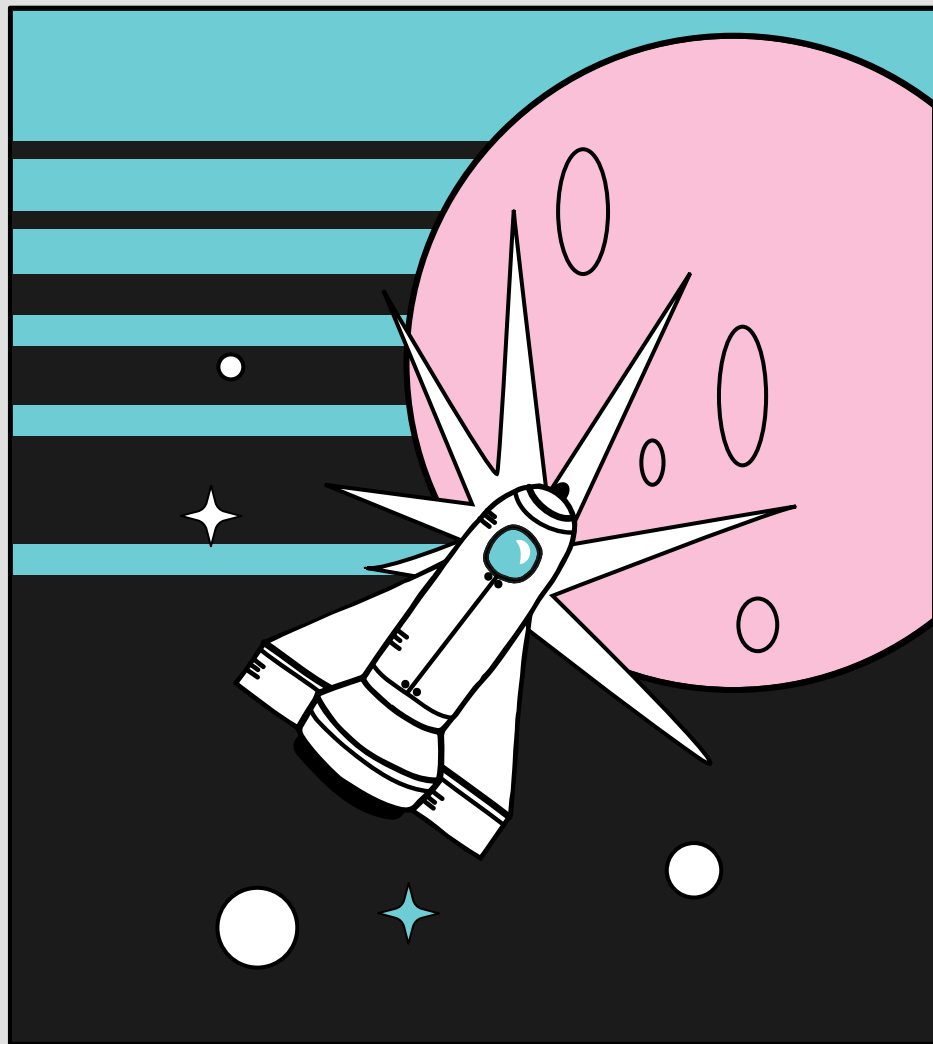




MEET INDRA

Uncovering the Hackers Behind
Attacks on Iran Railways



Who are we?



ALEXANDRA GOFMAN

Malware Analyst @ Threat Intelligence
Analysis Team

🐦 @_lostpacket_

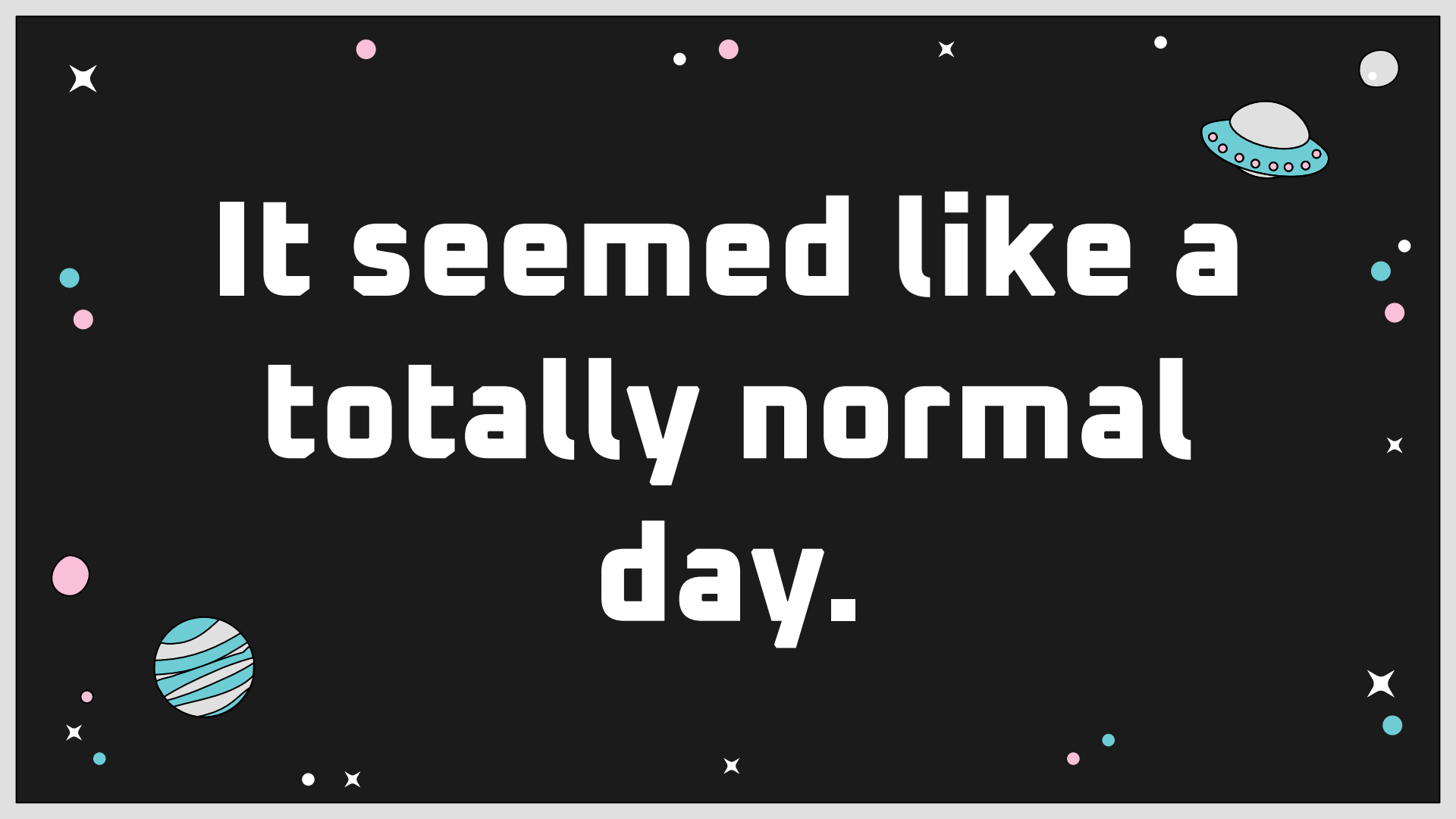


ITAY COHEN

Senior Malware Researcher
Co-Maintainer of **Rizin** & **Cutter**

🐦 @megabeets_



The background is a solid dark navy blue. It is decorated with various space-themed elements: several small white dots of varying sizes representing stars; a few four-pointed white stars; a pink planet in the upper left; a teal planet in the upper right; a light blue planet with horizontal white stripes in the lower left; a teal planet with horizontal white stripes in the lower right; a small teal UFO with a grey dome and a ring of red lights in the upper right; and a small pink planet in the lower left. The text is centered in a large, white, bold, sans-serif font.

**It seemed like a
totally normal
day.**



IRAN RAILWAY SYSTEM

UNDER ATTACK

"Long delays due to cyber attacks.
More information: 64411"



- ✧ **MINISTRY OF ROADS AND
URBAN DEVELOPMENTS
UNDER
ATTACK**



"We have cyber-attacked the computer systems of the Railway Company and the Ministry of Roads and Urban Development!

This message is for the administrator:

Do not extend your legs beyond your rug" .



بانک اطلاعات تهدیدات بدافزاری پادویش وب سایت امن پردار En

خانه / بدافزار / Trojan.Win32.BreakWin

Trojan.Win32.BreakWin2021-07-13

شرح کلی

نوع: تروجان (Trojan)
درجه تخریب: بالا
میزان شیوع در ایران: بالا

تروجان (Trojan) چیست؟

تروجان‌ها نوعی از بدافزار محسوب می‌شوند که خود را در قالب یک نرم‌افزار سالم و قانونی نشان می‌دهند و بسیار شبیه نرم‌افزارهای مفید و کاربردی رفتار می‌کنند. اما هنگامی که اجرا می‌شوند، خرابی‌های زیادی را برای سیستم ایجاد می‌کنند. نرم‌افزارهای دالود شده از اینترنت، جاسازی شدن در متن HTML، ضمیمه شدن به یک ایمیل و ... از جمله راه‌های ورود تروجان‌ها به سیستم هستند. تروجان‌ها برخلاف ویروس‌ها و کرم‌های کامپیوتری قادر به تکثیر خود نیستند.

بدافزار BreakWin چیست؟

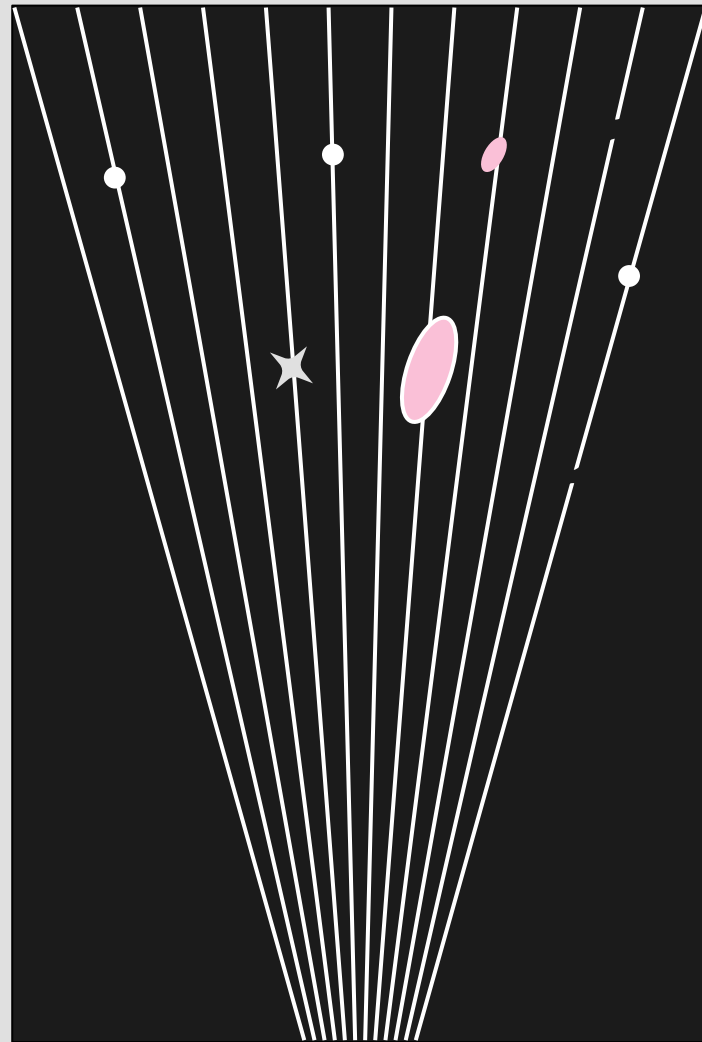
بدافزار ویندوزی Trojan.Win32.BreakWin یک بدافزار از نوع تروجان بوده که خود را منتشر نمی‌کند، بلکه به عنوان بدافزاری جهت از کار انداختن کلاینت‌ها در شبکه‌های مبتنی بر اکثو دایرکتوری مایکروسافت و نیز حذف اطلاعات آنها می‌باشد. این بدافزار برای انتشار نیازمند ابزارهای کمکی و با انتشار دستی می‌باشد.

توضیحات فنی

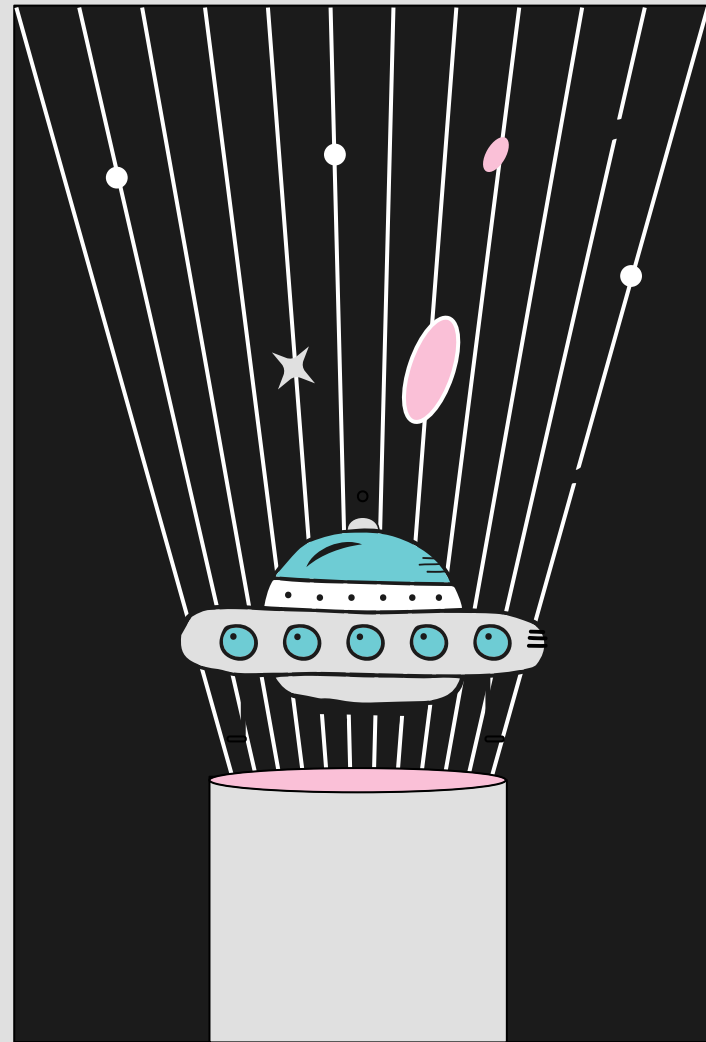
علائم آلودگی

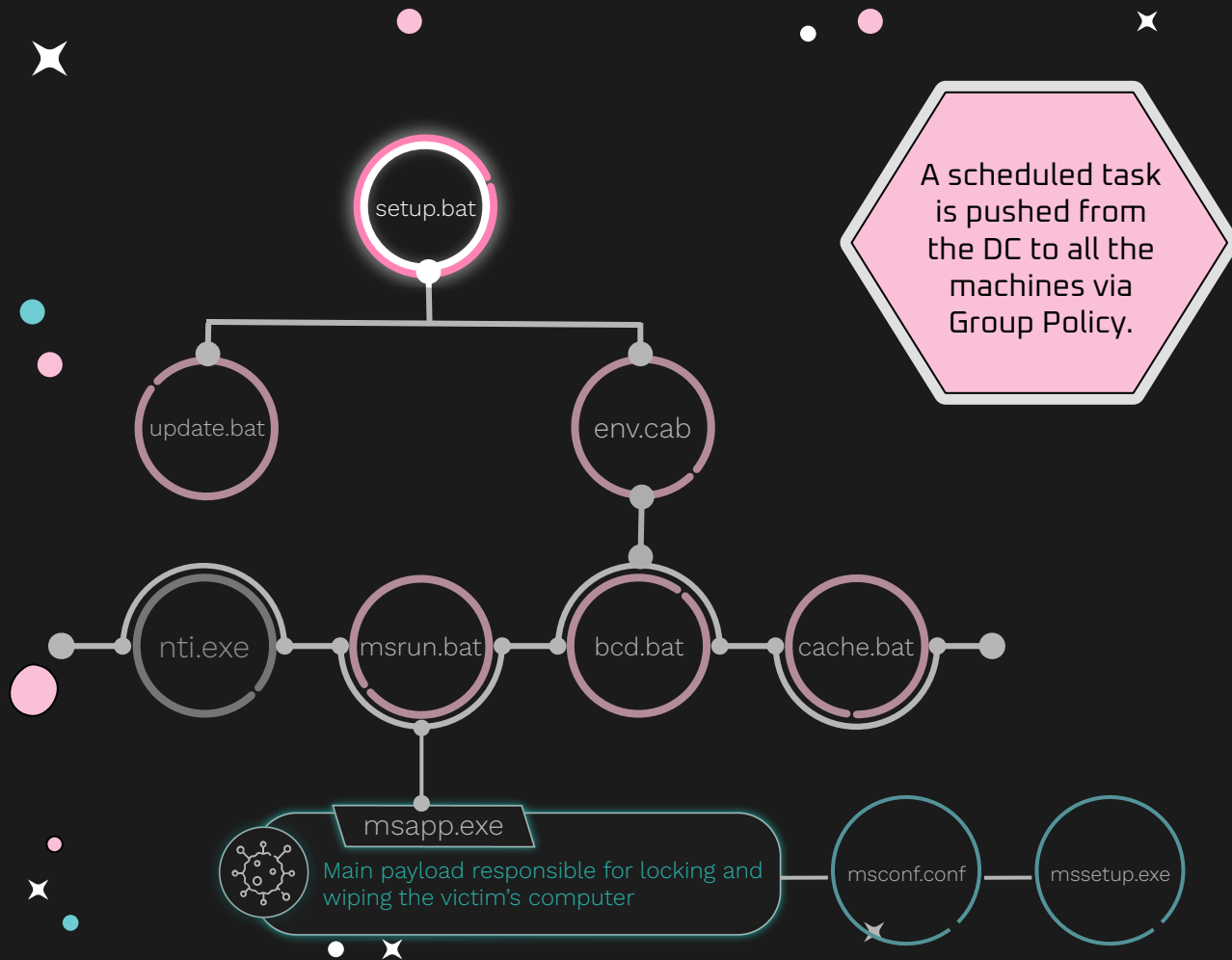
1. غیرفعال شدن کارت شبکه
2. خارج شدن سیستم از اکثو دایرکتوری
3. تغییر رمز عبور سیستم
4. تغییر پس‌زمینه دسکتاپ کاربر و نمایش پیغام مشکوک به جای بوت سیستم
5. تخریب بوت سیستم (bcd و boot.ini)
6. Wipe شدن اطلاعات هارد دیسک

First Lead: Padvish Report

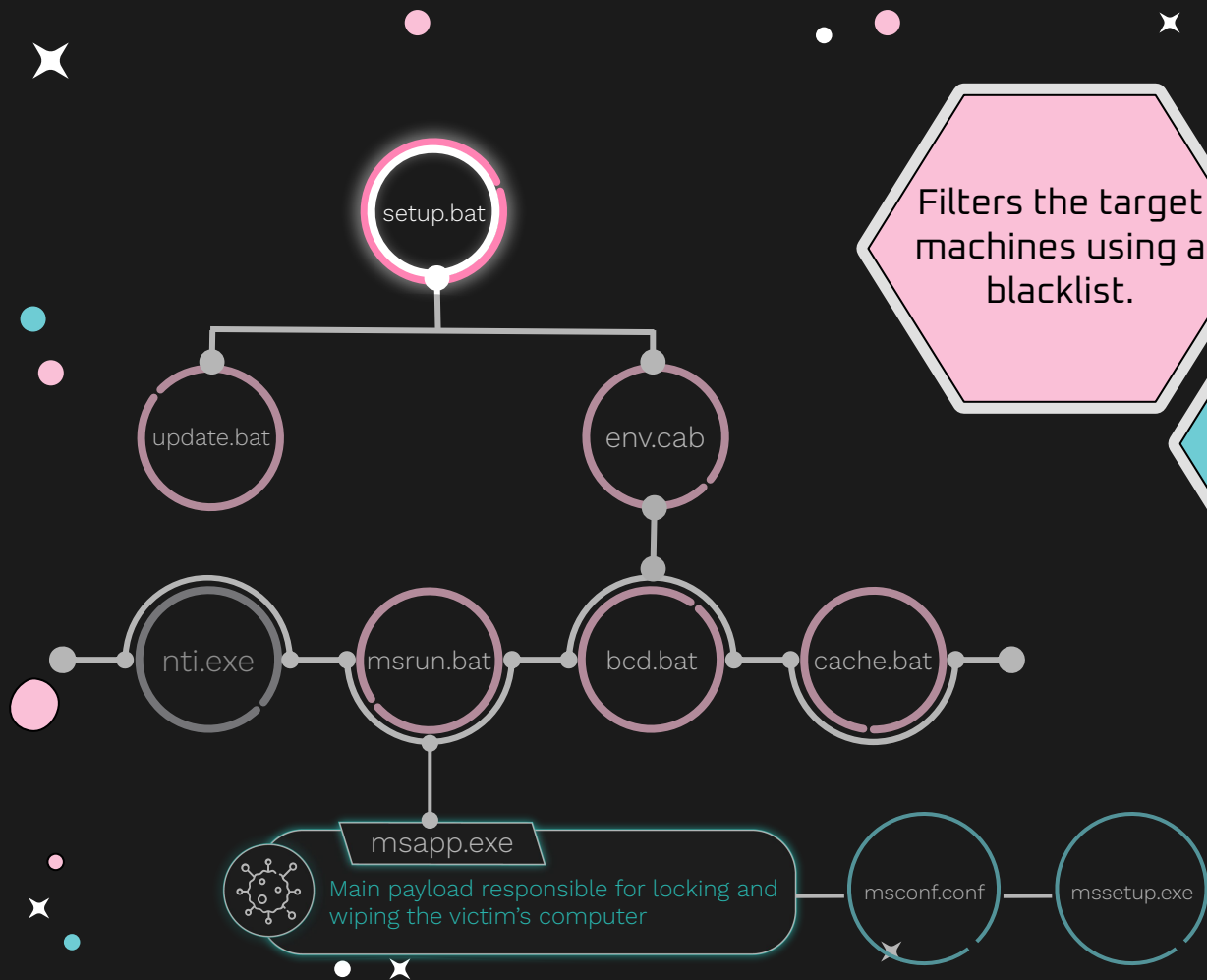


ANALYZING THE SAMPLES





A scheduled task is pushed from the DC to all the machines via Group Policy.

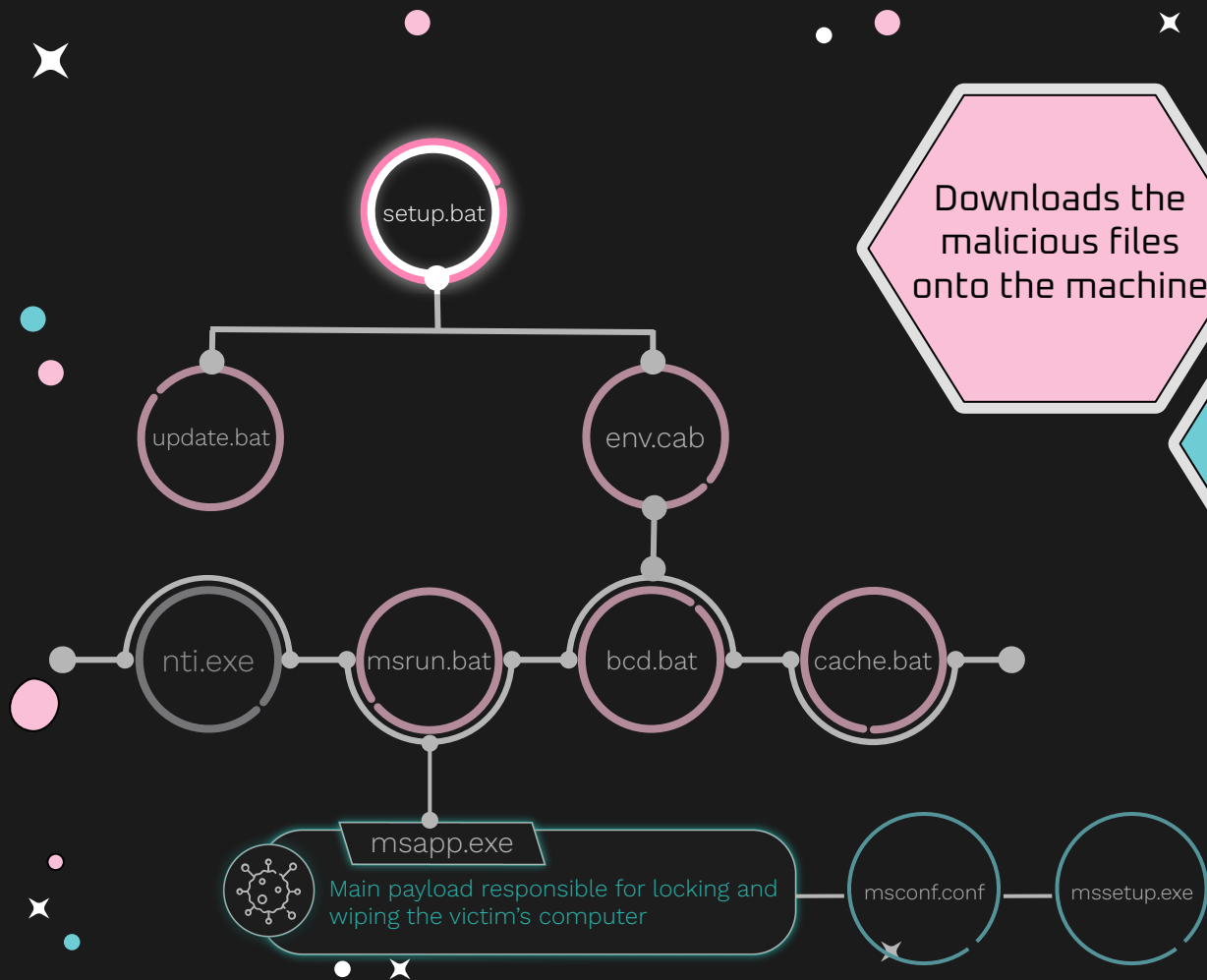


Filters the target machines using a blacklist.

Excluded hostnames:

PIS-APP
PIS-DB
PIS-MOB
WSUSPROXY

PIS stands for **Passenger Information System**

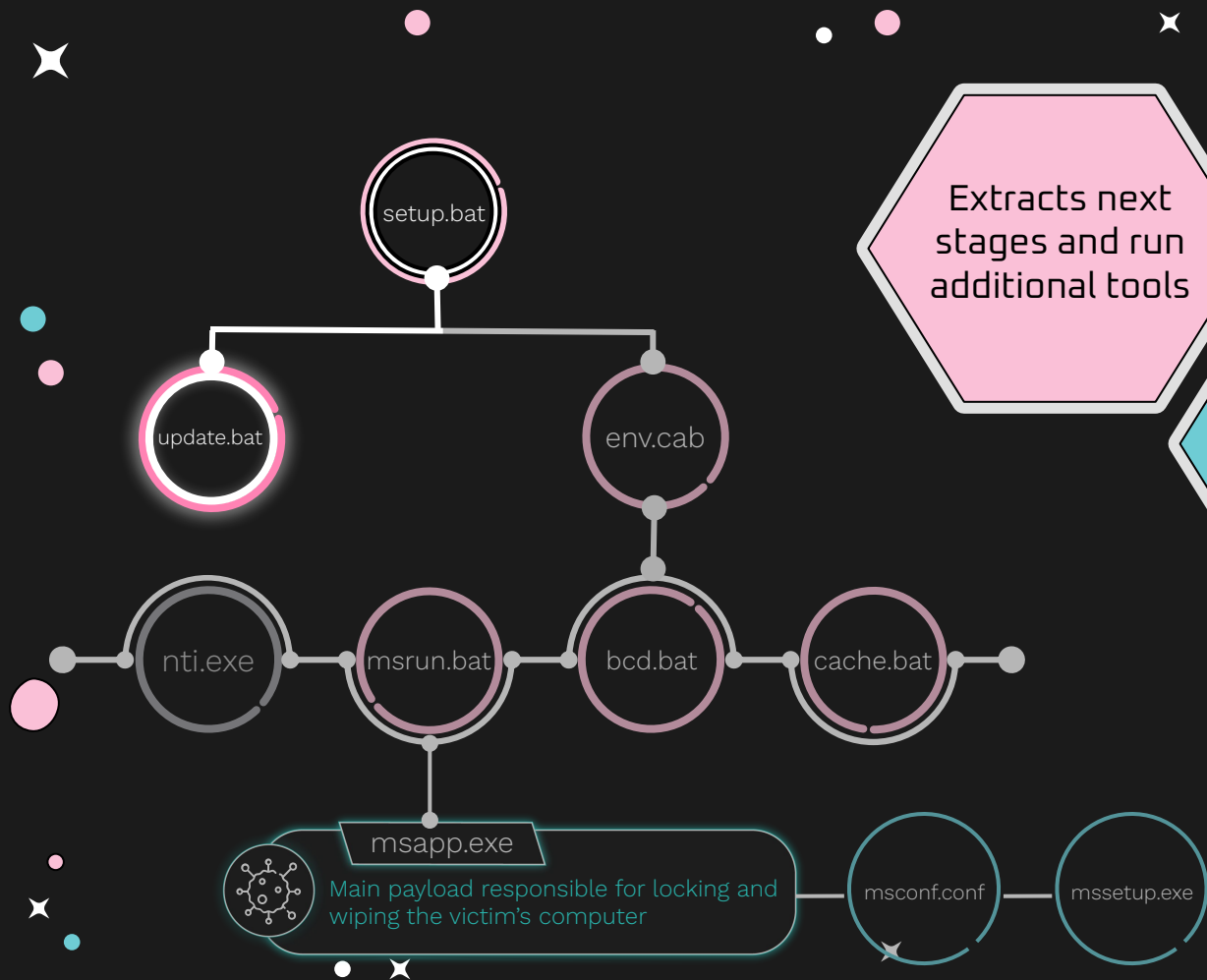


Downloads the
malicious files
onto the machine

Downloads from a
network share

`\\railways.ir\\sysvol\\railways.ir\\
scripts\\env.cab`

Indication of **prior
knowledge** of the
environment.

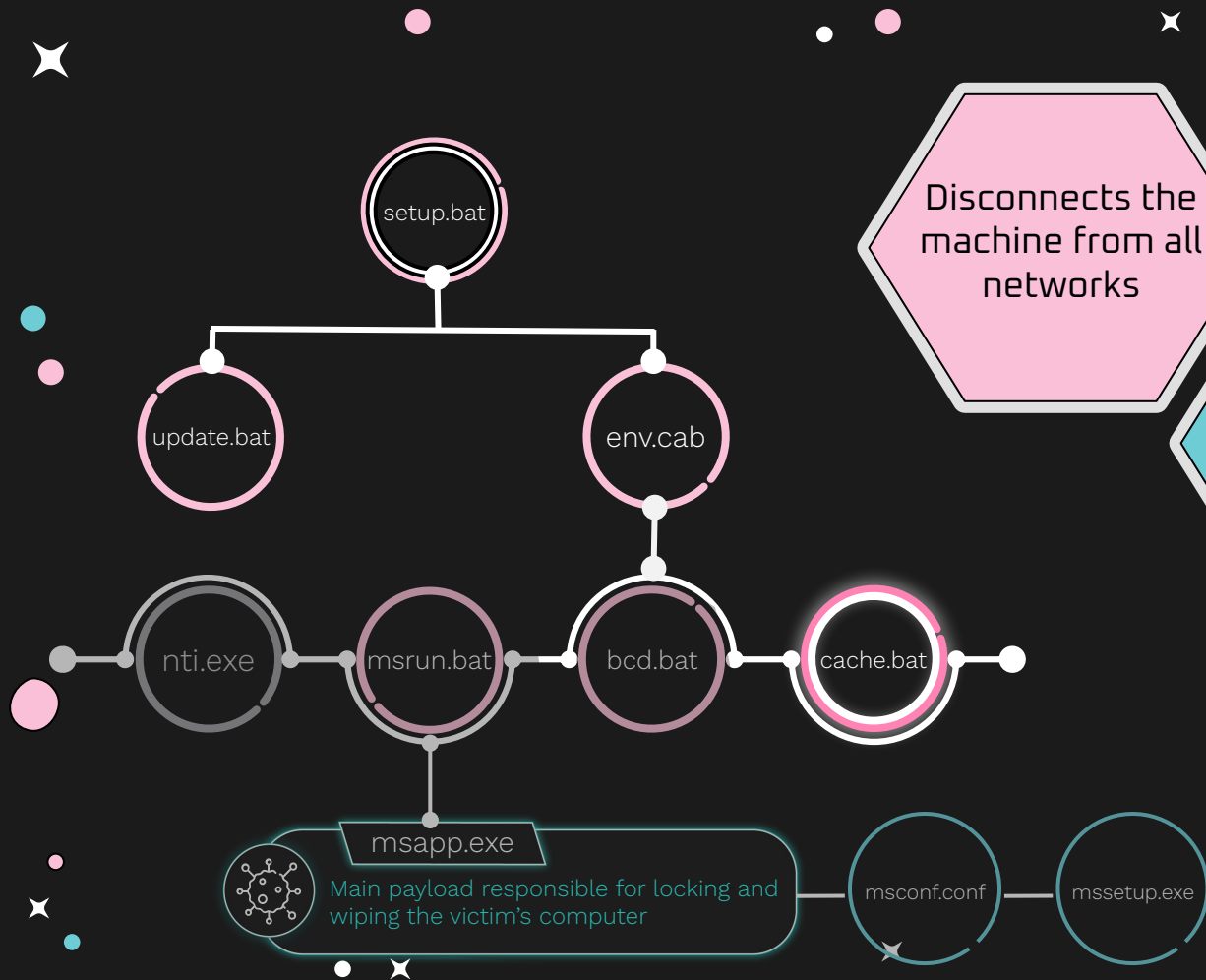


Extracts next stages and run additional tools

All the RAR archives that will be extracted are protected with the following password:

"hackemall"

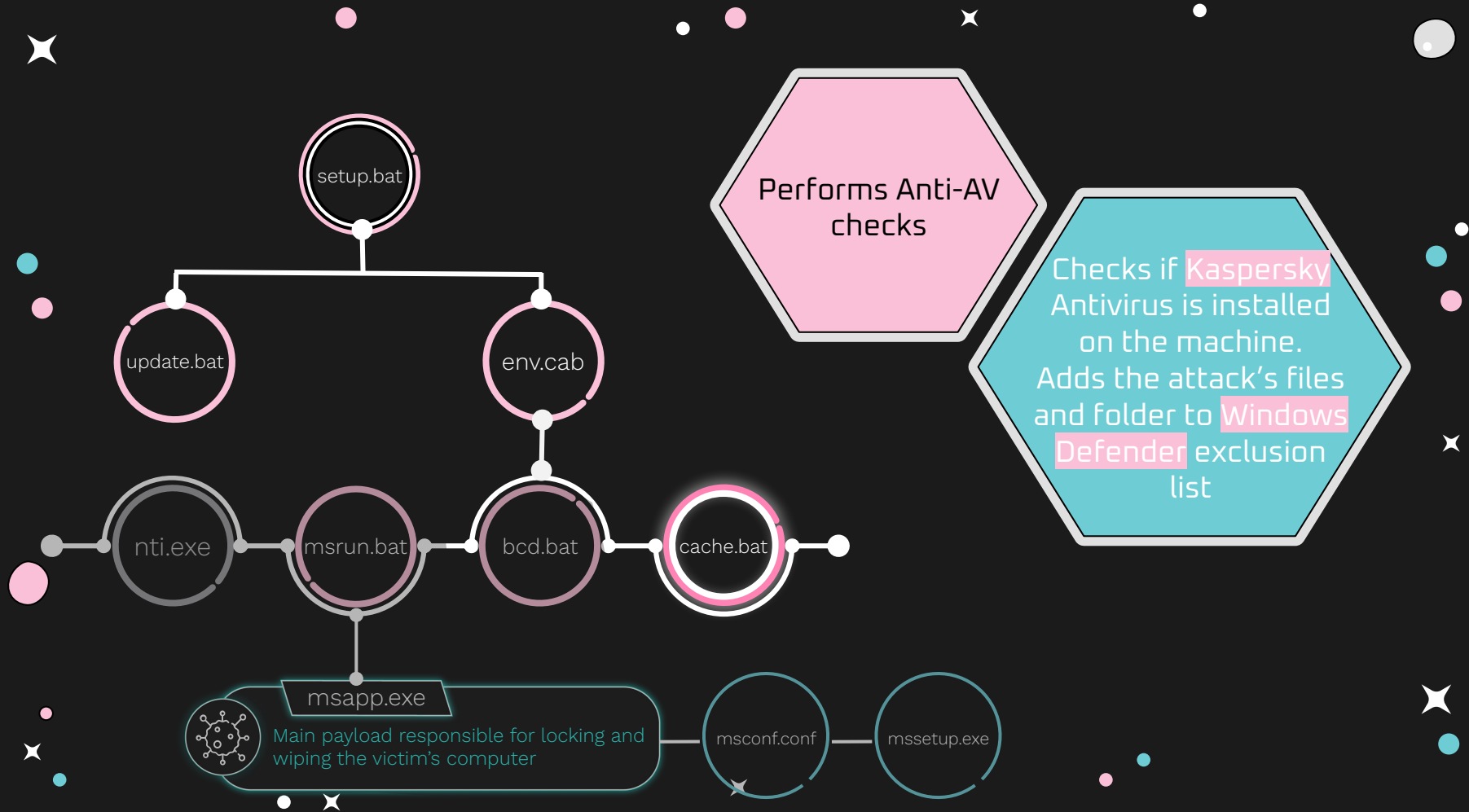


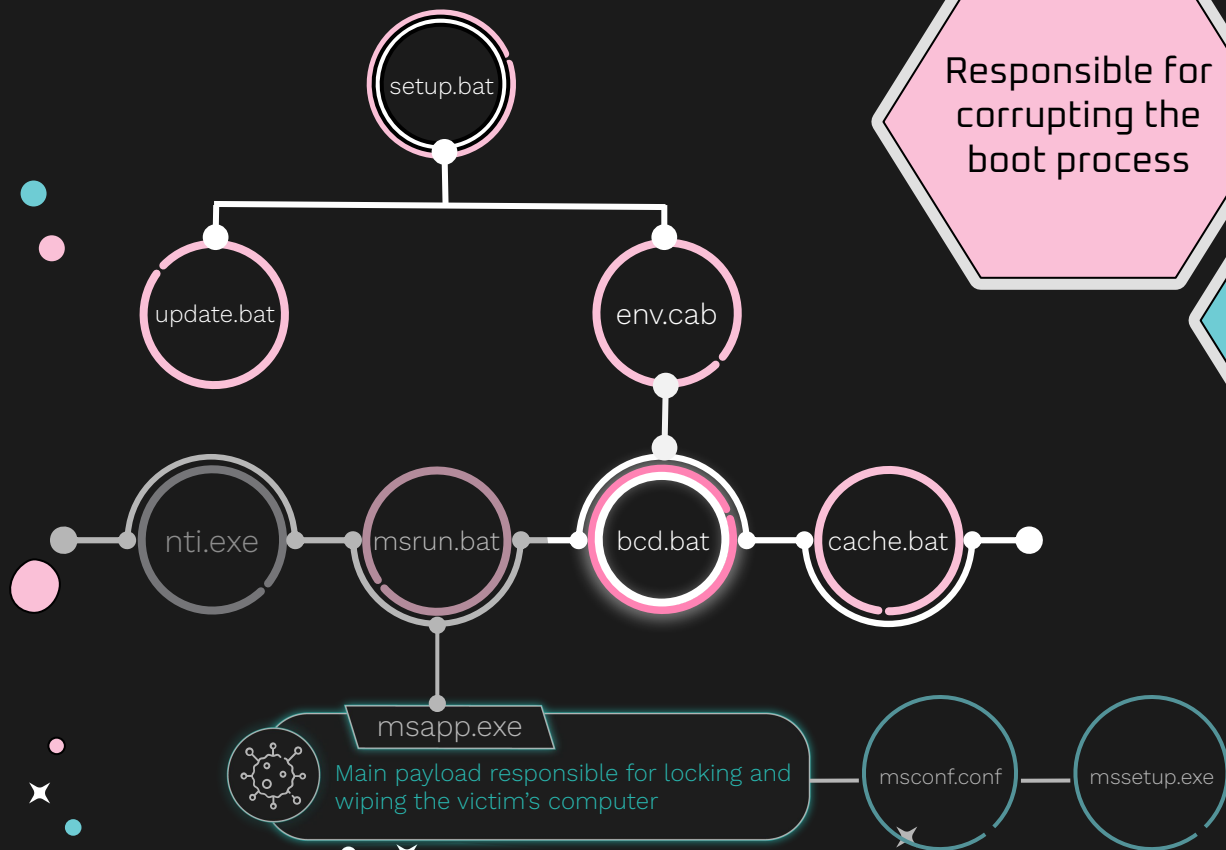


Disconnects the machine from all networks

Using Powershell:

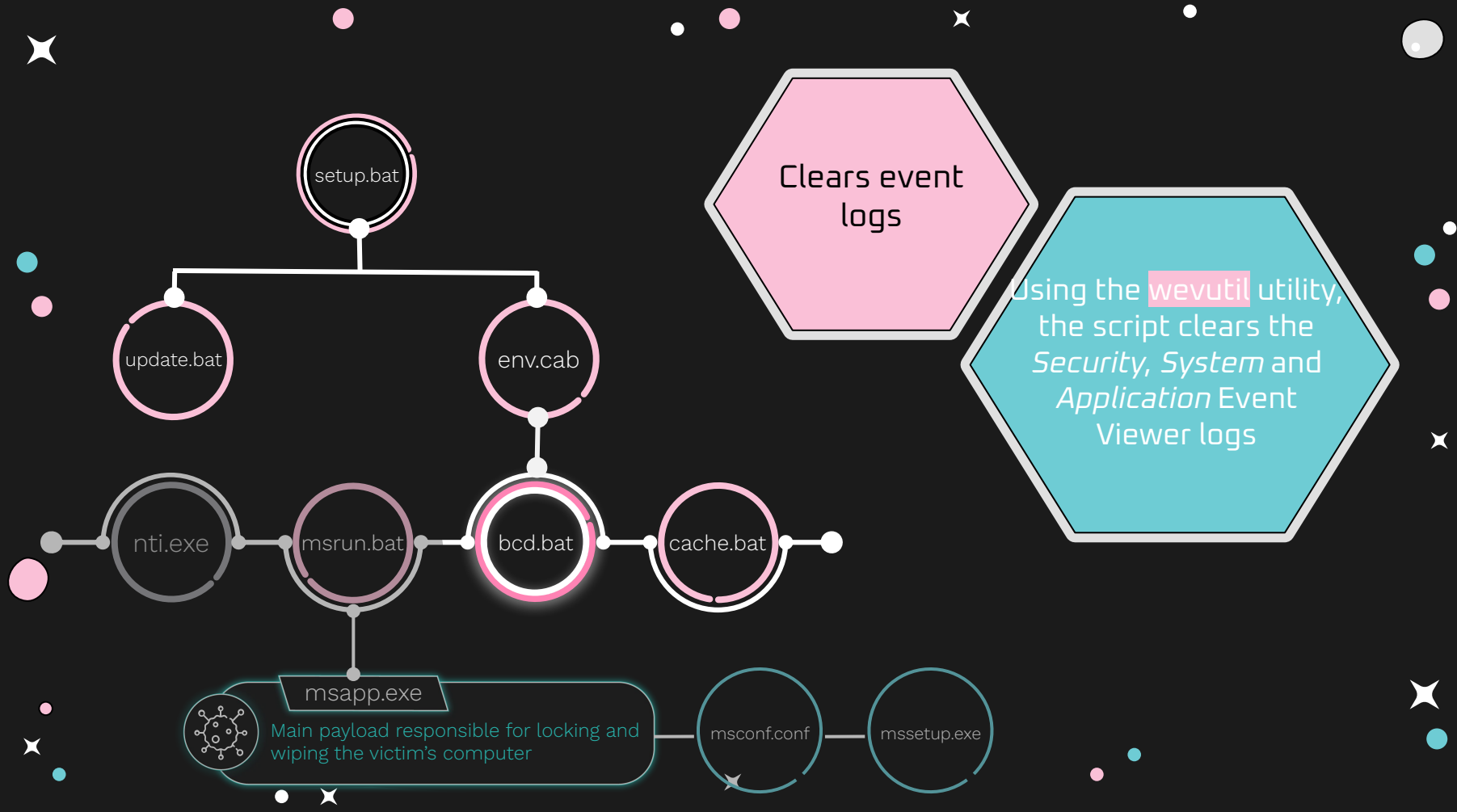
```
Get-WmiObject -class Win32_NetworkAdapter |  
ForEach { If ($_.NetEnabled) {  
    $_.Disable() } }
```

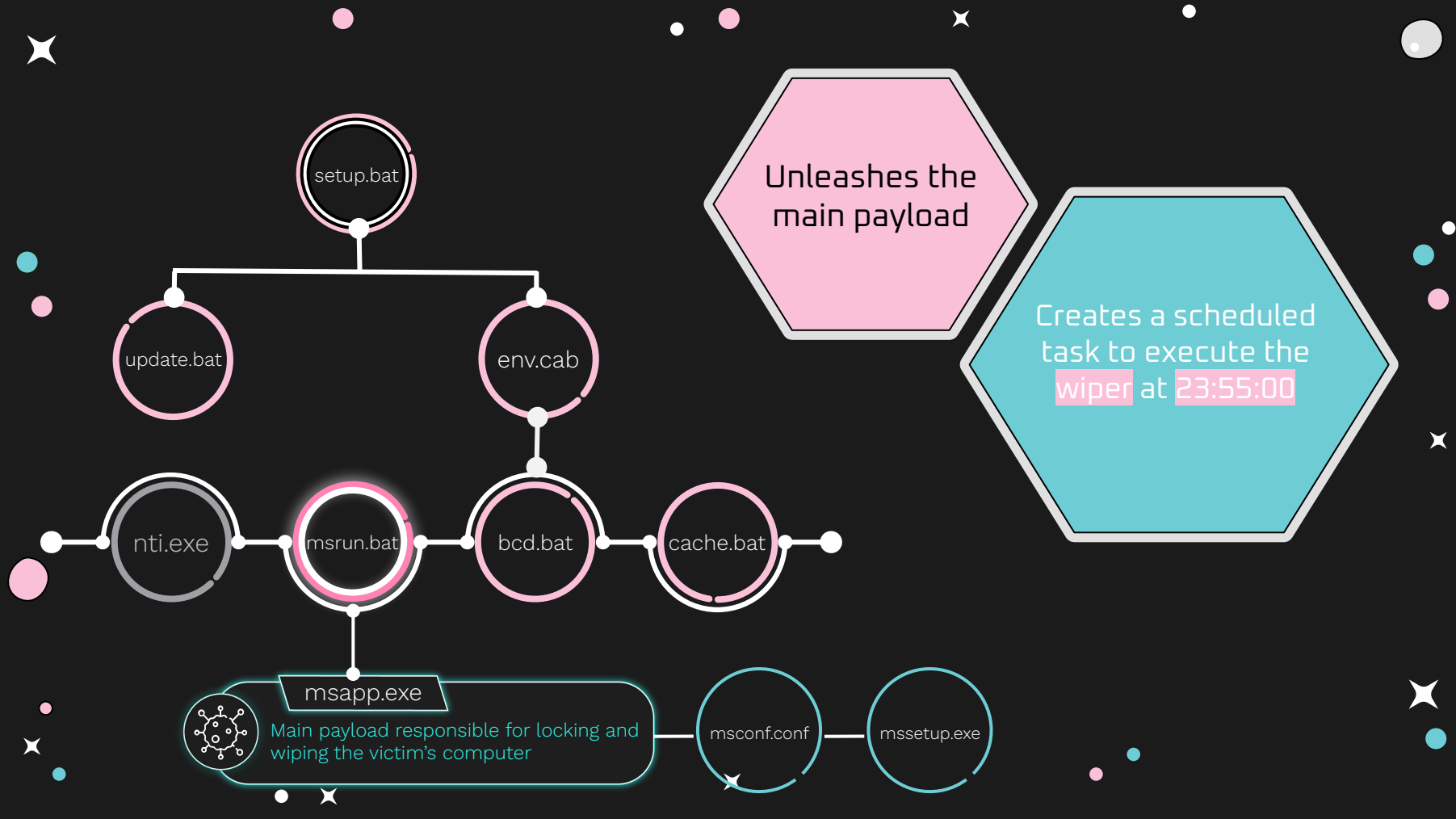


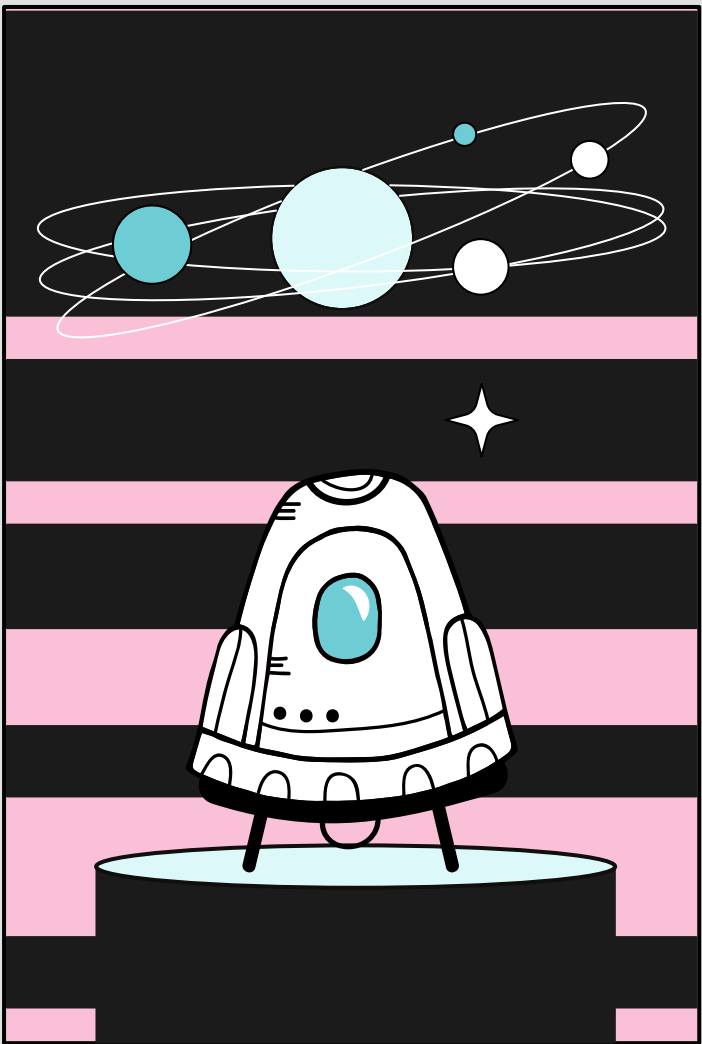


Responsible for
corrupting the
boot process

Overrides the `boot.ini`
file with new content and
deletes the different boot
identifiers using Windows
built-in `BCDEdit` tool







The Wiper: Meteor

Meteor **requires** a configuration to run

```
{  
  "log_file_path": "C:\\temp\\log",  
  "wiping_stage_logger_interval": 1000,  
  "is_alive_loop_interval": 5,  
  "locker_exe_path": "C:\\temp\\mssetup.exe",  
  "log_encryption_key": "abcdz",  
  "processes_to_kill": [],  
  "Locker_background_image_bmp_path": "C:\\temp\\mscap.bmp",  
  "process_termination_timeout": 15000,  
  "Locker_background_image_jpg_path": "C:\\temp\\mscap.jpg",  
  "paths_to_wipe": ["B:\\", "C:\\", "D:\\", ...]  
}
```



Meteor's Configuration

- `msconf.conf` is an encrypted configuration file
- Meteor supports more than `20` configuration fields, yet **only 10 are used**
 - This might suggest that the tool was not created specifically for this attack
- Allows flexibility during the execution of the wiper

Meteor's Functionality

- Writes "**Meteor** has started." to an encrypted log file
- Removes the machine from from the Active Directory domain
- Corrupts the computer's boot configuration
- Changes the password of the local users and logs off all the users
- Executes a "locker" program
- Wipes the system

Long delays due to cyber attack

More information: 64411



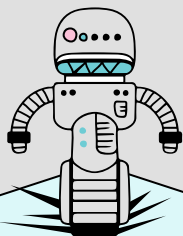
تاخیر زیاد بدلیل حملات سایبری

اطلاعات بیشتر: ۶۴۴۱۱



"Long delays due to cyber attacks.
More information: 64411"

Connecting the files to the attacks



01 Execution Flow As Seen In Padvish's Report

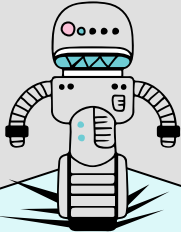
Similarities:

- Similar execution flow
- Similar files structure, same names and same functionality.

Differences:

- `nti.exe` was not used by `update.bat` — an MBR infector based on the one used by NotPetya.

Connecting the files to the attacks



01 Execution Flow As Seen In Padvish's Report

02 Configuration

Meteor's configuration is almost identical to the screenshot shared by Padvish

```
{
  "log_file_path": "C:\\temp\\log",
  "wiping_stage_logger_interval": 1000,
  "is_alive_loop_interval": 5,
  "locker_exe_path": "C:\\temp\\mssetup.exe",
  "log_encryption_key": "abcdz",
  "processes_to_kill": [],
  "locker_background_image_bmp_path": "C:\\temp\\mscap.bmp",
  "process_termination_timeout": 15000,
  "locker_background_image_jpg_path": "C:\\temp\\mscap.jpg",
  "paths_to_wipe": [
    "D:\\DISK4",
    "E:\\Veeam-backup",
    "E:\\Backups",
    "F:\\Backups",
    "C:\\Backup",
    "F:\\$RECYCLE.BIN",
    "c:\\ProgramData\\Veeam\\Backup",
    "C:\\Users\\All Users\\Veeam\\Backup",
    "B:\\",

```

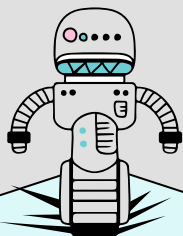
Config from Padvish's report

```
{
  "log_file_path": "C:\\temp\\log",
  "wiping_stage_logger_interval": 1000,
  "is_alive_loop_interval": 5,
  "locker_exe_path": "C:\\temp\\mssetup.exe",
  "log_encryption_key": "abcdz",
  "processes_to_kill": [],
  "locker_background_image_bmp_path": "C:\\temp\\mscap.bmp",
  "process_termination_timeout": 15000,
  "locker_background_image_jpg_path": "C:\\temp\\mscap.jpg",
  "paths_to_wipe": [
    "B:\\",
    "D:\\",
    "E:\\",
    "F:\\",
    "G:\\",
    "H:\\",
    "I:\\",
    "J:\\",
    "K:\\",

```

Config from Meteor

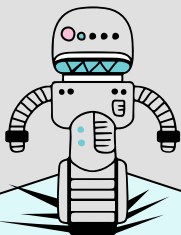
Connecting the files to the attacks



- | | |
|----|--|
| 01 | Execution Flow As Seen In Padvish's Report |
| 02 | Configuration |
| 03 | Similar message by the attacker |



Connecting the files to the attacks



01 Execution Flow As Seen In Padvish's Report

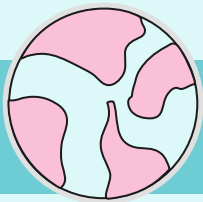
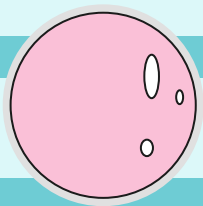
02 Configuration

03 Similar message by the attacker

04 Artifacts from Iran Railways' internal network

- Computer names and internal Active Directory object names
- Network shares

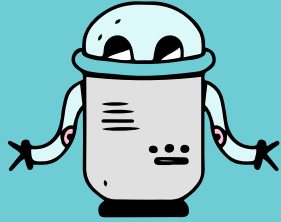
```
@echo off
SET dirPath=c:\Documents and Settings\All Users\Application
Data\Microsoft\Sounds
SET cabRemotePath="//railways.ir\sysvol\railways.ir\scripts\env.cab"
SET cabLocalPath="%dirPath%\env.cab"
```



Hunting for more files

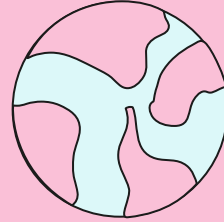
Found 3 separated incidents
possibly against targets in Syria

Comet and Stardust



Comet

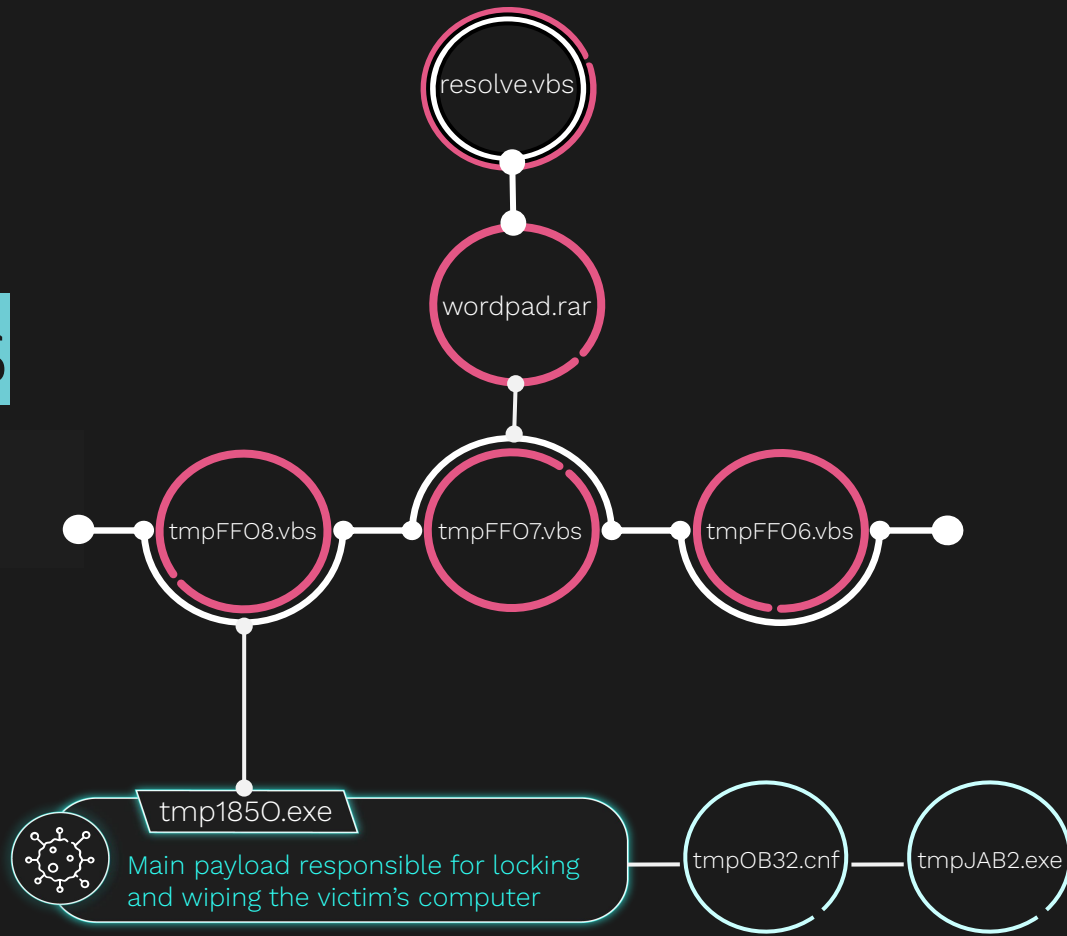
Uploaded to Virus Total on
January 2020.



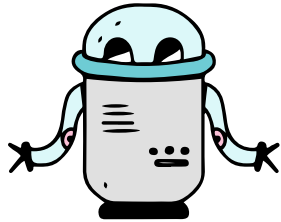
Stardust

Uploaded to Virus Total on
February and April 2020.

Stardust's Execution Flow

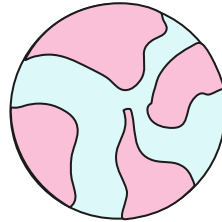


COMPARING VARIANTS



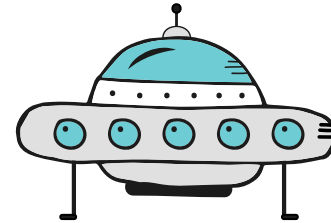
COMET

The first variant known to us. Was used against at least one target in Syria.



STARDUST

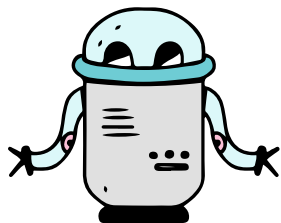
Comet's successor. Was used against at least two targets in Syria.



METEOR

The latest variant that was used against the Iranian targets.

COMPARING VARIANTS

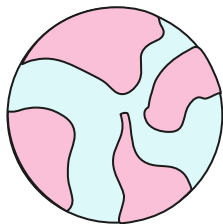


COMET

The first variant known to us. Was used against at least one target in Syria.

- References all the strings and features within it
- Kill Switch based on values from the config file
- Creates a user as an Administrator
- Files wiping based on priority specified in the config
- Adds itself to the auto logon
- No functionality of corrupting boot configuration

COMPARING VARIANTS

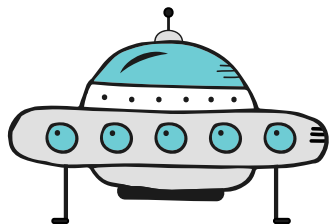


STARDUST

Comet's successor. Was used against at least two targets in Syria.

- Uses **Lock My PC 4** with a random password
- Sends a Base64-encoded log file to a remote server
- Introducing the deletion of BCD entries
- Kill Switch is dropped

COMPARING VARIANTS



METEOR

The latest variant that was used against the Iranian targets.

- Overrides the `boot.ini` file
- Does not use Lock My PC 4
- Does not utilize some configuration parameters
`process_to_kill`, `paths_to_wipe`, `log_server_ip`, and
`log_server_port`
- Disables screen saver

Stardust's Configurations

```
"paths_to_wipe": [ [...]  
    "c:\\\\Users\\\\administrator.KATERJIGROUP\\\\Desktop",  
    "c:\\\\Users\\\\administrator.KATERJIGROUP\\\\Documents", [...] ]
```

```
"paths_to_wipe": [ [...]  
    "c:\\\\Users\\\\administrator.ARFADA\\\\Desktop",  
    "c:\\\\Users\\\\administrator.ARFADA\\\\Documents", [...] ]
```

```
"locker_background_image_path": "C:\\Windows\\Temp\\logo.jpg"
```



I AM INDRA

INDRA
GOD OF WAR

Katerji Oil trades
with Quds Force
and your souls

رَضْنَةُ أَنْظَمَةٍ
شُرَكَائِكُمْ فِي الْمَاضِي وَالْآنَ فِي
الْحَاضِرِ وَحَذَرْتُكُمْ دَعَمَ إِرْهَابِ
حَرْبِ اللَّهِ وَفَيْلَقِ الْقُدْسِ حِينَ
ضَرَبْتُ سَفِينَكُمْ فِي الْبَحْرِ

مَا أَنْدَرَا بِغَافِلَةٍ عَمَّا تَعْمَلُونَ فَتَرْقُبُوا ضَرْبَاتِي الْقَادِمَةَ





Indra @Indra17857623 · Feb 18, 2020

2/5

...#ARFADA launders and transfers funds for #Hezbollah using affiliated traders and businessmen like #Tawfiq and #Alfadelex, who we've also recently hacked. These tainted funds are passed in cash to eventually reach the treacherous terrorist #Muhammad_Jaffer_Alqasir...



1



Indra @Indra17857623 · Feb 18, 2020

3/5

...We, #Indra God of War, have hacked the #Katerji Group's #ARFADA Petroleum company's systems and computers because of their business with #Quds_Forces and their support of #Hezbollah's terrors, and now all of their documents and information are under our control...



1



Indra @Indra17857623 · Feb 18, 2020

4/5

...We have been following them and watching for quite a while, but now is about time for #Katerji to understand, without a hint of doubt, that for their own good – it's time to put a stop to their actions or there will be dire consequences!...



1



Yesterday [#INDR](#)
demolishing their
company cripplec
data has been [#h](#)
response to Alfac
[#QF](#). Evidence wi



4:09 PM · Sep 14, 2019 · T

1 Retweet



Indra @Indra17857623 · Mar 8, 2020

[بنشر الفساد و](#)



Indra

@Indra17857623



شعبية
في هذا الفيديو
ميني ثم

اتي وما من

0:02 3.9K views



Indra @Indra17857623 · Mar 18, 2020



ults made in [#Iran](#)
these [#terrorists](#)!

[#حزب_الله_الارهابي](#) بقيادة [#حسن_نصرالله](#) [#سارق_لبنان](#)
[#يدمر_#الليرة_اللبنانية](#) ليقبض [#الدولار_الامريكي](#) المهرب على
حساب خراب [#لبنان](#) والمهم ان [#سلاح_المقاومة](#) يُشترى
من [#سوريا](#) مقابل تهريب [#الطحين_اللبناني](#).

Translate Tweet



5:37 PM · Jun 17, 2020 · Twitter Web App



3



1



← **Indra**
58 Tweets




Indra
@Indra17857623

Aiming to bring a stop to the horrors of QF and its murderous proxies in the region!
Facebook page:
facebook.com/Indra-Godofwar
t.me/INDRA_GODOFWAR Joined June 2019

58 Following 105 Followers




Indra Godofwar
@indragodofwar · News Personality


Contact Us

twitter.com


Indra Indra

HOME VIDEOS PLAYLISTS CHANNELS DISCUSSION ABOUT

Uploads



5 minutes describes the life of Qasem Soleimani 5 دقائق تشرح عن حياة قاسم سليماني و القليل من أفعاله
26 views · 1 year ago
... قاسم سليماني كاتبون شعوب الشرق الأوسط 5 دقائق سليماني يشرح القليل من جرائمه الإيرانية والمغربي اعطوا ريكام



INDRA GodOfWar
31 subscribers

Aiming to bring a stop to the horrors of QF and its murderous proxies

Facebook:
<https://www.facebook.com/indragodofwar...>

VIEW IN TELEGRAM

Preview channel

INDRA PROFILE



MOTIVATION

"Aiming to bring a stop to the horrors of Quds Force and its murderous proxies in the region!"

LANGUAGES

- Arabic
- English
- Persian

MODUS OPERANDI

- Site defacement
- Leak the data from victims' machines
- Demolish the networks with wiper

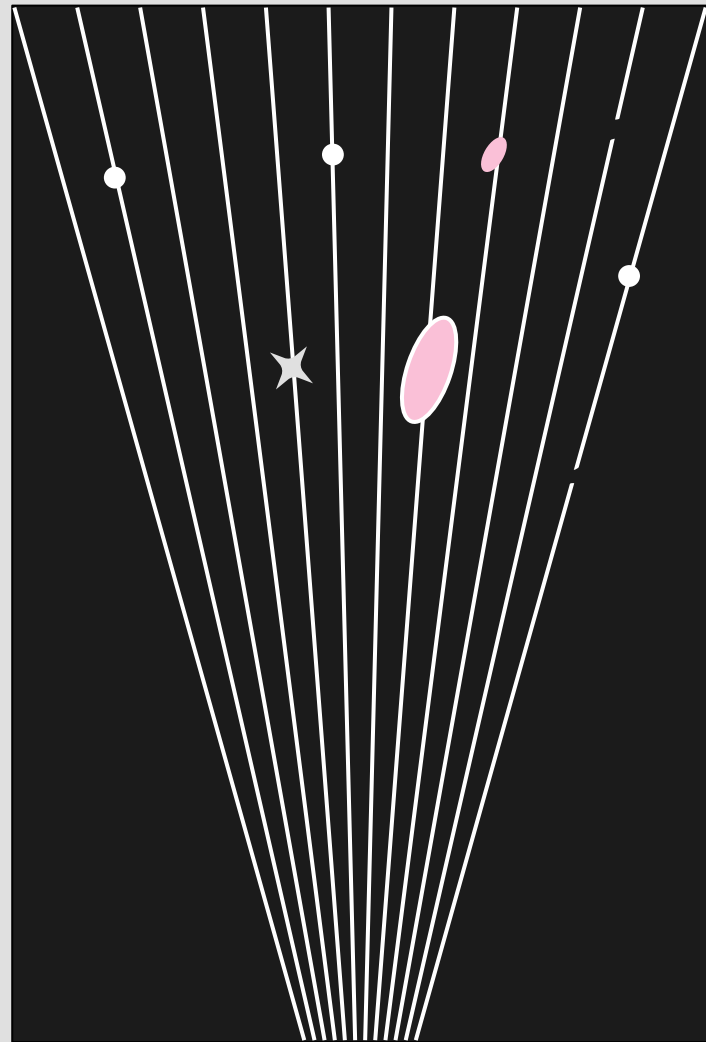
MAIN ADVERSARIES

Quds Force - Iranian (IRGC) military intelligence unit.

Hezbollah - militant group (Lebanon, Syria).



Previous Attacks





Indra's

Previous Attacks

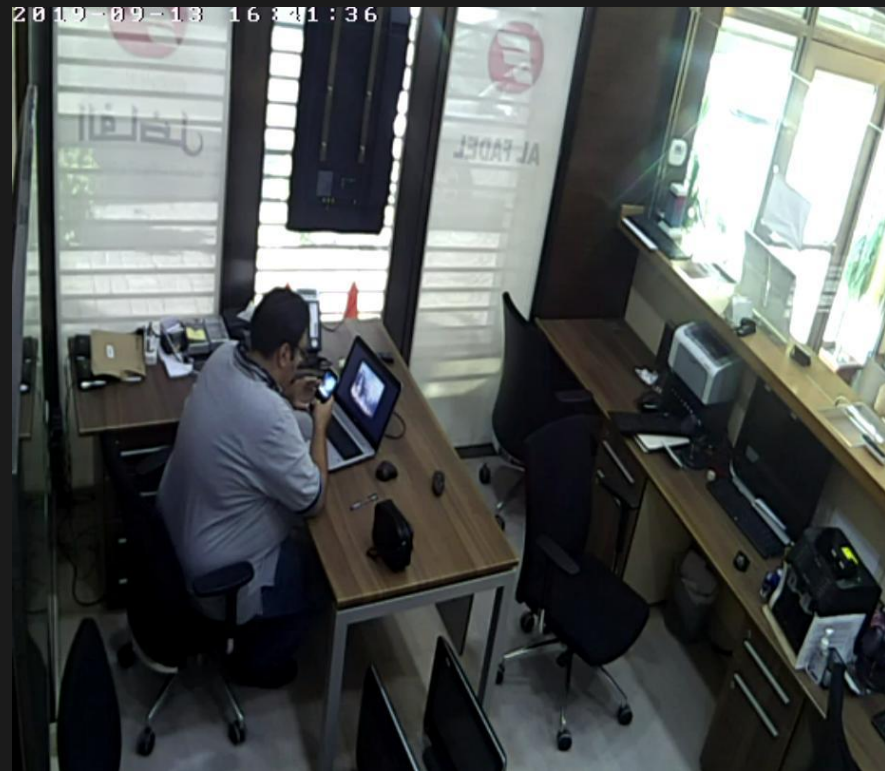
Alfadelex

Money exchange
and transfer

September 2019

Comet







Indra's

Previous Attacks

Alfadelex

Money exchange
and transfer

September 2019

Comet

Cham Wings

Private airline
company

January 2020

?





Indra's

Previous Attacks

Alfadelex

Money exchange
and transfer
September 2019

Comet

Cham Wings

Private airline
company
January 2020

?

Arfada

Oil trading
Company
February 2020

Stardust

Katerji Group

Multi-industry
trading company
April 2020

Stardust





Indra's

Previous Attacks

Alfadelex

Money exchange
and transfer

September 2019

Comet

Cham Wings

Private airline
company

January 2020

?

Arfada

Oil trading
company

February 2020

Stardust

Katerji Group

Multi-industry
trading company

April 2020

Stardust

Baniyas

Oil Refinery

November 2020

?



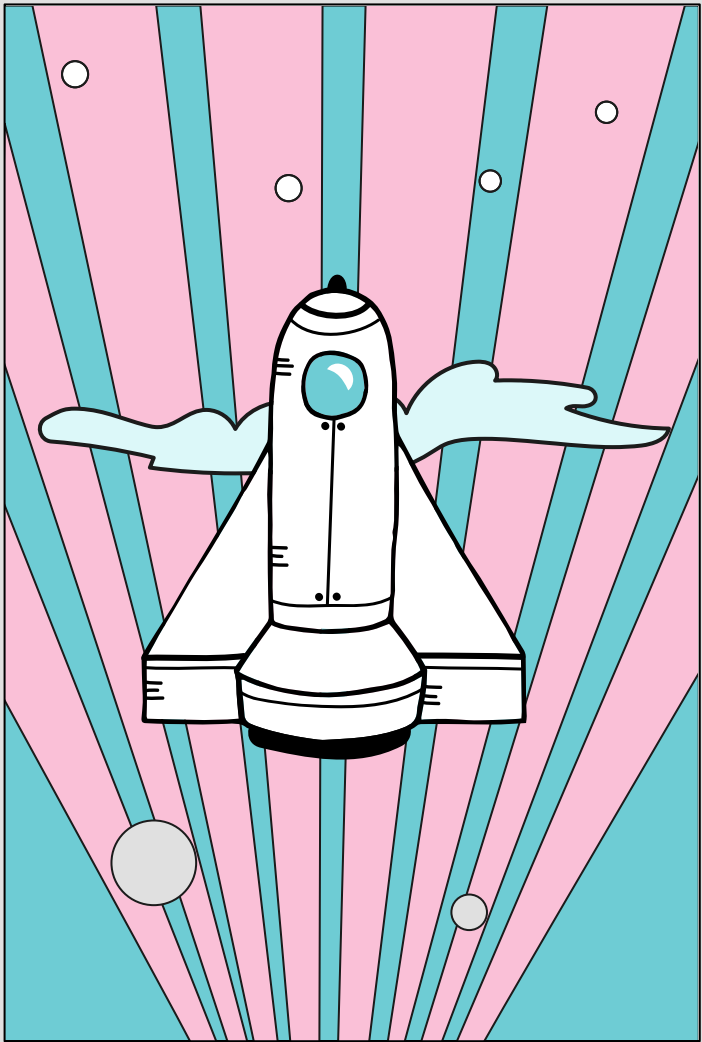


[HOME](#) / [HACKTIVIST ATTACK ON COMPANIES RELATED TO IRAN](#)

[Attack](#) [News](#) [Teams](#)

Hacktivist attack on companies related to Iran

🕒 2 years ago



Connecting Indra to the
attacks on the Iranian
targets

Connecting Indra to Iranian attacks

01 Targeting

Iran-related targets:

- 2019 - 2020: companies having ties with Iran
- 2021: Iran Railways and Iran's Ministry of Roads and Urban Development

Connecting Indra to Iranian attacks

01 Targeting

02 Execution flow

Multi-layered execution flow based on script files and archive files:

- Bath scripts used in attacks against Iran.
- VBS scripts used in attacks against Syrian companies.
- Different file types, almost the same functionality.

Connecting Indra to Iranian attacks

- 01 Targeting
- 02 Execution flow
- 03 Payloads

Comet, Stardust and Meteor represent the evolution of the same wiper.

Comet and Stardust contain "INDRA" string:

```
[0x004021c5]
27: fcn.init_INDRA ();
0x004021c5      push    str.INDRA ; "INDRA"
0x004021ca      mov     ecx, loc.INDRA
0x004021cf      call   copy_string
0x004021d4      push    fcn.47a5a2
0x004021d9      call   atexit
0x004021de      pop     ecx
0x004021df      ret
```

Connecting Indra to Iranian attacks

01 Targeting

02 Execution flow

03 Payloads

04 Target networks reconnaissance

Attacks against Syrian targets:

- access to web cameras
- few months of recon
- multiple exfiltrated documents

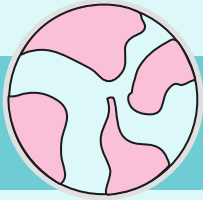
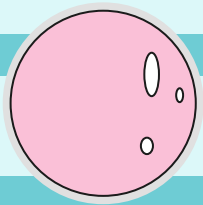
Iranian attacks:

- prior access to AD
- victims machines filtering by name

Connecting Indra to Iranian attacks

- | | |
|----|--------------------------------|
| 01 | Targeting |
| 02 | Execution flow |
| 03 | Payloads |
| 04 | Target networks reconnaissance |
| 05 | Attacks announcements |





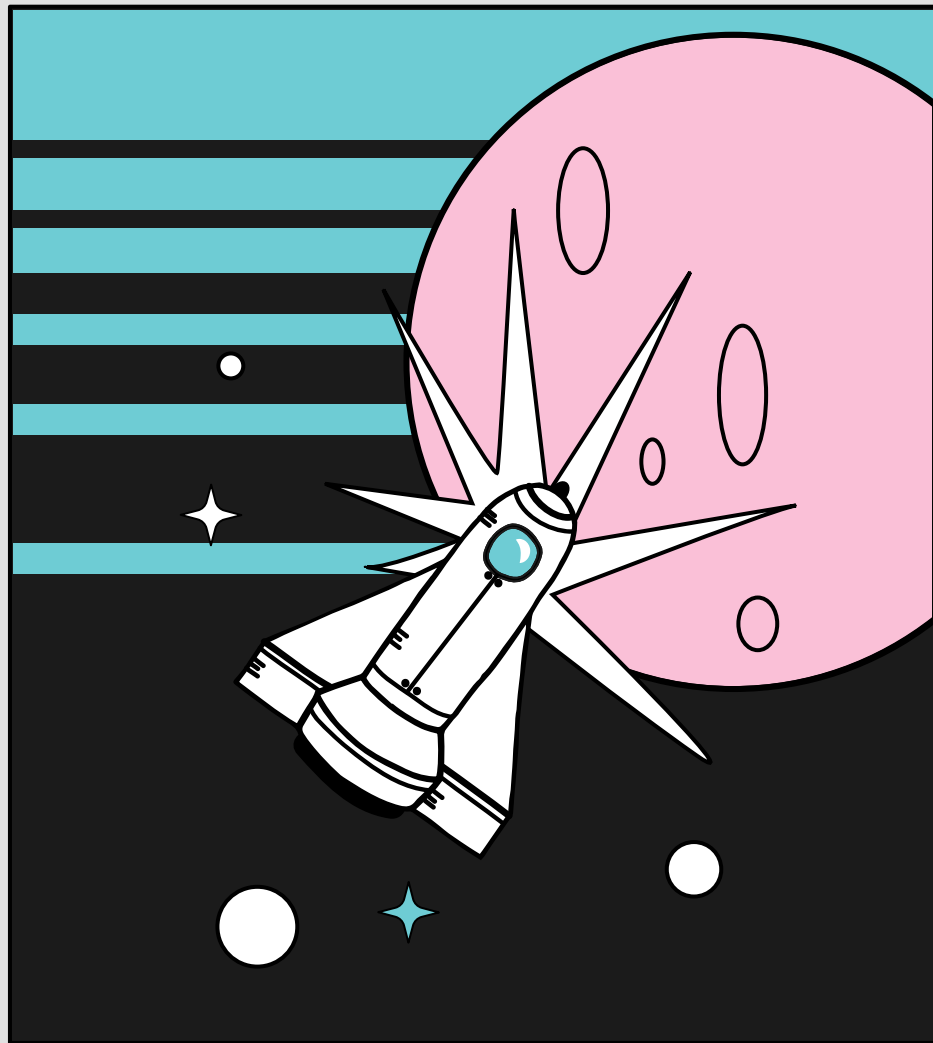
Differences

Indra did not take responsibility
for the attacks in Iran



**LET'S
TALK
ABOUT**

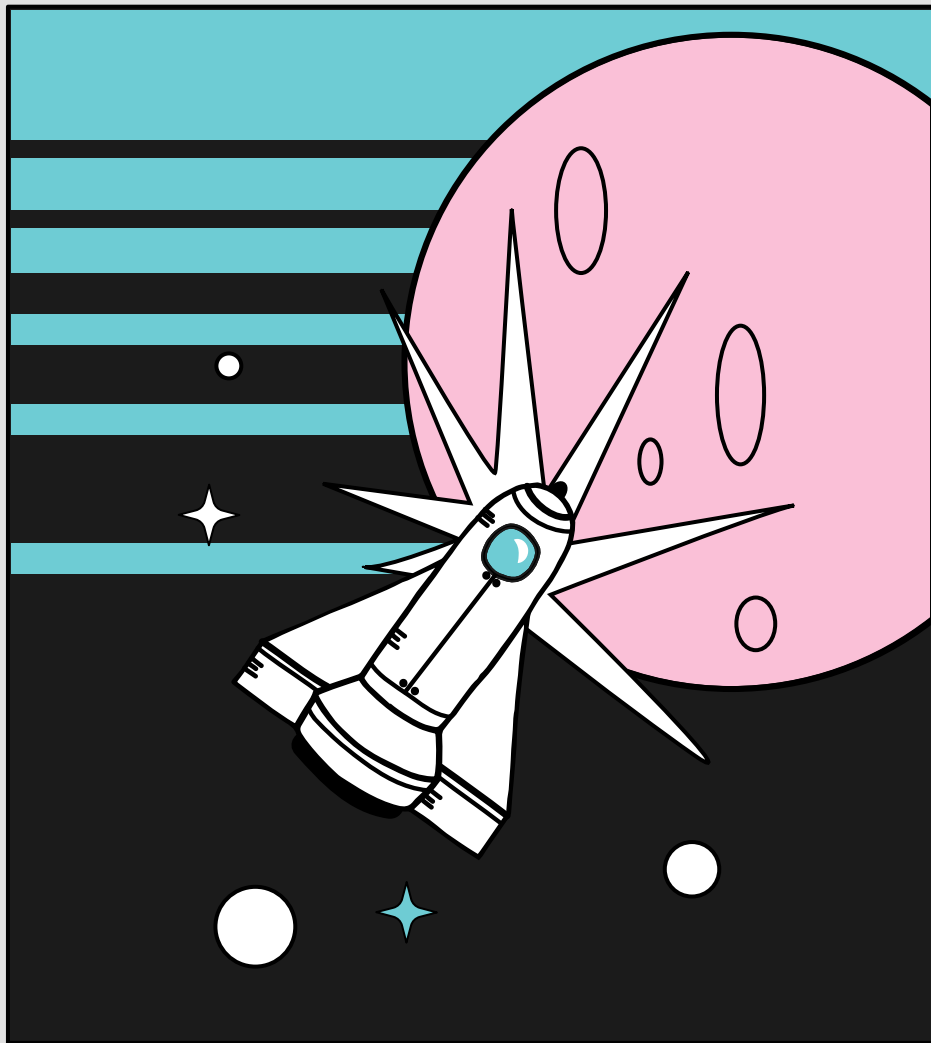
ATTRIBUTION





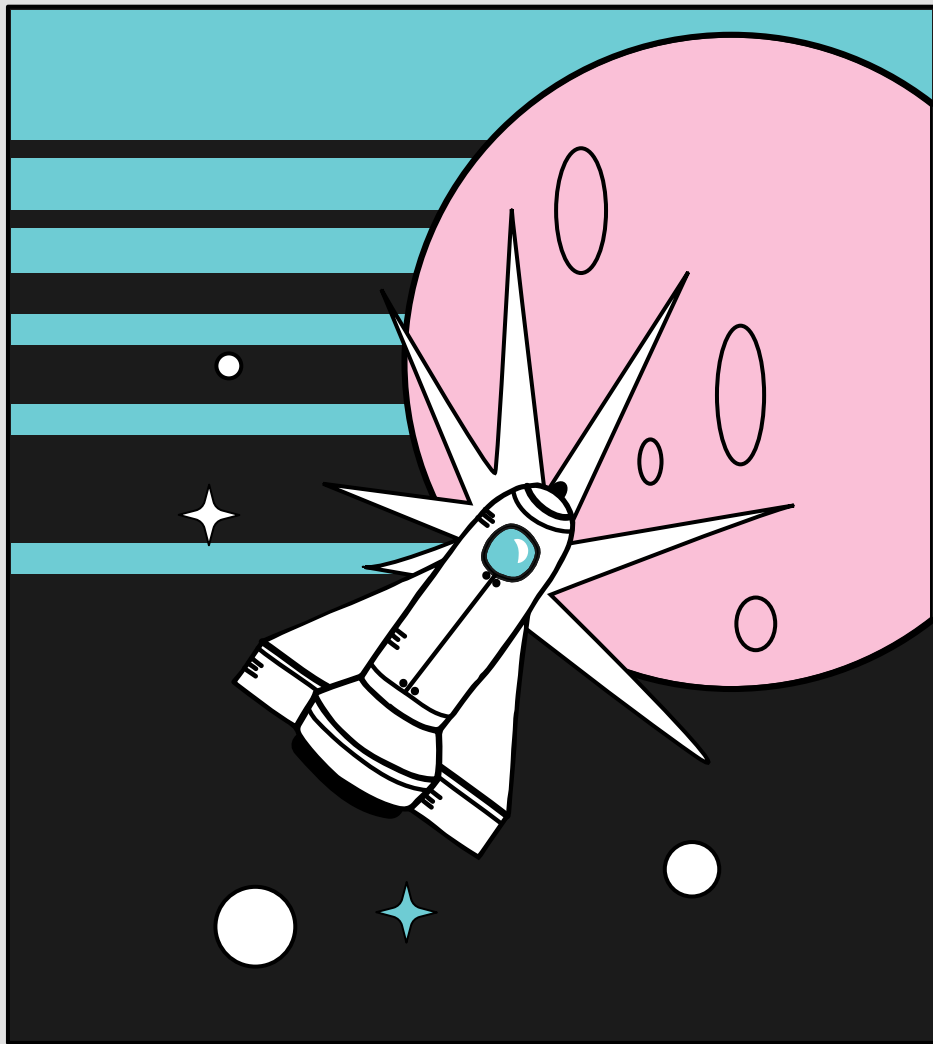
**LET'S
TALK
ABOUT**

ATTRIBUTION



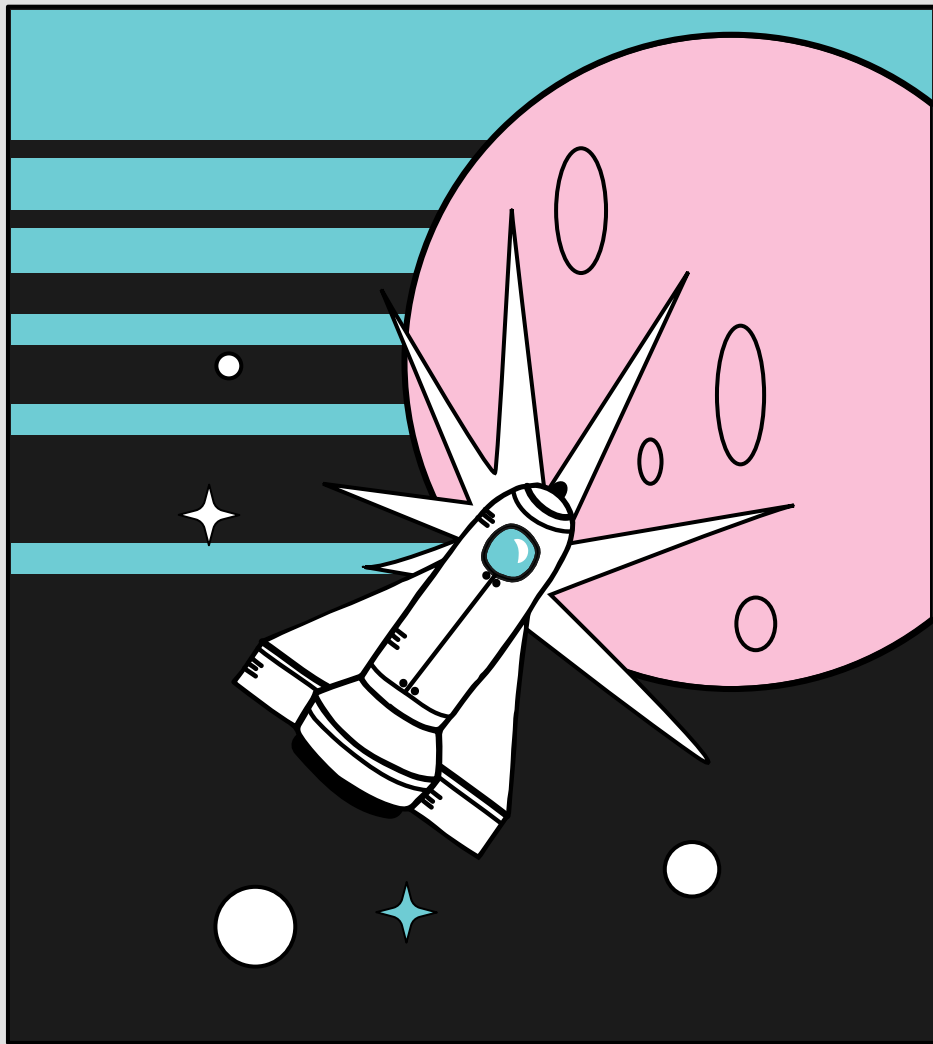


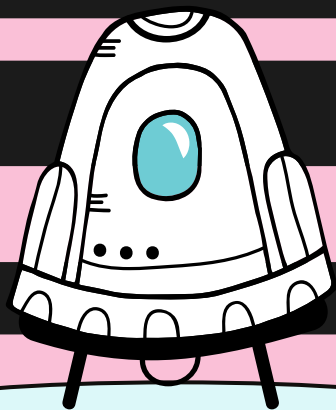
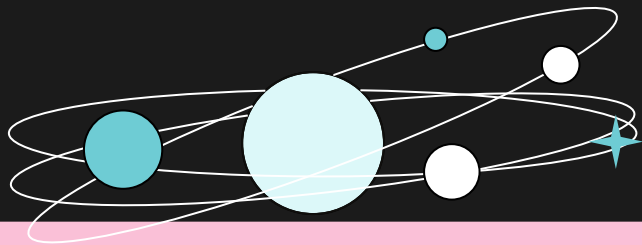
**WE
DON'T
KNOW**





**WE
DON'T
KNOW**





Thank you! ✨

 @megabeets_

Itay Cohen

 @_lostpacket_

Alexandra Gofman



64411

cp< r >

CHECK POINT RESEARCH

CREDITS: This presentation template was created by Slidesgo,
including icons by Flaticon, and infographics & images by Freepik