Web Security Trends and Insights 2023-2024

Romy Liram
Director of Sales EMEA

Web Security Insights **2023**

1. Global Cybersecurity Shortage
2. Cybersecurity budgets have been reduced compared to earlier years, yet critical security concerns remain the top priority
3. Rapid vulnerability use and diverse threat actors challenge global organizations.
4. Increase of number and volume of Distributed Denial of Service (DDoS) attacks
5. Current AI tools used for attacks provide mainly higher volume of attacks (not sophistication)

Web Security Insights

2023

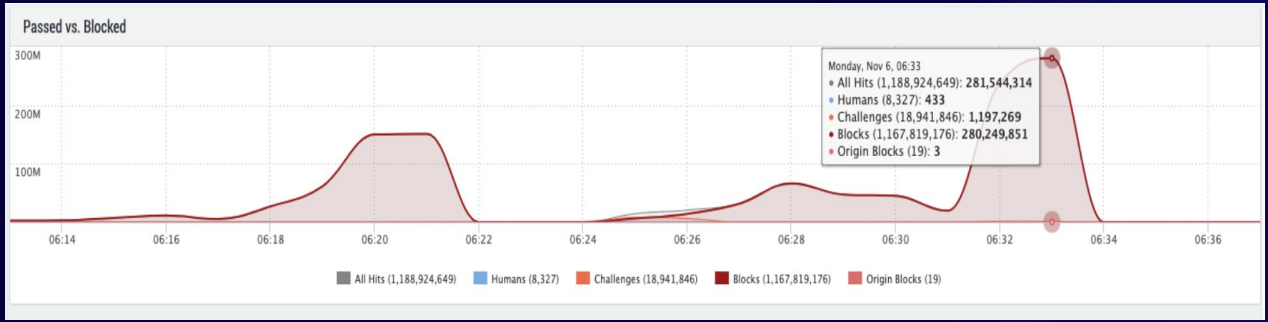
Global security shortage, combined with the financial situation led some companies to compromise their security.

DDoS Attacks are on the Rise

Although lacking in sophistication, duration and volume increase constantly

DDoS Attacks are on the Rise

Although lacking in sophistication, duration and volume increase constantly



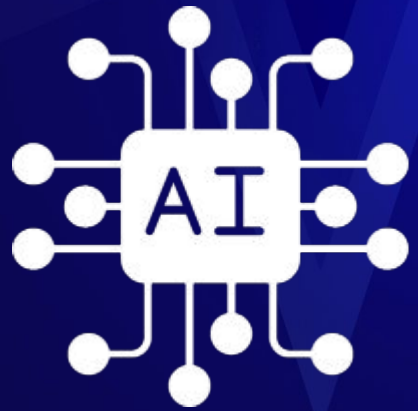
Top Countries

Country	Hits	Passed	Blocks
Indonesia	218,551,958	3	218,551,955
United States	93,726,347	116,578	87,931,292
Russia	59,322,149	24,283	58,563,860
Brazil	55,911,982	11,280	54,392,292
India	46,987,721	15,534	45,890,981
Colombia	46,469,012	3,990	45,995,822
Germany	39,511,544	17,874	39,353,714
China	38,109,297	10,383	36,940,998
Mexico	32,761,442	5,078	32,585,109
Thailand	32,091,153	2,441	31,030,086
France	31,977,888	1,944	31,968,565
Vietnam	30,268,622	10,910	28,512,998
Bangladesh	26,529,862	1	26,529,861
Ecuador	21,783,095	8,107	21,535,288
Singapore	21,763,141	5,038	20,503,282

AI in the Cyber Industry

2023

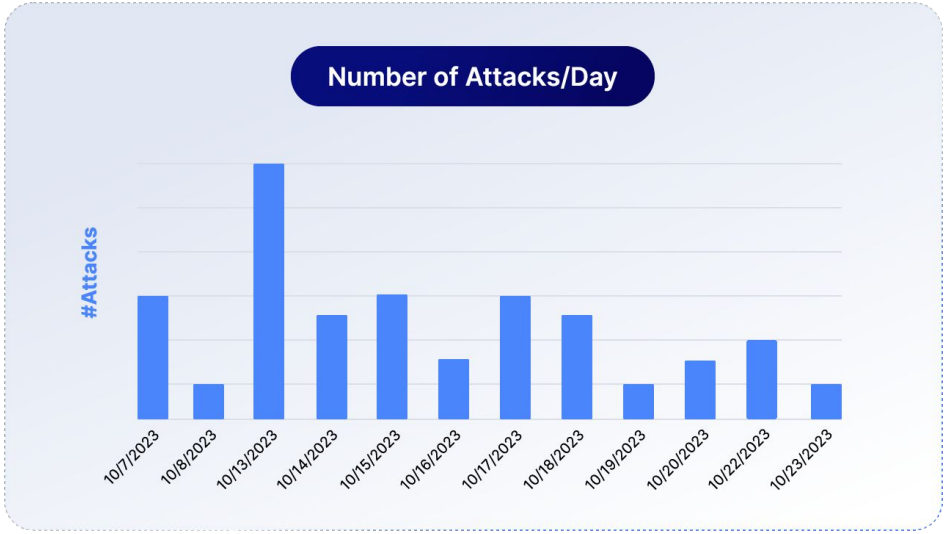
AI is not fully utilized for attacks, this will change in the foreseeable future

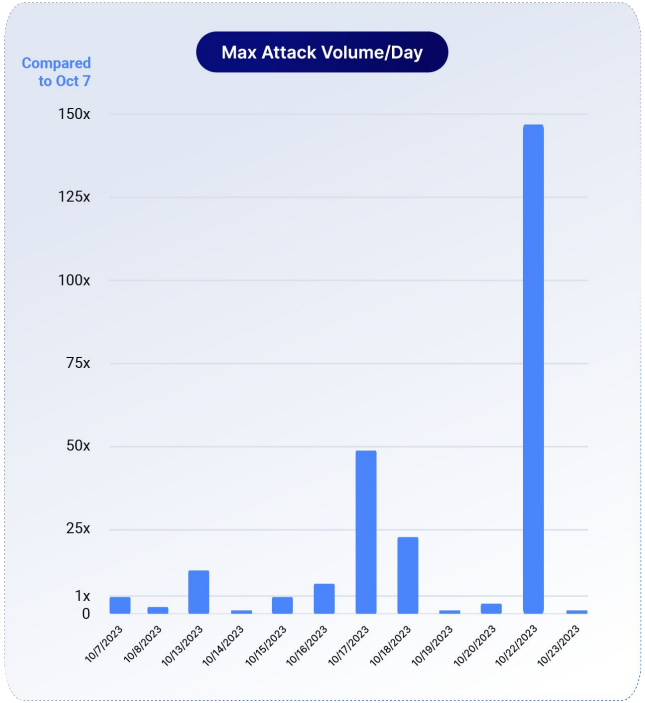


Web Attacks Against Israel Insights 2023

1. The war between Israel and Hamas has seen an ongoing series of cyberattacks waged against various Israeli institutions.
2. Hackers have ongoing access to significant and reliable source of financing for their activities.
3. Inconsistent in both timing and volume of attacks as well as lacking sophistication
4. Hackers have made it even easier than usual to identify and correlate their activities
5. All of these facts combined means that **defending against their attacks has been straightforward.**

Web Attacks Since Oct. 7th





What can we expect in 2024?

Continuous, Ever Increasing Challenge

- The capacity of recruit talents in the organization is getting weaker
- Growing sophisticated cyber attacks
- Adoption of new digital technology like AI
- Old legacy technology can’t take the new attacks
- Regulatory changes
- Geopolitical attacks for example on hospital to create more chaos
- Need to change from reactive to proactive
- Moving to a unified platform of cyber defense solutions to deal with increasing complexity

Got Questions?
We’ve Got Answers.

Contact us at **romy@reblaze.com**

Or visit **www.reblaze.com**

Reblaze Technologies Ltd.
3031 Tisch Way - 110 Plaza West,
San Jose, CA 95128

More Insights for 2023

- at the stage of the war, most of the attacks are aimed at harmMore than more attacks for espionage and information theft
- During this period we observed the use of techniques, tactics and procedures which were used frequently
  n other events in the world, such as the Ukraine-Russia war. About: Use of apostates and Wiper-type abusers

- A prominent attack outline is seen in a wide spraying activity - in this outline, an attempt was made
  exploit known vulnerabilities and human error in applying configuration settings
  Misconfiguration, such as the use of weak passwords and the lack of enforcement to lock an account
  After setting a threshold for failed authentication attempts.
- Extensive use of distributed denial of service (DDoS) attacks - at the application level
  (7Layer) (and at the media level as well as in website defacement (Defacement).
- Many attempts to penetrate various properties in the area - in order to obtain a hold and realize leaked information
  and/or data deletion (Wiper).
- Phishing attacks - through social engineering, both in emails and messages
  SMS to increase reliability. Sometimes an element of sending personal information of the recipient is even added,
  for him to activate the link or the link. It is true that this is a striking method of attack in the routine, but
  During the war, a significant increase in this type of campaign was observed.
  • Attacking mobile applications (smartphone applications) - or infrastructures of these applications,
  6 Through the publication of impersonating applications, exploiting security gaps in the application infrastructure, and more.
  • Assaults of organizations belonging to the MSP sector - which constitute an essential supply chain
  to many organizations in the economy. In this category you can find web hosting and hosting companies as well as companies
  Integration and provision of ICT services.

Web Security Insights **2023**

1. As the fighting drags on, the boldness and creativity of the attackers increases
2. Target organizations that serve many organizations -
3. Distributed Denial of Service (DDoS) attacks -
4. The existence redundancy
5. Using GeoLocation to prevent access by attackers from abroad

כלי תקיפה ושיטות בשימוש תוקפים

1. שימוש בשיטות תקיפה מבוססות כלים המותקנים ביעד התקיפה כחלק ממערכת ההפעלה או היישומים (LOLBAS (Living Off The Land Binaries, Scripts and Libraries.[8]
2. הנגשת כלי תקיפה לשימוש גורמים ללא ידע טכני. לדוגמה, הנגשת אתר הכולל Script לתקיפת מניעת שירות (DDoS) כאשר על התוקף רק להזין את כתובת יעד התקיפה.
3. ניצול שירותים לשיתוף קבצים לטובת הפעלת כלי תקיפה או שימוש ביוזר לגיטימי לצורך גישה ראשונית לרשת הארגון, תוך מעקף אמצעי האבטחה **וכן בערוץ להדלפת מידע.** שירותים בגון Microsoft OneDrive, Google Drive, Dropbox, Discord Servers.
4. שימוש בכלי קוד-פתוח (Open Source) שהוסבו על-ידי התוקפים, דוגמת DCOMpotato[9], כאשר חלק מכלים אלו עושים שימוש לרעה ב- WinAPI.[10]
5. שימוש בתשתיות Proxy ו-VPN חינמיות ומסחריות, או לחילופין עמדות קצה שהותקפו על מנת לשמש כ-Proxy ייעודי, לטובת עקיפת הגבלות בגון שימוש ב-GeoLocation למניעת גישה מחו"ל.
6. ניצול לרעה של פונקציונליות לגיטימיות של מערך הדוא"ל הארגוני, לאחר השתלטות על תיבת דואר של אחד ממשתמשי הארגון. לדוגמה, הגדרת חוקי Outlook/OWA/Office365 לשליחת העתק דוא"ל לתוקף ומחיקת ההודעה שנשלחה.
7. שימוש ב-Reverse Shell לשם יצירת קשר עם שרת הניהול (C&C) והדלפת מידע.[11]

Cyberwarfare 2023 - Key Takeaways

- Initial war phase lacked coordinated cyber attacks with the launch date; the significant surge happened six days later.
- The hackers repeatedly attacked various targets using the same group of IP addresses, making the connections between the attacks obvious.
- Terrorist-affiliated groups showed preparation with increased hostile activities before October 7, but the lack of immediate or organized escalation at the war's onset raises doubts about their coordinated cyberoffensive planning.