



Cyber threats and attacks in the oil and gas industry

Eyal Sela - Head of Threat Intelligence

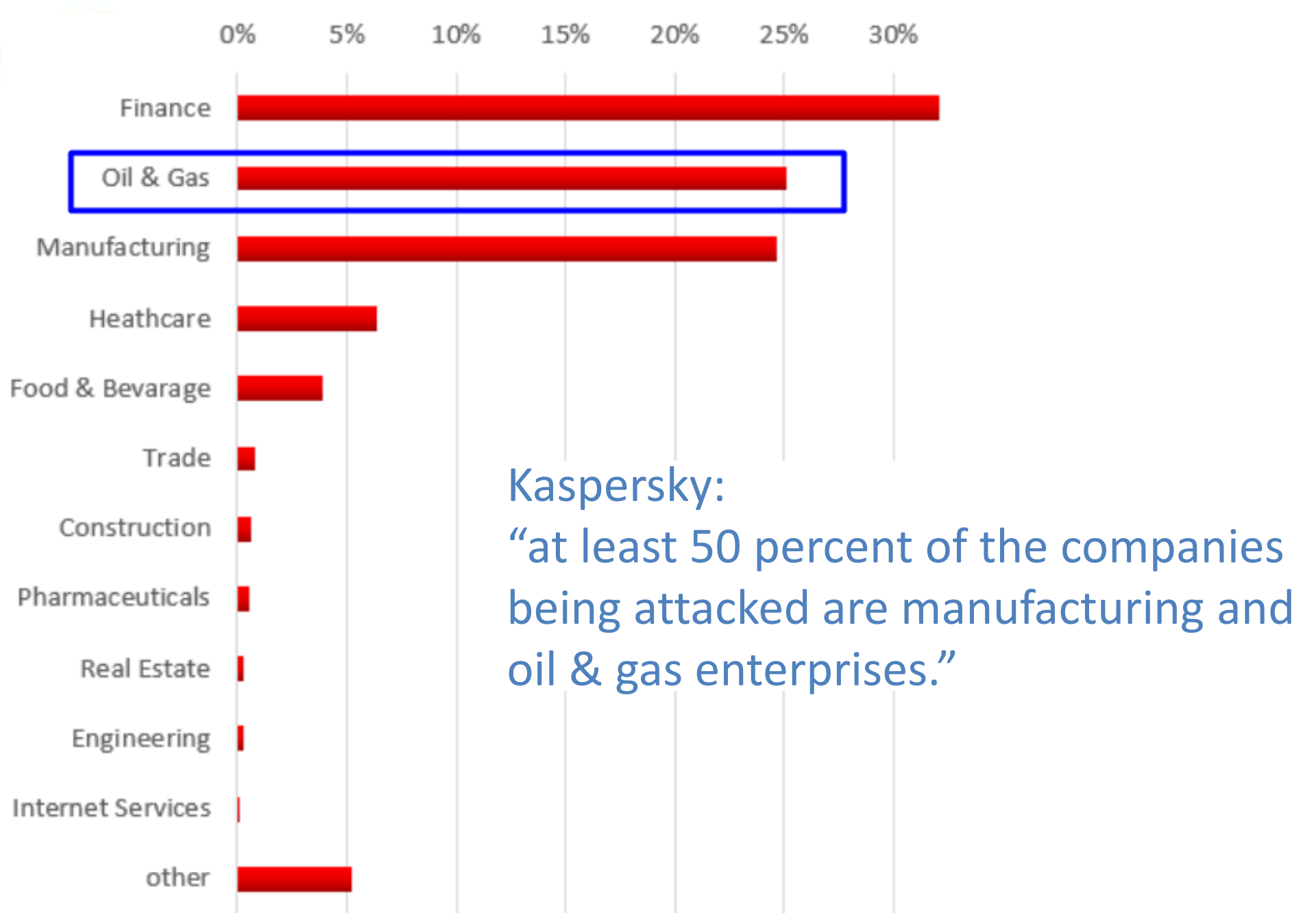
Content

3 types of cyber attacks
against Oil and Gas or
Energy organization.

Notpetya

Non targeted, disruption

- Wiper worm masquerading as ransomware
- MEDoc, Ukrainian tax accounting software, update function was used to infect the victim's computers.
- operational ICS networks are facing traditional business threats.
- Maersklost \$300 million USD rebuild and replace most of its IT and operations network.



Kaspersky:
“at least 50 percent of the companies being attacked are manufacturing and oil & gas enterprises.”

Source: <https://ics-cert.kaspersky.com/alerts/2017/06/29/more-than-50-percent-of-organizations-attacked-by-expetr-petya-cryptolocker-are-industrial-companies/>

Triton

disruption/distraction

- First malware to target **industrial safety systems**
- Petrochemical facility in Saudi Arabia
- Tamper or Disable Triconex products
- Run unauthorized programs by leveraging a previously unknown bug



Illustration: Triconex by Schneider Electric

<https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html>


Operation Electric Powder

Low sophistication espionage

- Targeting Israel Electric Company
- Facebook profiles, breached websites, self-hosted and cloud based websites.
- Low operational technological sophistication
- Likely for tactical, strategic, or business espionage



Linda Santos

 Add Friend

 Follow

 Message



Timeline

About

Friends

Photos

More ▾

DO YOU KNOW LINDA?

To see what she shares with friends, send her a friend request.


 Add Friend

 Intro

 Works at Mobile Programming LLC

 Lives in Tel Aviv, Israel

 From Jerusalem, Israel

 Followed by 4 people



Linda Santos shared Ivgeni Zarubinski's post.

June 16 · 





חברת החשמל לישראל Israel Electric Corporation

50 mins · 🌐

גם באזור טבריה נמשכת ההיערכות לחורף: כשברקע נוף קסום לכנרת, היום בוצעו עבודות תשתית בקו מתח גבוה בעיר. העבודה בוצעה במתח חי מבלי להפסיק את אספקת החשמל ללקוחות האזור. את העבודה העבודה בוצעה בשיתוף פעולה בין קבוצות הרשת של מחוז הצפון, השגחת אזור טבריה, מחלקת קשר ואלקטרוניקה צפון ובסיוע של מחלקות התחבורה וציוד מכני נייד (צמ"ן).

Atara Tal Oma Vagman הרצל פרידמן מחזקים את עובדי חברת חשמל שבשטחעיריית טבריה הדף הרשמיTiberias, Israel



👍 Like 💬 Comment

Moti Baikin, Sufyan Adeas, Hosam Gbareen and 11 others like this.

Top Comments -

1 share



Linda Santos ynetnewes.com/video/Newfilm.html

16 mins

Friends

All Friends Recently Added Followers Following

Search Friends



[REDACTED]

Project Manager at חברת החשמל לישראל
Israel Electric Corporation

[Add Friend](#)



[REDACTED]

Works at Israel Electric Corporation

[Add Friend](#)



[REDACTED]

[Add Friend](#)



[REDACTED]

Works at Israel Electric Corporation

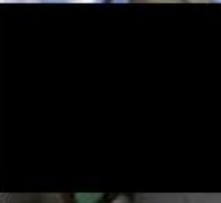
[Add Friend](#)



[REDACTED]

Works at חברת החשמל לישראל
Israel Electric Corporation

[Add Friend](#)



[REDACTED]

[Add Friend](#)



Pokemon-Go

July 14 · 🌐

Pokemon Go Games, play with your friends and catch the pokemons.

לשחק עם החברים שלך ולתפוס את פוקימונים, Go משחקי פוקימון

עבור מחשבים ניידים ונייד

<http://pokemonisrael.yolasite.com>



Pokemon

POKEMONISRAEL.YOLASITE.COM

👍 Like

💬 Comment

➦ Share

👍 13



Pokemon Go

Its new game for collection Pokemons and Competition
With Your Friends Game for

Computers , Android

להורדה טלפון ומחשב



להורדה טלפון ומחשב

79081e664393cad10c1f93835fd29fa36071e216b6e43bdc8f9650ef3eeae671.rar

Open Add Files Extract

Back Location: /

Name	Size	Type	Modified
IEC.pdf	358.5 kB	PDF docum...	10 אוגוסט 2016 05:28
svchost.exe	295.4 kB	DOS/Windo...	06 ספטמבר 2016 10:55

Pokémon GO

Do you want to install this application? It does not require any special access.

Google Service

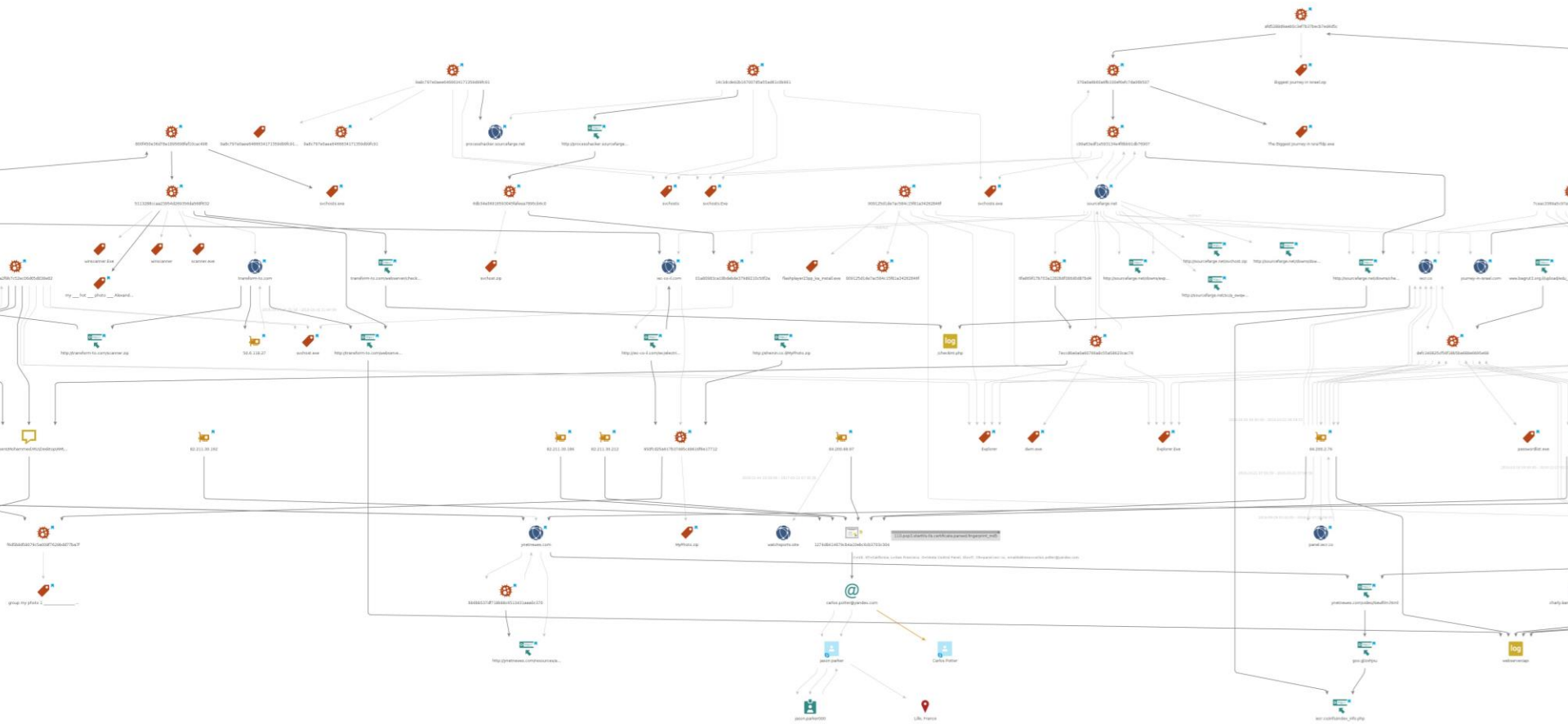
Do you want to install this application? It will get access to:

- read your contacts
- read your Web bookmarks and history
- modify or delete the contents of your SD card
- read the contents of your SD card
- find accounts on the device

DEVICE ACCESS

- connect and disconnect from Wi-Fi
- full network access
- view network connections

Cancel Next



Resources

- <https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf>
- <https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html>
- <https://www.clearskysec.com/iec/>