions. For example, if the file has the DOCX extension, it will be opened by the program registered to open such files (in our case, Microsoft Word).

The T&T Security sandbox also builds a graph of the dynamic behaviour of an object:

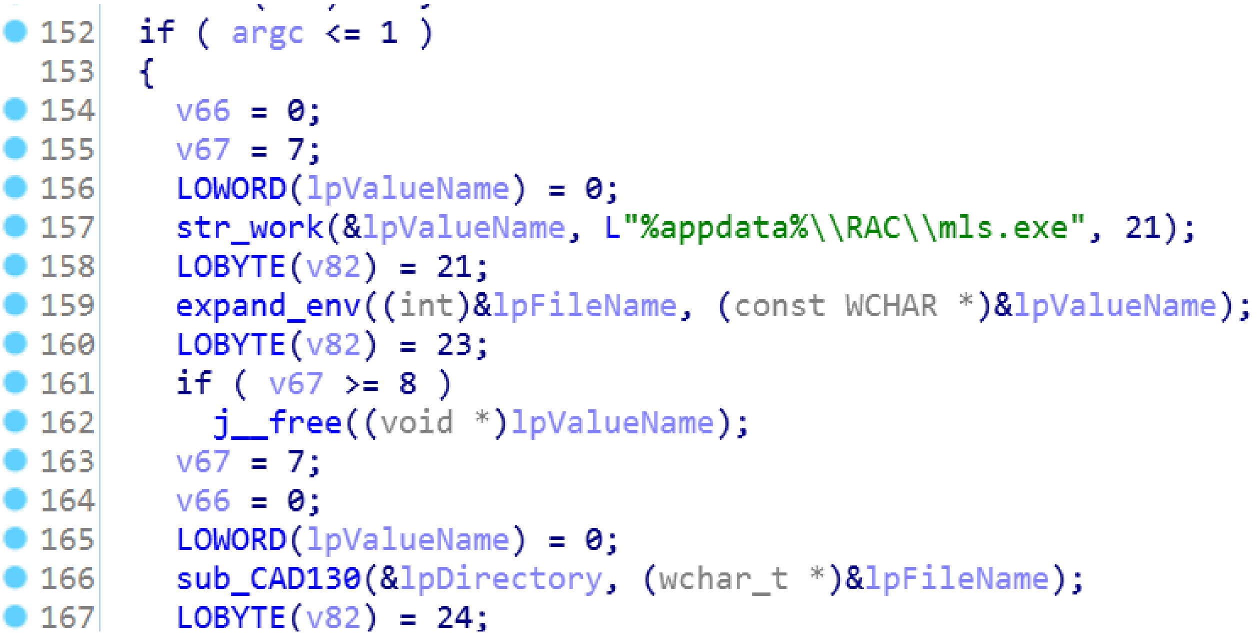


⌄ ● Новый процесс	
● Командная строка	"C:\Program Files\Microsoft Office\Office15\WINWORD.EXE" /n "C:\Users\Администратор\Desktop\MAPKEP.docx" /o "u"
› ● Процесс-родитель	C:\Users\Администратор\Desktop\MAPKEP.bin
› ● Файл нового процесса	C:\Program Files\Microsoft Office\Office15\WINWORD.EXE

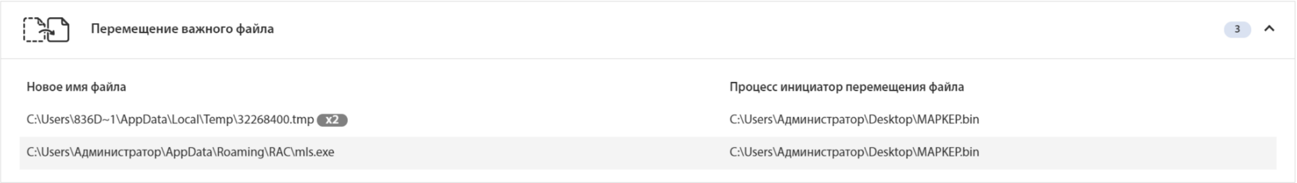
A detailed report on the tLab system

The Word document does not contain any macros and is not malicious, according to the initial analysis. Presumably, the purpose of opening an office document is to conceal malicious activity.

At the same time, the malicious file creates a copy of itself in the APPDATA \ RAC folder under the name mls.exe:



```
if ( argc <= 1 )
{
  v66 = 0;
  v67 = 7;
  LOWORD(lpValueName) = 0;
  str_work(&lpValueName, L"%appdata%\\RAC\\mls.exe", 21);
  LOBYTE(v82) = 21;
  expand_env((int)&lpFileName, (const WCHAR *)&lpValueName);
  LOBYTE(v82) = 23;
  if ( v67 >= 8 )
    j__free((void *)lpValueName);
  v67 = 7;
  v66 = 0;
  LOWORD(lpValueName) = 0;
  sub_CAD130(&lpDirectory, (wchar_t *)&lpFileName);
  LOBYTE(v82) = 24;
```

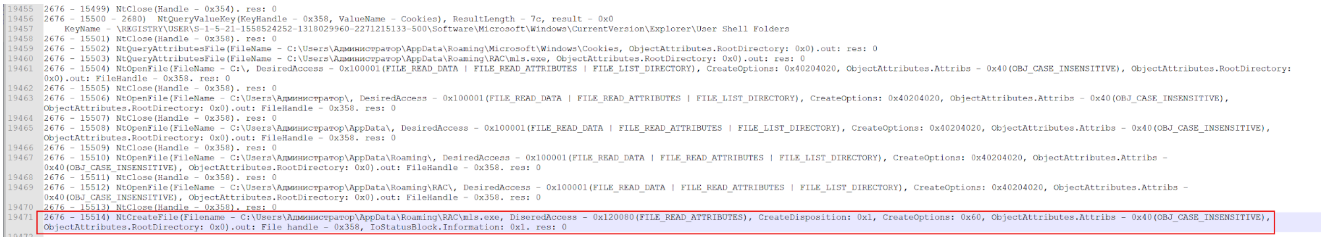


Перемещение важного файла 3

Новое имя файла	Процесс инициатор перемещения файла
C:\Users\836D~1\AppData\Local\Temp\32268400.tmp x2	C:\Users\Администратор\Desktop\MAPKEP.bin
C:\Users\Администратор\AppData\Roaming\RAC\mls.exe	C:\Users\Администратор\Desktop\MAPKEP.bin

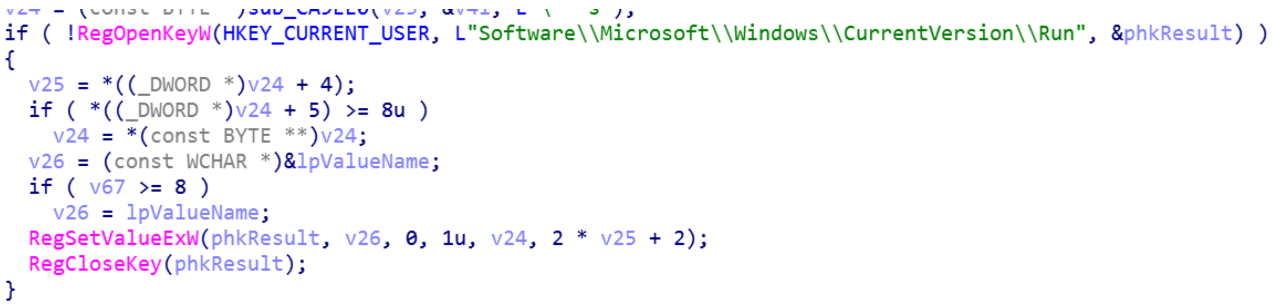
Detection in tLab system

One can also observe this activity through the system call logs

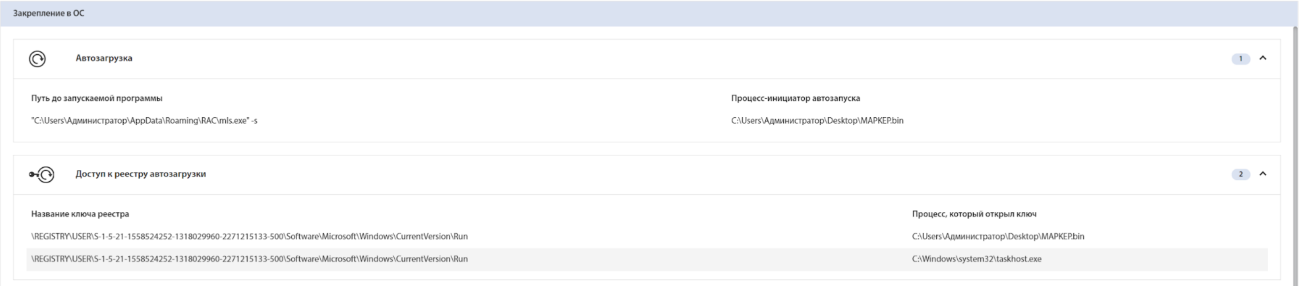


```
2676 - 15499) NtClose(Handle - 0x354). res: 0
2676 - 15500 - 2680)  NtQueryValueKey(KeyHandle - 0x358, ValueName - Cookies), ResultLength - 7c, result - 0x0
    KeyName - \REGISTRY\USER\S-1-5-21-1558524252-1318029960-2271215133-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
2676 - 15501) NtClose(Handle - 0x358). res: 0
2676 - 15502) NtQueryAttributesFile(FileName - C:\Users\Администратор\AppData\Roaming\Microsoft\Windows\Cookies, ObjectAttributes.RootDirectory: 0x0).out: res: 0
2676 - 15503) NtQueryAttributesFile(FileName - C:\Users\Администратор\AppData\Roaming\RAC\mls.exe, ObjectAttributes.RootDirectory: 0x0).out: res: 0
2676 - 15504) NtOpenFile(FileName - C:\, DesiredAccess - 0x100001(FILE_READ_DATA | FILE_READ_ATTRIBUTES | FILE_LIST_DIRECTORY), CreateOptions: 0x40204020, ObjectAttributes.Attribs - 0x40(OBJ_CASE_INSENSITIVE), ObjectAttributes.RootDirectory:
0x0).out: FileHandle - 0x358. res: 0
2676 - 15505) NtClose(Handle - 0x358). res: 0
2676 - 15506) NtOpenFile(FileName - C:\Users\Администратор\, DesiredAccess - 0x100001(FILE_READ_DATA | FILE_READ_ATTRIBUTES | FILE_LIST_DIRECTORY), CreateOptions: 0x40204020, ObjectAttributes.Attribs - 0x40(OBJ_CASE_INSENSITIVE),
ObjectAttributes.RootDirectory: 0x0).out: FileHandle - 0x358. res: 0
2676 - 15507) NtClose(Handle - 0x358). res: 0
2676 - 15508) NtOpenFile(FileName - C:\Users\Администратор\AppData\, DesiredAccess - 0x100001(FILE_READ_DATA | FILE_READ_ATTRIBUTES | FILE_LIST_DIRECTORY), CreateOptions: 0x40204020, ObjectAttributes.Attribs - 0x40(OBJ_CASE_INSENSITIVE),
ObjectAttributes.RootDirectory: 0x0).out: FileHandle - 0x358. res: 0
2676 - 15509) NtClose(Handle - 0x358). res: 0
2676 - 15510) NtOpenFile(FileName - C:\Users\Администратор\AppData\Roaming\, DesiredAccess - 0x100001(FILE_READ_DATA | FILE_READ_ATTRIBUTES | FILE_LIST_DIRECTORY), CreateOptions: 0x40204020, ObjectAttributes.Attribs -
0x40(OBJ_CASE_INSENSITIVE), ObjectAttributes.RootDirectory: 0x0).out: FileHandle - 0x358. res: 0
2676 - 15511) NtClose(Handle - 0x358). res: 0
2676 - 15512) NtOpenFile(FileName - C:\Users\Администратор\AppData\Roaming\RAC\, DesiredAccess - 0x100001(FILE_READ_DATA | FILE_READ_ATTRIBUTES | FILE_LIST_DIRECTORY), CreateOptions: 0x40204020, ObjectAttributes.Attribs -
0x40(OBJ_CASE_INSENSITIVE), ObjectAttributes.RootDirectory: 0x0).out: FileHandle - 0x358. res: 0
2676 - 15513) NtClose(Handle - 0x358). res: 0
2676 - 15514) NtCreateFile(Filename - C:\Users\Администратор\AppData\Roaming\RAC\mls.exe, DiseredAccess - 0x120080(FILE_READ_ATTRIBUTES), CreateDisposition: 0x1, CreateOptions: 0x60, ObjectAttributes.Attribs - 0x40(OBJ_CASE_INSENSITIVE),
ObjectAttributes.RootDirectory: 0x0).out: File handle - 0x358, IoStatusBlock.Information: 0x1. res: 0
```

Next, mls.exe sets itself to startup in the registry with the -s parameter:



```
if ( !RegOpenKeyW(HKEY_CURRENT_USER, L"Software\\Microsoft\\Windows\\CurrentVersion\\Run", &phkResult) )
{
  v25 = *((_DWORD *)v24 + 4);
  if ( *((_DWORD *)v24 + 5) >= 8u )
    v24 = *(const BYTE **)v24;
  v26 = (const WCHAR *)&lpValueName;
  if ( v67 >= 8 )
    v26 = lpValueName;
  RegSetValueExW(phkResult, v26, 0, 1u, v24, 2 * v25 + 2);
  RegCloseKey(phkResult);
}
```



Закрепление в ОС

Автозагрузка

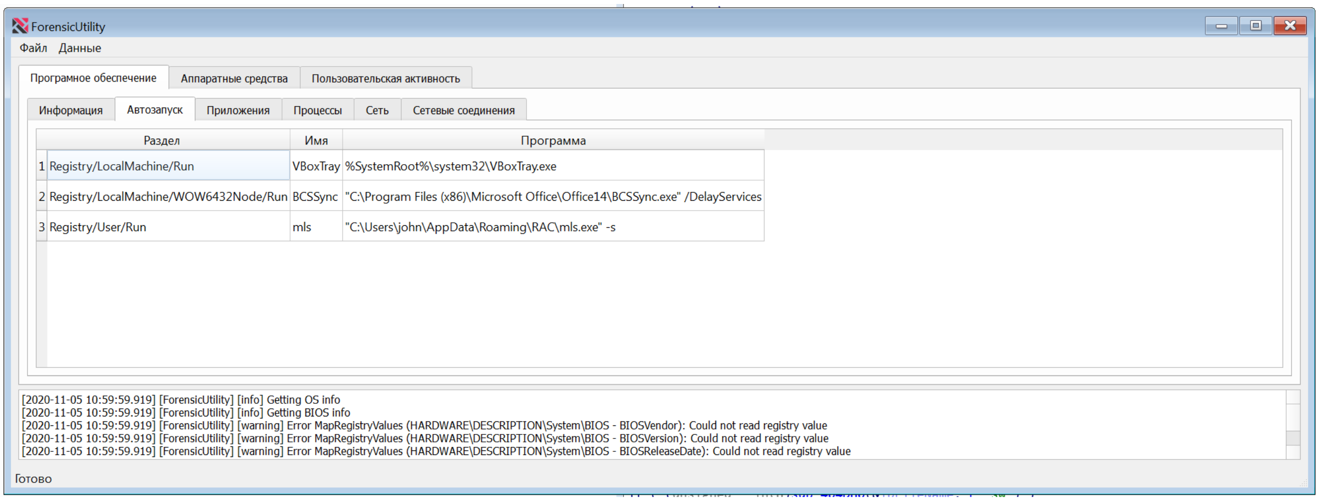
Путь до запускаемой программы	Процесс-инициатор автозапуска
"C:\Users\Администратор\AppData\Roaming\RAC\mls.exe" -s	C:\Users\Администратор\Desktop\MAPKEP.bin

Доступ к реестру автозагрузки

Название ключа реестра	Процесс, который открыл ключ
\REGISTRY\USER\S-1-5-21-1558524252-1318029960-2271215133-500\Software\Microsoft\Windows\CurrentVersion\Run	C:\Users\Администратор\Desktop\MAPKEP.bin
\REGISTRY\USER\S-1-5-21-1558524252-1318029960-2271215133-500\Software\Microsoft\Windows\CurrentVersion\Run	C:\Windows\system32\taskhost.exe

Autoload indication on the tLab system

The file is present in the AutoStartup section of the T&T Security forensics tool

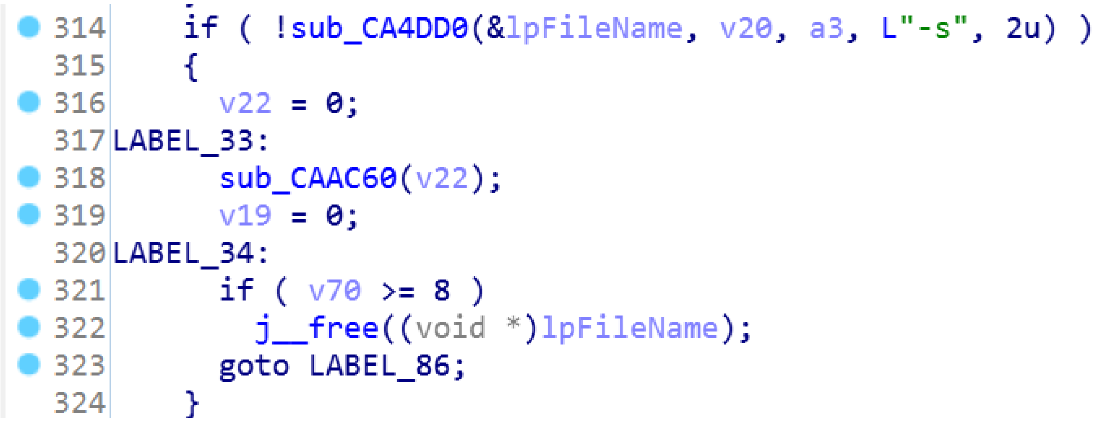


	Раздел	Имя	Программа
1	Registry/LocalMachine/Run	VBoxTray	%SystemRoot%\system32\VBoxTray.exe
2	Registry/LocalMachine/WOW6432Node/Run	BCSSync	"C:\Program Files (x86)\Microsoft Office\Office14\BCSSync.exe" /DelayServices
3	Registry/User/Run	mls	"C:\Users\john\AppData\Roaming\RAC\mls.exe" -s

```
[2020-11-05 10:59:59.919] [ForensicUtility] [info] Getting OS info
[2020-11-05 10:59:59.919] [ForensicUtility] [info] Getting BIOS info
[2020-11-05 10:59:59.919] [ForensicUtility] [warning] Error MapRegistryValues (HARDWARE\DESCRIPTION\System\BIOS - BIOSVendor): Could not read registry value
[2020-11-05 10:59:59.919] [ForensicUtility] [warning] Error MapRegistryValues (HARDWARE\DESCRIPTION\System\BIOS - BIOSVersion): Could not read registry value
[2020-11-05 10:59:59.919] [ForensicUtility] [warning] Error MapRegistryValues (HARDWARE\DESCRIPTION\System\BIOS - BIOSReleaseDate): Could not read registry value
```

Malicious file at autorun in T&T Security forensics tool

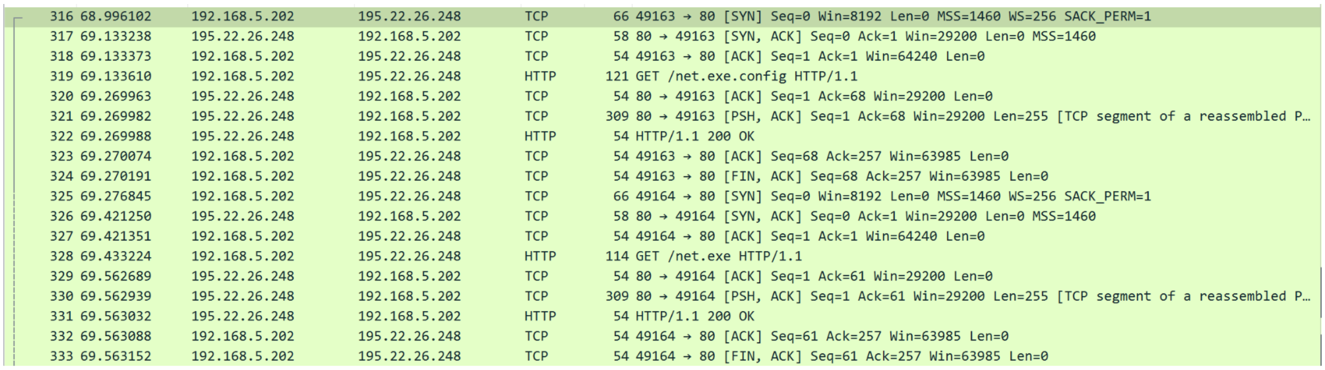
After rebooting, mls.exe will run with the -s option



```
    if ( !sub_CA4DD0(&lpFileName, v20, a3, L"-s", 2u) )
    {
      v22 = 0;
LABEL_33:
      sub_CAAC60(v22);
      v19 = 0;
LABEL_34:
      if ( v70 >= 8 )
        j__free((void *)lpFileName);
      goto LABEL_86;
    }
```

The condition for the file restart

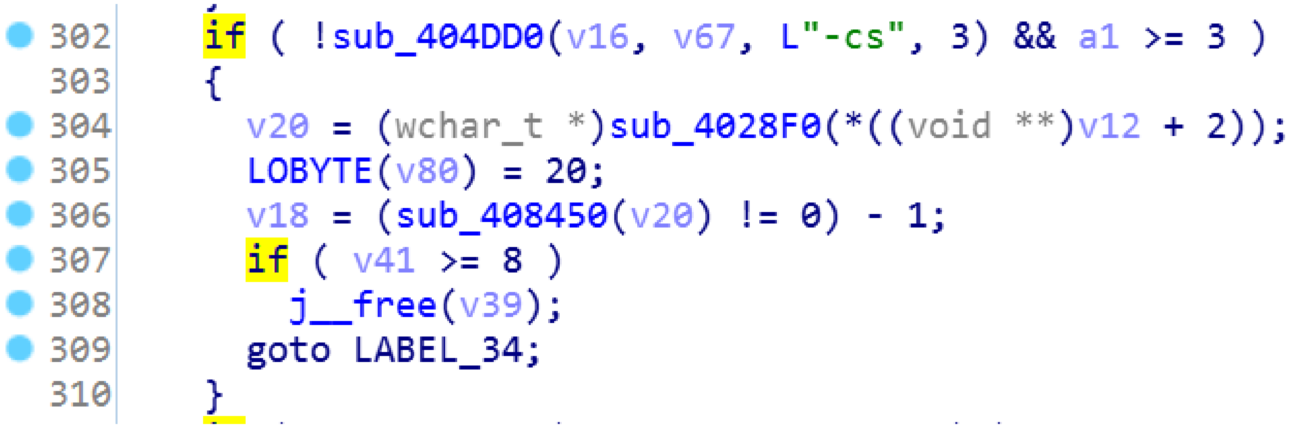
After starting with the -s parameter, it calls the addresses hxxp: //wxanalytics.ru/net.exe.config and hxxp: //wxanalytics.ru/net.exe



```
316 68.996102   192.168.5.202   195.22.26.248   TCP    66 49163 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
317 69.133238   195.22.26.248   192.168.5.202   TCP    58 80 → 49163 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
318 69.133373   192.168.5.202   195.22.26.248   TCP    54 49163 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
319 69.133610   192.168.5.202   195.22.26.248   HTTP  121 GET /net.exe.config HTTP/1.1
320 69.269963   195.22.26.248   192.168.5.202   TCP    54 80 → 49163 [ACK] Seq=1 Ack=68 Win=29200 Len=0
321 69.269982   195.22.26.248   192.168.5.202   TCP   309 80 → 49163 [PSH, ACK] Seq=1 Ack=68 Win=29200 Len=255 [TCP segment of a reassembled P…
322 69.269988   195.22.26.248   192.168.5.202   HTTP   54 HTTP/1.1 200 OK
323 69.270074   192.168.5.202   195.22.26.248   TCP    54 49163 → 80 [ACK] Seq=68 Ack=257 Win=63985 Len=0
324 69.270191   192.168.5.202   195.22.26.248   TCP    54 49163 → 80 [FIN, ACK] Seq=68 Ack=257 Win=63985 Len=0
325 69.276845   192.168.5.202   195.22.26.248   TCP    66 49164 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
326 69.421250   195.22.26.248   192.168.5.202   TCP    58 80 → 49164 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
327 69.421351   192.168.5.202   195.22.26.248   TCP    54 49164 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
328 69.433224   192.168.5.202   195.22.26.248   HTTP  114 GET /net.exe HTTP/1.1
329 69.562689   195.22.26.248   192.168.5.202   TCP    54 80 → 49164 [ACK] Seq=1 Ack=61 Win=29200 Len=0
330 69.562939   195.22.26.248   192.168.5.202   TCP   309 80 → 49164 [PSH, ACK] Seq=1 Ack=61 Win=29200 Len=255 [TCP segment of a reassembled P…
331 69.563032   195.22.26.248   192.168.5.202   HTTP   54 HTTP/1.1 200 OK
332 69.563088   192.168.5.202   195.22.26.248   TCP    54 49164 → 80 [ACK] Seq=61 Ack=257 Win=63985 Len=0
333 69.563152   192.168.5.202   195.22.26.248   TCP    54 49164 → 80 [FIN, ACK] Seq=61 Ack=257 Win=63985 Len=0
```

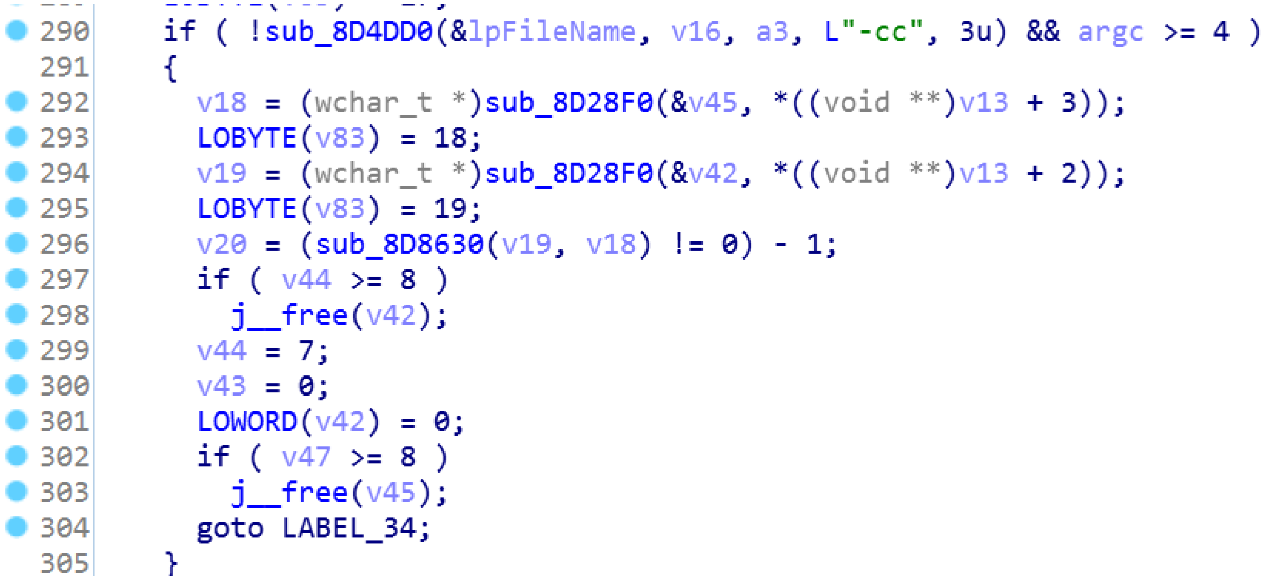
PCAP file content view on the tLab system

The file can run with the -cs and -cc options. In this case, it takes the location path for the original malicious file.



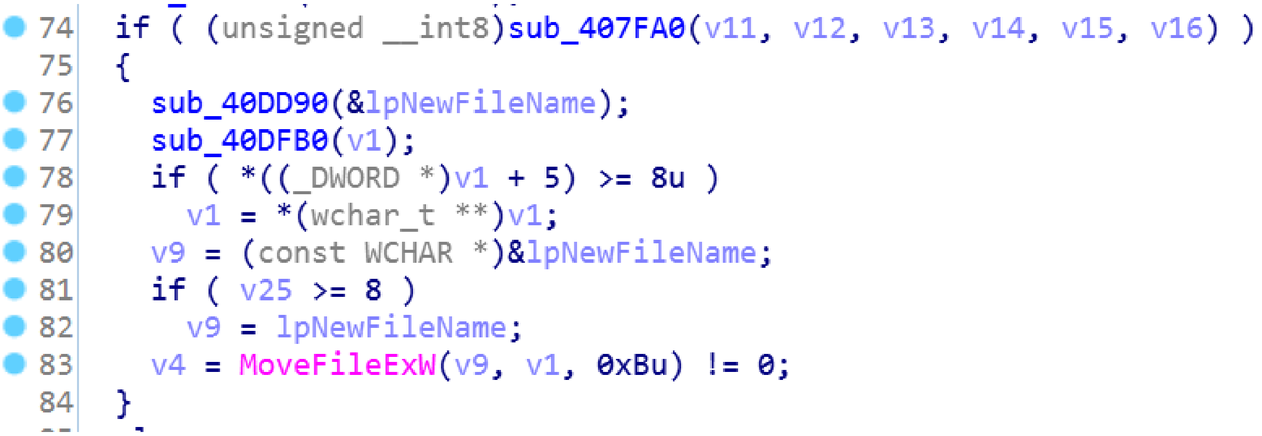
```
if ( !sub_404DD0(v16, v67, L"-cs", 3) && a1 >= 3 )
{
  v20 = (wchar_t *)sub_4028F0(*((void **)v12 + 2));
  LOBYTE(v80) = 20;
  v18 = (sub_408450(v20) != 0) - 1;
  if ( v41 >= 8 )
    j__free(v39);
  goto LABEL_34;
}
```

Handling the -cs parameter



```
if ( !sub_8D4DD0(&lpFileName, v16, a3, L"-cc", 3u) && argc >= 4 )
{
  v18 = (wchar_t *)sub_8D28F0(&v45, *((void **)v13 + 3));
  LOBYTE(v83) = 18;
  v19 = (wchar_t *)sub_8D28F0(&v42, *((void **)v13 + 2));
  LOBYTE(v83) = 19;
  v20 = (sub_8D8630(v19, v18) != 0) - 1;
  if ( v44 >= 8 )
    j__free(v42);
  v44 = 7;
  v43 = 0;
  LOWORD(v42) = 0;
  if ( v47 >= 8 )
    j__free(v45);
  goto LABEL_34;
}
```

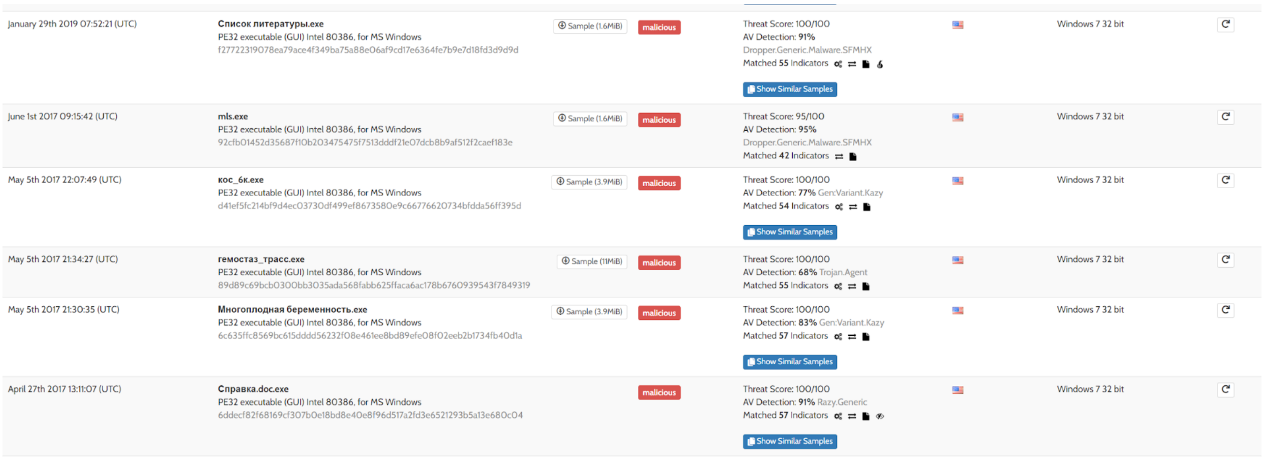
Handling the -cc parameter



```
if ( (unsigned __int8)sub_407FA0(v11, v12, v13, v14, v15, v16) )
{
  sub_40DD90(&lpNewFileName);
  sub_40DFB0(v1);
  if ( *((_DWORD *)v1 + 5) >= 8u )
    v1 = *(wchar_t **)v1;
  v9 = (const WCHAR *)&lpNewFileName;
  if ( v25 >= 8 )
    v9 = lpNewFileName;
  v4 = MoveFileExW(v9, v1, 0xBu) != 0;
}
```

File moving code

By looking at the list of malicious files that have accessed the same addresses, we will see they have different names.

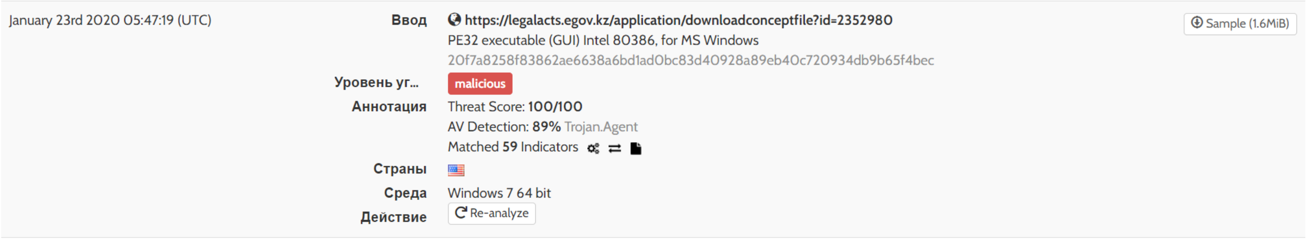


January 29th 2019 07:52:21 (UTC)	**Список литературы.exe** PE32 executable (GUI) Intel 80386, for MS Windows f27722319078ea79ace4f349ba75a88e06af9cd17e6364fe7b9e7d18fd3d9d9d	Sample (1.6MiB)	malicious	Threat Score: 100/100 AV Detection: 91% Dropper.Generic.Malware.SFMHX Matched 55 Indicators Show Similar Samples	🇺🇸	Windows 7 32 bit	↻
June 1st 2017 09:15:42 (UTC)	**mls.exe** PE32 executable (GUI) Intel 80386, for MS Windows 92cfb01452d35687f10b203475475f7513dddf21e07dcb8b9af512f2caef183e	Sample (1.6MiB)	malicious	Threat Score: 95/100 AV Detection: 95% Dropper.Generic.Malware.SFMHX Matched 42 Indicators	🇺🇸	Windows 7 32 bit	↻
May 5th 2017 22:07:49 (UTC)	**кос_6к.exe** PE32 executable (GUI) Intel 80386, for MS Windows d41ef5fc214bf9d4ec03730df499ef8673580e9c66776620734bfdda56ff395d	Sample (3.9MiB)	malicious	Threat Score: 100/100 AV Detection: 77% Gen:Variant.Kazy Matched 54 Indicators Show Similar Samples	🇺🇸	Windows 7 32 bit	↻
May 5th 2017 21:34:27 (UTC)	**гемостаз_трасс.exe** PE32 executable (GUI) Intel 80386, for MS Windows 89d89c69bcb0300bb3035ada568fabb625ffaca6ac178b6760939543f7849319	Sample (11MiB)	malicious	Threat Score: 100/100 AV Detection: 68% Trojan.Agent Matched 55 Indicators	🇺🇸	Windows 7 32 bit	↻
May 5th 2017 21:30:35 (UTC)	**Многоплодная беременность.exe** PE32 executable (GUI) Intel 80386, for MS Windows 6c635ffc8569bc615dddd56232f08e461ee8bd89efe08f02eeb2b1734fb40d1a	Sample (3.9MiB)	malicious	Threat Score: 100/100 AV Detection: 83% Gen:Variant.Kazy Matched 57 Indicators Show Similar Samples	🇺🇸	Windows 7 32 bit	↻
April 27th 2017 13:11:07 (UTC)	**Справка.doc.exe** PE32 executable (GUI) Intel 80386, for MS Windows 6ddecf82f68169cf307b0e18bd8e40e8f96d517a2fd3e6521293b5a13e680c04		malicious	Threat Score: 100/100 AV Detection: 91% Razy.Generic Matched 57 Indicators Show Similar Samples	🇺🇸	Windows 7 32 bit	↻

List of malicious files accessing vwanalytics.ru

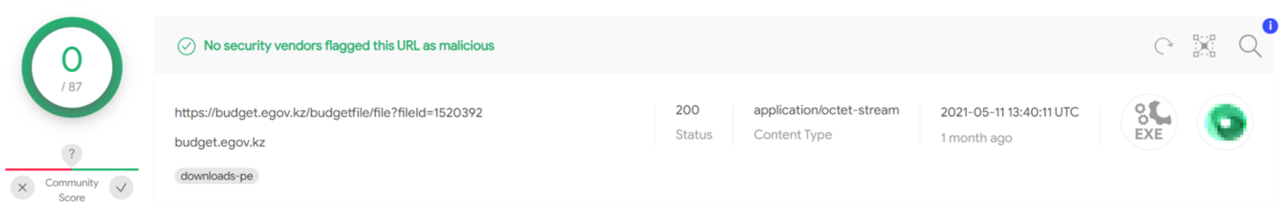
Attackers often name malicious files based on the area of interest of potential victims.

Several samples of malicious files on this list were uploaded documents to legalacts.egov.kz and budget.egov.kz. As previously noted, this type of attack is called a watering hole attack.



January 23rd 2020 05:47:19 (UTC)	**Ввод**	**https://legalacts.egov.kz/application/downloadconceptfile?id=2352980** PE32 executable (GUI) Intel 80386, for MS Windows 20f7a8258f83862ae6638a6bd1ad0bc83d40928a89eb40c720934db9b65f4bec
	Уровень ур...	malicious
	Аннотация	Threat Score: **100/100** AV Detection: **89%** Trojan.Agent Matched **59** Indicators
	Страны	🇺🇸
	Среда	Windows 7 64 bit
	Действие	↻ Re-analyze

Sample (1.6MiB)



No security vendors flagged this URL as malicious

https://budget.egov.kz/budgetfile/file?fileId=1520392
budget.egov.kz
downloads-pe

200	application/octet-stream	2021-05-11 13:40:11 UTC
Status	Content Type	1 month ago

Malicious links:

- hxxps://budget.egov.kz/budgetfile/file?fileId=1520392
- hxxps://legalacts.egov.kz/application/downloadnpa?id=532231

The files are the same old malicious Razy downloader Trojan. We assume that cybercriminals published malicious software under the guise of DOCX by gaining access to uploading files to the legalacts.egov.kz site. As of May 11, 2021, only a few well-known anti-viruses identified the object, while none of them could detect the link to the object itself as malicious.

Conclusion

These days even an ordinary user can unravel such techniques as hiding files and faking the icons.
The malicious Trojan downloader itself is not packed in any way to stay undetected by the antivirus signature. The file creation date indicates the use of old-style malware. The hash sums of the studied samples (without resources) coincide with so many other files seen in similar attacks.
All this suggests that the attackers, in this case, used quite an old malware, changing only the office document displayed to the user, which indicates the low qualifications of the attacker. Regardless, the Razy Trojan still poses a live threat and uses actual white papers.