

# What's behind the NewsJacking

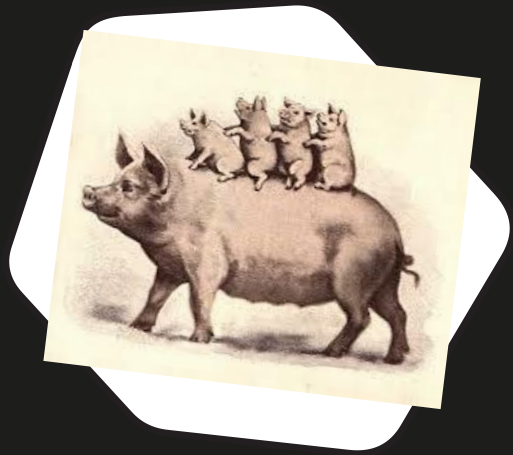


---

## Intro – What is NewsJacking ?

2

Newsjacking is the practice of aligning a brand with a current event in an attempt to generate media attention and boost the brand's exposure. Companies create related blog content and social posts to instantly reach a wider audience.



Newsjacking is a term coined by David Meerman Scott in his book, “Newsjacking.” According to Scott, Newsjacking is the process of adding your thoughts and opinions into breaking news stories. It's piggybacking on trending news topics to get yourself noticed!

The (Kaspersky intelligence) coding for this is TR\_%var%newsjacking

*We discovered an active phishing campaign, spreading both phishing emails and malicious pages on the behalf of the national ...*

Summer 2022

3

# Danas

☰ Najnovije Vesti ▾ Na lokalu ▾

Свет Политика Друштво

Početna ▶ Dijalog ▶ Lični stavovi ▶ „Hakerski napad“

■ LIČNI STAVOVI |

## „Hakerski napad na RGZ: Kolaps“

### Хакерски напад на РГЗ: Колас

Сви термини које су користили хакери су пропали, а заказаних проради



# ПОЛИТИКА

Top Latest People Photos Videos



TV N1 Beograd @N1infoBG · Jun 20

Rodić: Napad na RGZ deo trenda, moguće da je tražen otkup za podatke



rs.n1info.com

Rodić: Napad na RGZ deo trenda, moguće da je tražen otkup za podat...

Hakerski napad na Republički geodetski zavod (RGZ) najverovatnije je "tipični slučaj rensomver napada", rekao je za N1 IT stručnjak i ...

Google search:  
Napad na RGZ

About 29,900  
results

<https://eid.gov.rs> › [uslovi-koriscenja](#) · [Translate this page](#)

[Uslovi korišćenja - eid.gov.rs](#)

Portalom eUpra

Registracija kor

## Otvoren novi objekat u Data centru, prema rečima Brnabić „srce naše bezbednosti“

VESTI | Autor: Milan Nikić, Beta | 07. jul 2022 12:09 > 12:15 | 16 komentara

Podeli: [f](#) [t](#) [e](#) [s](#)



Google search:  
vesti drzavni data  
centar

About 1,310k  
results



---

From an attacker perspective it's only RnR !

5



FileMessageTell me what you want to do...

Bojan Despic <bojan.despic@rgz.gov.rs>Kreiran ugovor eKatastar

Поштовани,  
Креиран Вам је нови уговор број: 09-750/20  
На мејл: [REDACTED]  
Висина таксе за од 0 до 20 упита месечно и


From: admin@eid.gov.rs <admin@eid.gov.rs>  
Sent: Thursday, September 8, 2022 10:29 AM  
To: undisclosed-recipients:  
Subject: eid.gov.rs: Ваш нови подаци за пријаву

FileMessageTell me what you want to do...

Bojan Despic <bnar.doe@strumlineco.com>[REDACTED]  
Re: Kreiran ugovor eKatastar

Goedemorgen  
Met deze brief stuur ik u alle nodige documentatie over onze komende bijeenkomst, precies zoals we onlangs hebben besproken. Bekijk de nodige gegevens via de volgende link:


Ову пошту Влада Србије је аутоматски послала преко eid.gov.rs

eID.gov.rs






Портал за електронску идентификацију

Крећемо са надоградњом веб сајта и одржавањем система. У прилогу су ваши нови подаци за пријаву. Преузмите и сачувајте ову лозинку јер ће вам требати након овог одржавања наше веб странице да би

<https://eid.gov.rs>

eID.gov.rs

Портал за електронску идентификацију



# Threat Intelligence Portal

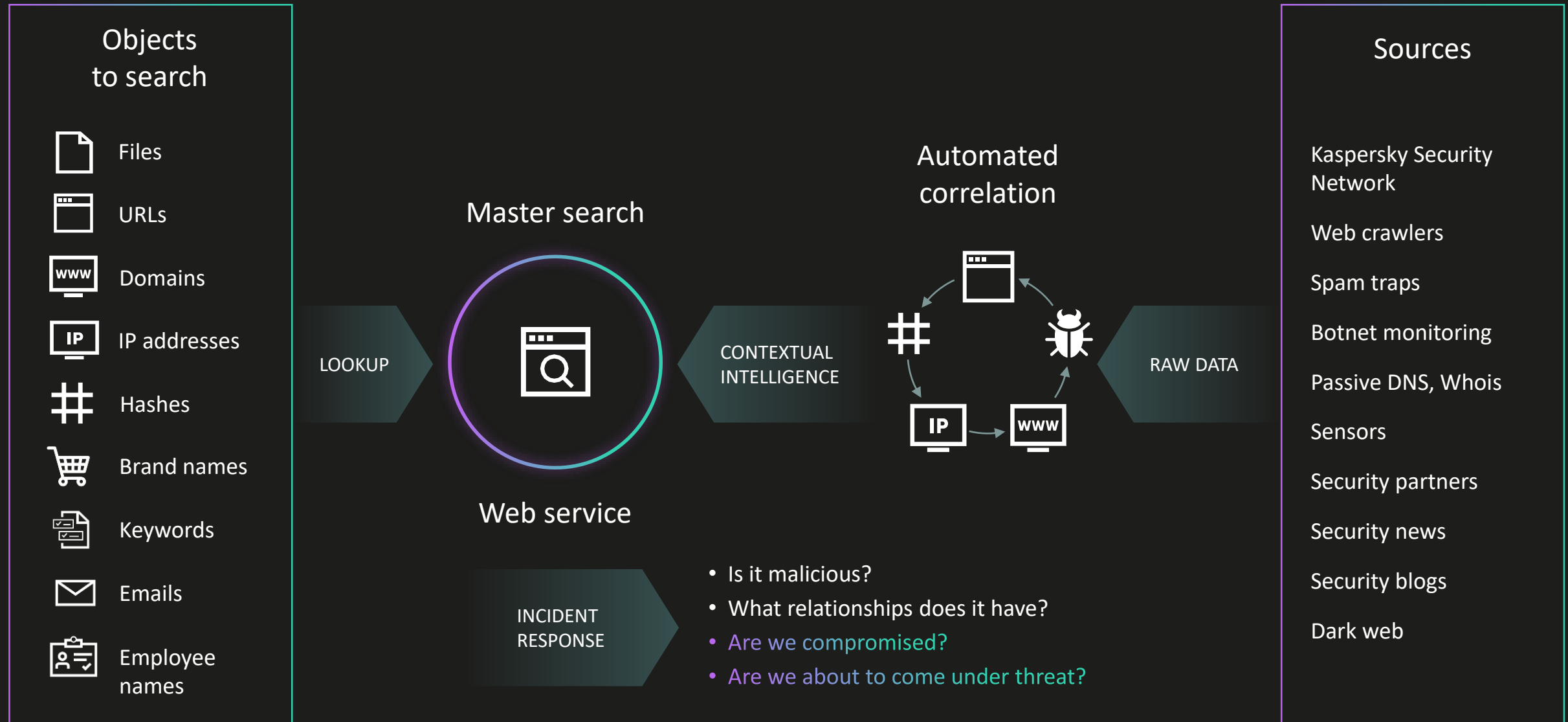
– let's see what's  
behind the candelabra





# Real-time search across Kaspersky's, surface and dark web sources

8





Master Search (RGZ) phishing mail -> url -> malware download -> execution

Threat Lookup

Lookup 1Dark web 10000+Surface web 1629OSINT IoCs 0Reporting 15Actors 0Digital Footprint 0

Daily request quota for your group: 5

Report for web address

dbspssre.com/oelnr

Danger

Threat Lookup

Lookup 1Dark web 0Surface web 0OSINT IoCs 0Reporting 0Actors 0Digital Footprint 0

Daily request quota for your group: 994 of 1000 left

Report for MD5 hash

AEC8FD604B7928C19C8DAABD9755AA71

Malware

Open in research graphCopy requestExport results

Overview

IPv4 count 5File count 2

Categories 1

Files t

Statistics

No data found

WHOIS

Domain name dbspssre.com

Domain status clientDeleteFclientTransfeclientRenewFclientUpdate

Created 19 Apr 2019

Updated 21 Apr 2022

Paid until 19 Apr 2023

Overview

Hits ~ 100

Size 257.88 KB (264069 B)

Signed by —

First seen 15 Feb 2022 18:40

Format xlsb

Packed by —

Signature trust —

Last seen 21 Sep 2022 10:36

Statistics

MD5 AEC8FD604B7928C19C8DAABD9755AA71

SHA-1 11748DB09F0BE4951FCEC653426A434058AB9EF9

Clear

SHA-256 B32346595C2E18E179384B4CD57C28E8D8060BA2C9977B3CDFD5887C0CEE93CB

Categories General

Statistics

No data found

Detection names

16 Feb 2022 05:59

BSS:Exploit.Win32.Generic

15 Feb 2022 23:27

HEUR:Trojan.MSOffice.Emotet.gen

30 Aug 2022 14:12

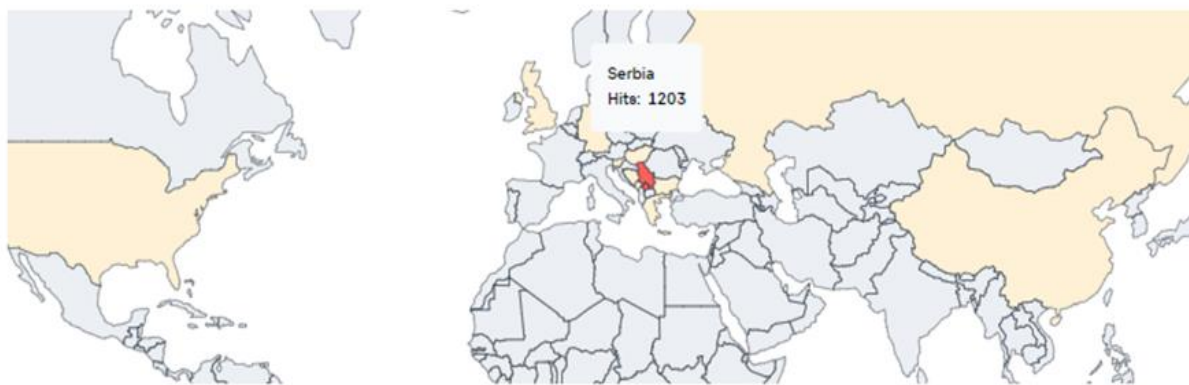
HEUR:Trojan.MSOffice.Generic

21 Sep 2022 12:41

HEUR:Trojan-Downloader.MSOffice.SLoad.gen

## Main results (RGZ)

### Statistics ⓘ



- Source of phishing
- Spread in Serbia ~ 1000 hits
- Newsjacking - RGZ
- Malware distributed via website
- [strumlineco.com/laedlmsu/yh\\_3215567430.zip](http://strumlineco.com/laedlmsu/yh_3215567430.zip)
- URL/Malware dynamic analyses
- Trojan-Downloader.MSOffice.SLoad.gen
- Similarity with EMOTET
- IP used in MIRAI botnet
- Idea, who might be a threat actor

Master Search (eUprava) phishing email -> malware attached -> dropper -> ... -> execution

Threat Lookup

Lookups

Dark web

Surface web

OSINT IoCs

Reporting

Actors

Digital Footprint

Daily request qu

Detection names

Report for

69D86

Malwa

Overview

Hits

Format

MD5

SHA-1

SHA-256

Categories

8 Sep 2022 10:42

Backdoor.Win32.Androm

26 Sep 2022 11:01

HEUR:Trojan-Spy.MSIL.Noon.gen

8 Sep 2022 10:42

PDM:Exploit.Win32.Generic

8 Sep 2022 10:42

PDM:Trojan.Win32.Generic

8 Sep 2022 10:42

Trojan.MSIL.Crypt.sb

8 Sep 2022 10:42

Trojan.MSIL.Inject.sb

8 Sep 2022 10:42

Trojan.Win32.BypassUAC.Agent.sb

8 Sep 2022 10:42

Trojan.Win32.Vimditor.sb

8 Sep 2022 10:42

Trojan.Win32.Zonidel.sb

8 Sep 2022 10:42

Trojan-Dropper.Win32.Injector

8 Sep 2022 10:42

Trojan-PSW.Win32.Stealer.sb

8 Sep 2022 10:42

Trojan-Spy.Win32.AveMaria.sb

File signatures

File downloaded from URLs and domains

Download data

Statistic

No data found

Container sign

No data found

File names

Status	URL	Last downloaded	Domain
Good	websrv3.viser.edu.rs	20 Sep 2022 14:02	websrv3.viser.edu.rs
Good	mail.alatnica-krstic.co.rs	13 Sep 2022 02:08	mail.alatnica-krstic.co.rs
Good	webattach.mail.yandex.net	12 Sep 2022 11:44	webattach.mail.yandex.net
Good	mail.alatnica-krstic.co.rs	9 Sep 2022 12:07	mail.alatnica-krstic.co.rs
Good	cpanel2.orion.rs	8 Sep 2022 20:04	cpanel2.orion.rs
Good	mail.unistours.com	8 Sep 2022 20:02	mail.unistours.com



**Kaspersky**  
**Threat Analysis**  
**Threat attribution**  
**Sandboxing**



Yes, we have sample to sandbox – boom !

Sandb

Report for 79229

Malware

Summary

Detected

Uploaded

Analyzed

Database up

File size

File type

Process creation

Command\_line: "\$selfpath\$selfname.exe"

ImagePath: \$selfpath\$selfname.exe

Process creation

Command\_line: "\$windir\system32\WindowsPowerShell\v1.0\powershell.exe"

ImagePath: \$windir\system32\WindowsPowerShell\v1.0\powershell.exe

Process creation

Command\_line: "powershell Add-MpPreference -ExclusionPath C:\ProgramData\Microsoft\Windows Defender\Signature Updates\B2215298-46F0-4B70-BE96-438D75796097\mpengine.dll"

ImagePath: \$windir\system32\WindowsPowerShell\v1.0\powershell.exe

Adding the File to Autorun via Registry (MITRE: T1547.001 Registry Run Keys / Startup Folder)

Image\_path: \$selfpath\$selfname.exe

registry\_key: \REGISTRY\MACHINE\SOFTWARE\Wow6432No...

Process creation

Command\_line: "\$user\Documents\Adobe5151.exe"

ImagePath: \$user\Documents\Adobe5151.exe

Adding the Open Directory Path in the Run Keys via Registry (MITRE: T1547.001 Registry Run Keys / ...)

Image\_path: \$selfpath\$selfname.exe

registry\_key: \REGISTRY\MACHINE\SOFTWARE\Wow6432No...

Process creation

Command\_line: powershell Add-MpPreference -ExclusionPath C:\ProgramData\Microsoft\Windows Defender\Signature Updates\B2215298-46F0-4B70-BE96-438D75796097\mpengine.dll"

ImagePath: \$windir\system32\WindowsPowerShell\v1.0\powershell.exe

Adding the File to Autorun via Registry (MITRE: T1547.001 Registry Run Keys / Startup Folder)

Image\_path: \$selfpath\$selfname.exe

registry\_key: \REGISTRY\MACHINE\SOFTWARE\Wow6432No...

Dropping and Executing File or Script (MITRE: T1204.002 User Execution: Malicious File).

dropped\_file: \$user\Documents\Adobe5151.exe

dropper\_image\_path: \$selfpath\$selfname.exe

Windows Defender Modification via PowerShell (MITRE: T1562.001 Impair Defenses: Disable or ...)

Command\_line: powershell Add-MpPreference -ExclusionPath C:\ProgramData\Microsoft\Windows Defender\Signature Updates\B2215298-46F0-4B70-BE96-438D75796097\mpengine.dll"

Image\_path: \$windir\system32\WindowsPowerShell\v1.0\powershell.exe

Windows Defender Modification via PowerShell (MITRE: T1562.001 Impair Defenses: Disable or ...)

Command\_line: "\$windir\system32\WindowsPowerShell\v1.0\powershell.exe"

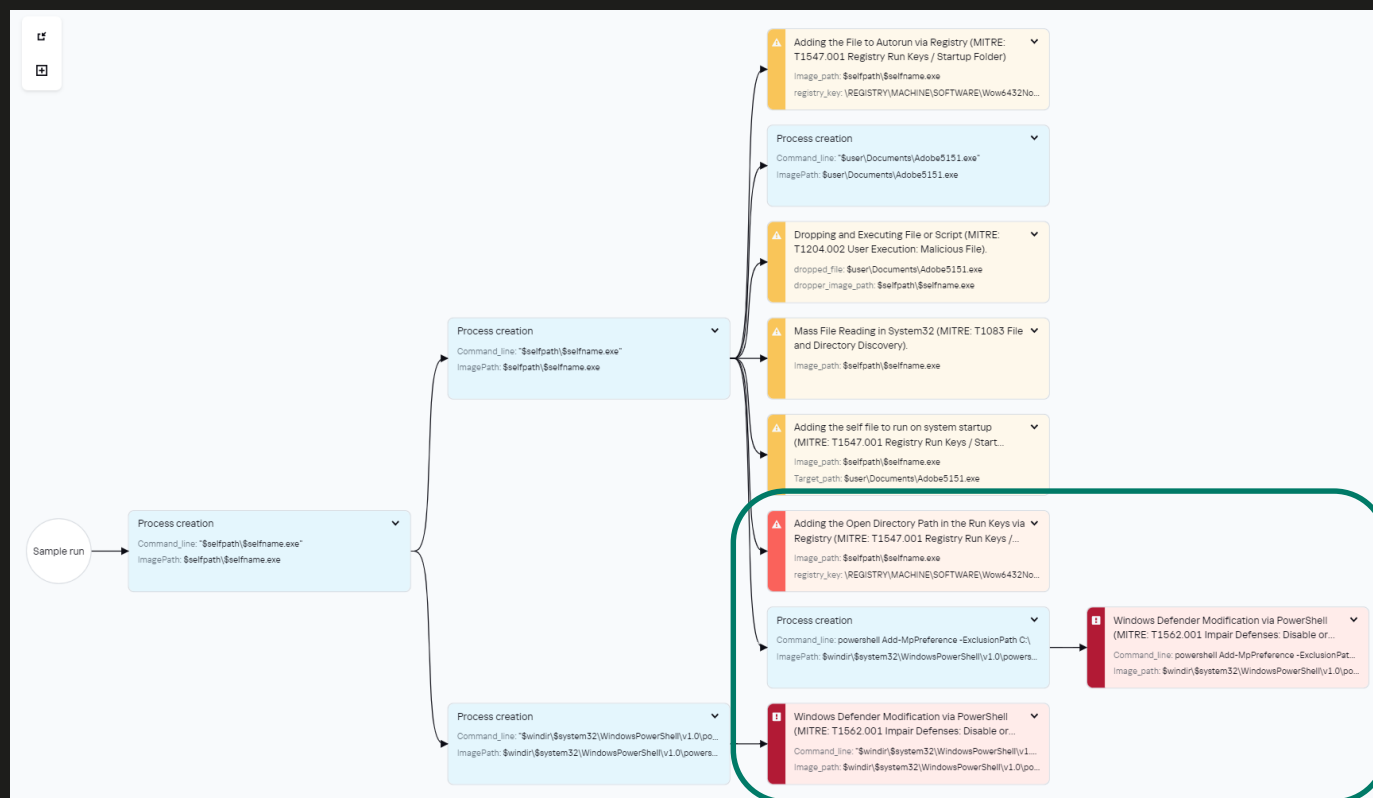
Image\_path: \$windir\system32\WindowsPowerShell\v1.0\powershell.exe

Dropped files ⓘ

Download data

Status	Categories	MD5	Detection name	File name
Malware	—	69D86282FE302BC53974C260A33DB01D	Backdoor.Win32.Androm	Adobe5151.exe

## Main results (eUprava)



- Spread in Serbia mostly
- Newsjacking eUprava
- Malicious code attached
- Dynamic malware analyses
- Trojan-Spy.MSIL.Noon.gen
- Sources of distribution
- MITRE ATT&CK matrix mapping
- Windows Defender – Disable !
- Dropped Backdoor.Win32.Androm
- Trojan.MSIL.Crypt.sb – possible connection with threat actor





# Threat Attribution

Report for file

6390258634227712.zip

Malware

## Summary

MD5	4a1f41b3eb52f70d34aa889e839c0ae6	Matched attribution entities	Similarity not found
File size	745.49 KB (763383 B)	Extracted path	—
Reset similarity thresholds	✕	Unpack	✓

## Sample & Content

	Status	MD5	File name	Size	Bad genotypes (matched/total)	Bad strings (matched/total)	Attribution
<input type="radio"/>	▼  Malware	4a1f41b3eb52f70d34aa889e839c0ae6	6390258634227712.zip	745.49 KB (763383 B)	— (—)	— (—)	Similarity not found
<input checked="" type="radio"/>	Malware	845205b7fd1c98125aaf32399bd3a1a8	Obavestenje o prilivu za 0065328-8375-1105-pdf.exe	938.00 KB (960512 B)	— (—)	22 (23)	BlackremoteRAT

## File content

### Similar samples

Status	Status	MD5	Size	Genotypes matched (total)	Strings matched (total)	Similarity	Attribution entities
Malware	Malware	0678af95de42e923672429dafef872d3	1019.50 KB (1043968 B)	0 (2715)	22 (946)	2	BlackremoteRAT >

Let's continue our hunts !



**Hvala !**  
**Happy Hunting !**

kaspersky