

CYBER SECURITY NEWS BULLETIN



August 2023

Content:

- Official meeting between the Ambassador of Israel and the National Authority for Electronic Certification and Cyber Security
- Google Workspace requires two administrator logins during critical changes.
- A new malware identified as WikiLoader is discovered
- Microsoft - patching alert



Official meeting between the Ambassador of Israel and the National Authority for Electronic Certification and Cyber Security

On August 15, the Ambassador of Israel, Ms. Galit Peleg, in the framework of friendship and cooperation between our countries, held an official meeting at the National Authority for Electronic Certification and Cyber Security, where she was received by the Director General, Mr. Igli Tafa and the staff of the Authority. In this meeting, the possibility of cooperation between the institutions of the two countries was discussed, including institutions in the field of cyber security.

Ms. Ambassador, expressed appreciation and consideration for a great development that Albania has taken in a short time in various sectors, including the field of Cyber Security.

The Director of the Authority, Mr. Tafa, expressed his thanks to the Ambassador for the support given and presented the challenges and the institutional strategy aimed at enabling an increase in the level of Cyber Security in the country.



A new malware identified as WikiLoader is discovered

Proofpoint researchers have identified a new malware called WikiLoader that has been detected in at least eight campaigns targeting Italian organizations since December 2022.

These campaigns used emails containing Microsoft Excel attachments, Microsoft OneNote attachments, or PDF attachments, causing the Ursnif Trojan to be downloaded as an additional payload.

[Read more](#)



Google Workspace requires two administrator logins during critical changes.

Google recently announced new cybersecurity protection controls that will allow security teams to thwart social engineering attacks targeting Workspace users.

Google also explained how an Android malware could infect the Google Play Store with the help of a tactic known as versioning that allows malicious actors to bypass security checks.

[Read more](#)



Microsoft releases patches for 74 new vulnerabilities in August update.

Microsoft has patched a total of 74 vulnerabilities in its software as part of the company's August 2023 updates. This includes six critical, 67 important, and one moderate-severity vulnerability. Released along with the security improvements are two deep update reports (ADV230003) and (ADV230004).

Microsoft announced that installing the latest update "stops the chain of attack" that leads to the remote code execution bug.

[Read more](#)

CYBER SECURITY NEWS BULLETIN



Content:

- Cyber Security for Businesses.
- Security tips for businesses:

Cyber Security for Businesses.

"One of the biggest mistakes small businesses make is employers or employees not creating and managing passwords properly."

Scott Schober

Cyber security has become a necessity for businesses of all sizes as their systems and networks containing sensitive and valuable data are put under the clutches of malicious actors.

Without a cyber security strategy, your business cannot protect itself from threats leaving it vulnerable to malicious actors who will identify your business as an easy target. Along with the way technology has evolved over the years, there has also been a steady increase in risks to businesses.



Security tips for businesses:

1. Be sure to keep your passwords private



2. Protect all your devices with an antivirus program

3. Do not open attachments in suspicious emails. Be wary of Word, Excel, PowerPoint or PDF attachments.



4. Apply additional security to your login process by configuring multi-factor authentication (MFA).