TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC

July 09, 2024

GLESEC 07/09/2024

TLP AMBER BOARDROOM

EXECUTIVE REPORT

This report corresponds to THIS MONTH and it is directed to Director or VP of IT, Cyber Security, Cyber Security Compliance or equivalent. The information is delivered following the GLESEC`s Seven Elements Cyber Security Model (7eCSM TM), these elements are: Risk, Vulnerabilities, Threats, Assets, Compliance, Cyber Security Validation and Access

ABOUT THIS REPORT

The purpose of this document is to report on the “state” of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed.

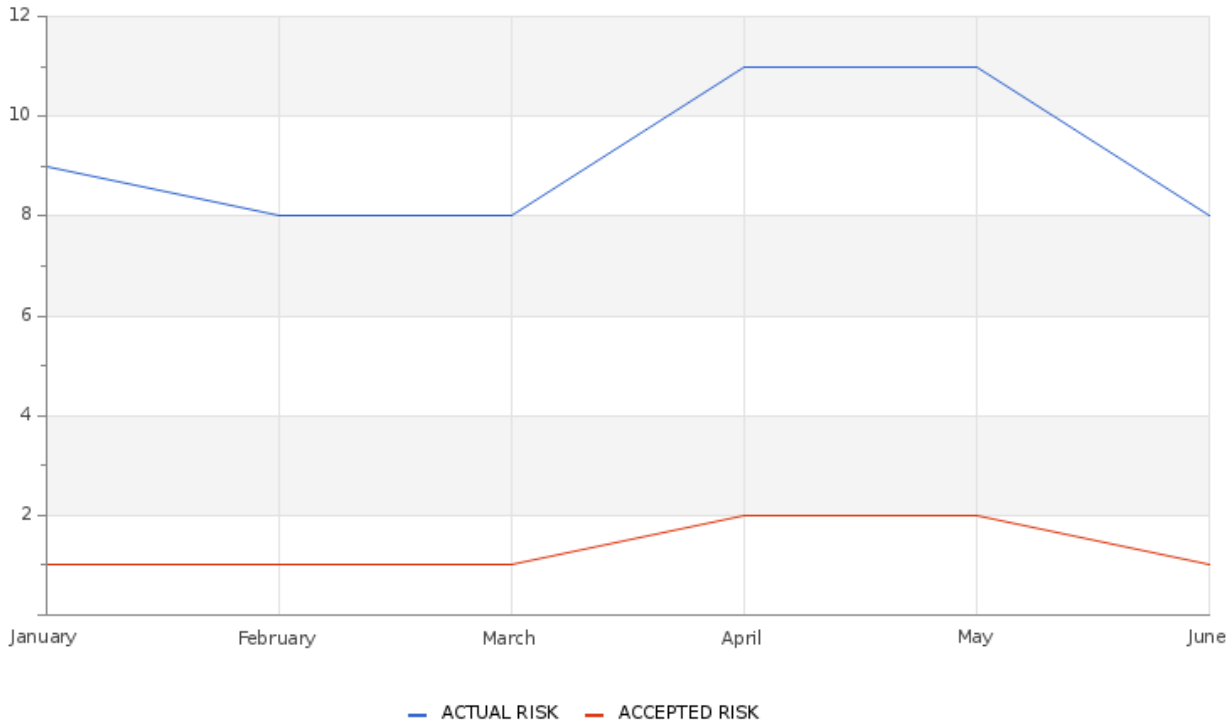
Actual Risk	Accepted Risk	Confidence
8%	1%	Medium

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 07/09/2024

Accepted & Actual Risk



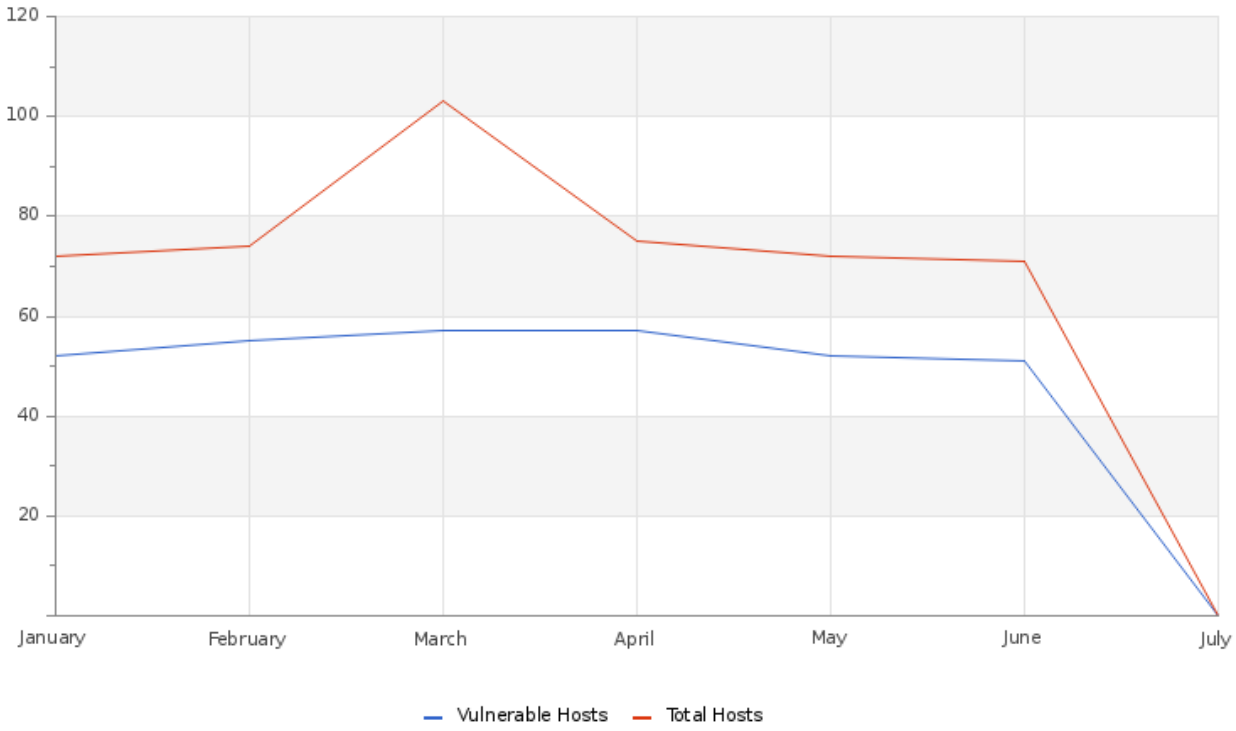
During the past month, risk levels have remained stable. Currently, the actual risk stands at 8%, while the accepted risk is 1%. These figures indicate continuity with respect to the previous month, when the actual risk was also 11% and the accepted risk was 0%.

Hosts & Vulnerable Hosts In Last 6 Months

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 07/09/2024



The graph illustrates a rise in the number of identified hosts coupled with a decline in vulnerabilities over the month, which may indicate potential breaches in the security perimeter. Noteworthy among the high-risk vulnerabilities are several iterations of Adobe Acrobat, each with distinct issues. Additionally, significant vulnerabilities include:
- Google Chrome < 123.0.6312.58 Multiple Vulnerabilities
- KB5035849: Windows 10 version 1809 / Windows Server 2019 Security Update (June 2024)
- OpenSSL 1.0.2 < 1.0.2zf Vulnerability
- Security Update for Microsoft Visual Studio Code (November 2023)

Total Attacks Successfully Blocked

10405

During the month, our systems identified and neutralized 10405 attempted attacks on your devices. Thanks to constant vigilance and rapid intervention, we have implemented specific strategies to counter continued attacks. It is important to note that a large proportion of these attempts came from compromised IP addresses and Botnets, known for their disruptive nature.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

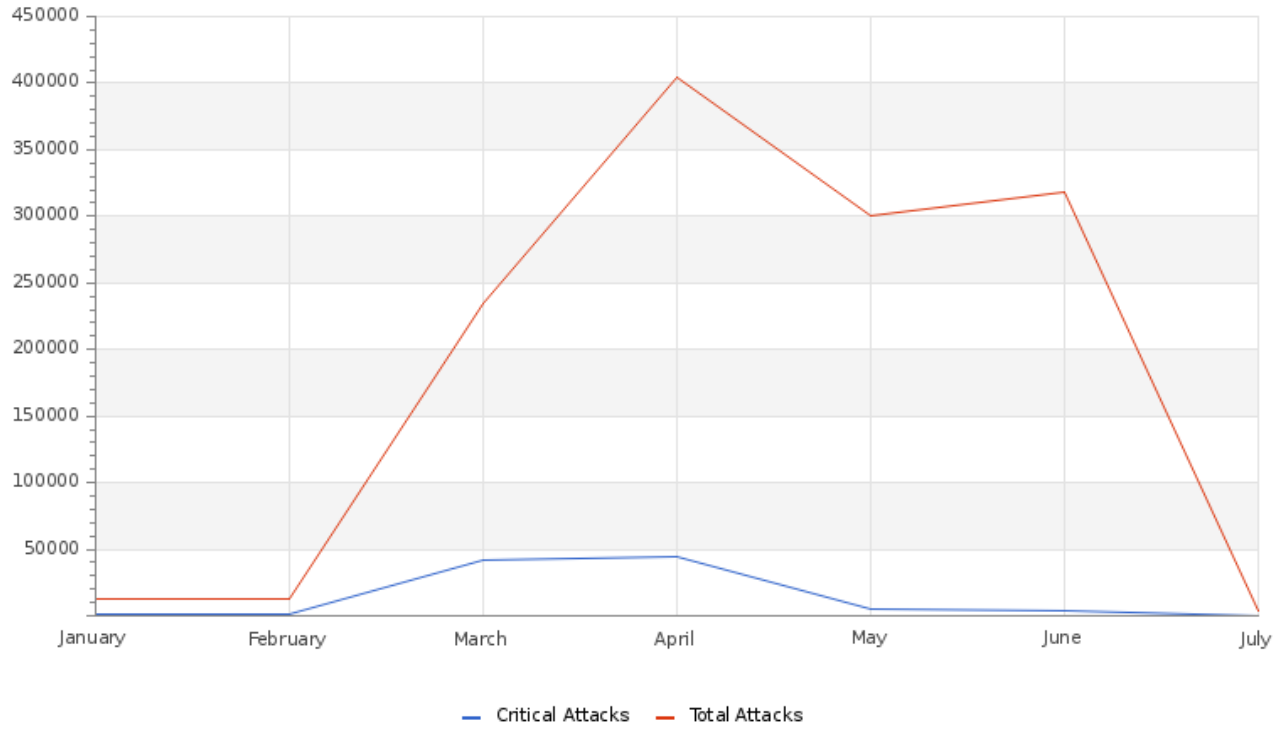
GLESEC 07/09/2024

Critical Attacks Successfully Blocked

18

Throughout this month, we managed to maintain the number at 18 critical attacks, in contrast to 393 incidents in the previous month. Our strategy, based on real-time intelligence, continues to provide a robust defense against emerging threats, including DDoS attacks, evolving IoT and novel DNS attack vectors. This is a clear demonstration of the effectiveness and adaptability of our system in the face of the changing threat landscape.

Attacks Successfully Blocked



The chart distinctly illustrates the positive effect of implemented security measures. Compared to the previous month, there has been a reduction in the total number of attacks, accompanied by an increase in the number of successfully thwarted attacks

Vulnerability Metric

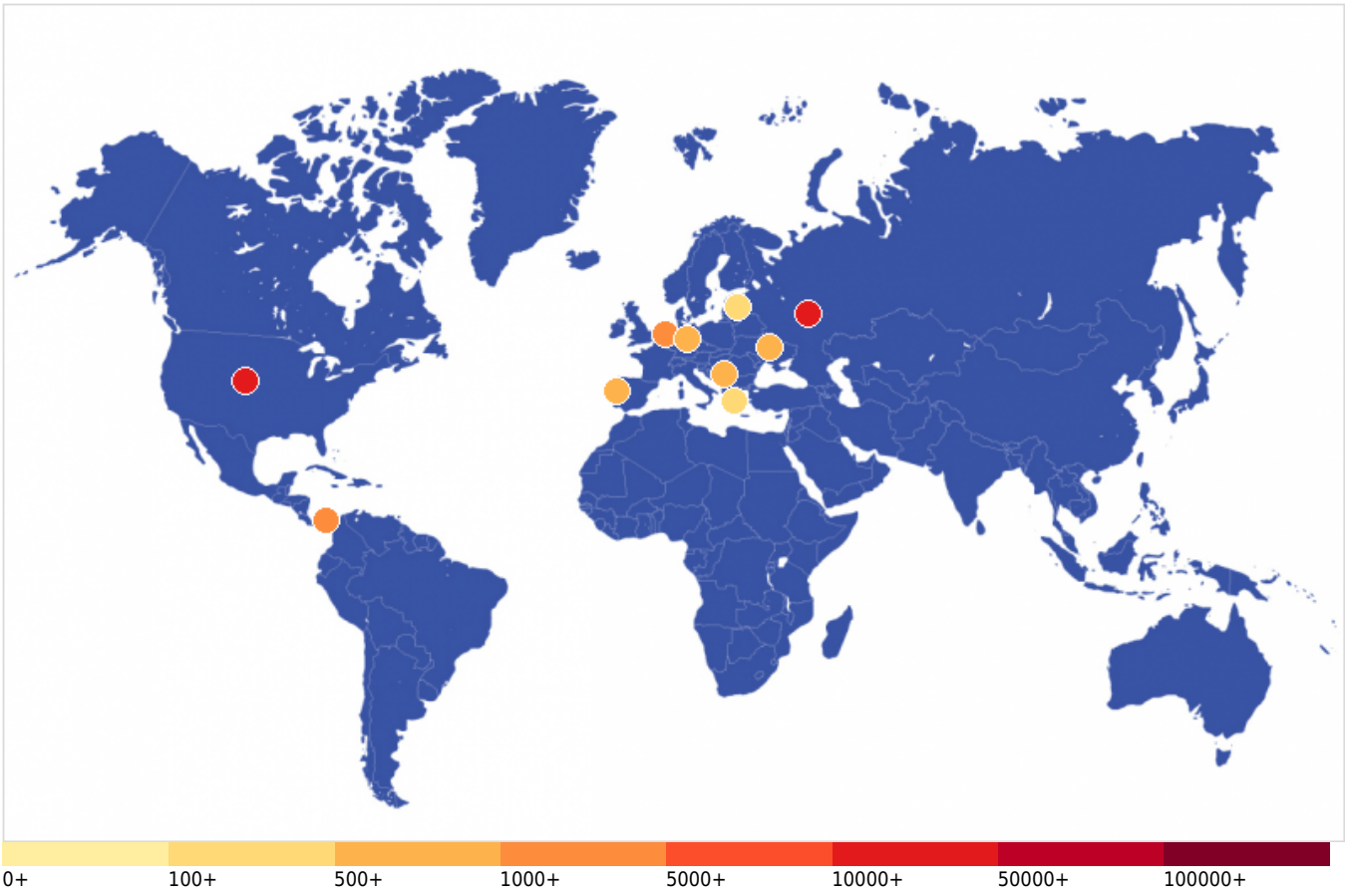
46

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 07/09/2024

Critical Attacks Per Country In Past Week



United States - 49340
Germany - 856
Greece - 456
Russia - 47052
Portugal - 622
Latvia - 395
Panama - 2281
Ukraine - 544
Netherlands - 1460
Serbia - 500

This graph displays the distribution of cyber attacks by country, highlighting the United States' dominance with 49,340 attacks. It is followed by the Russia with 47,052 and Panama with 2,281. Other countries like Netherlands, Germany, Portugal, Ukraine, Serbia, Greece, and Latvia report lower figures. The map underscores the need to focus cybersecurity efforts mainly on threats originating from the U.S., while maintaining global vigilance.

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500