



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC
May 21, 2024



GLESEC 05/21/2024

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

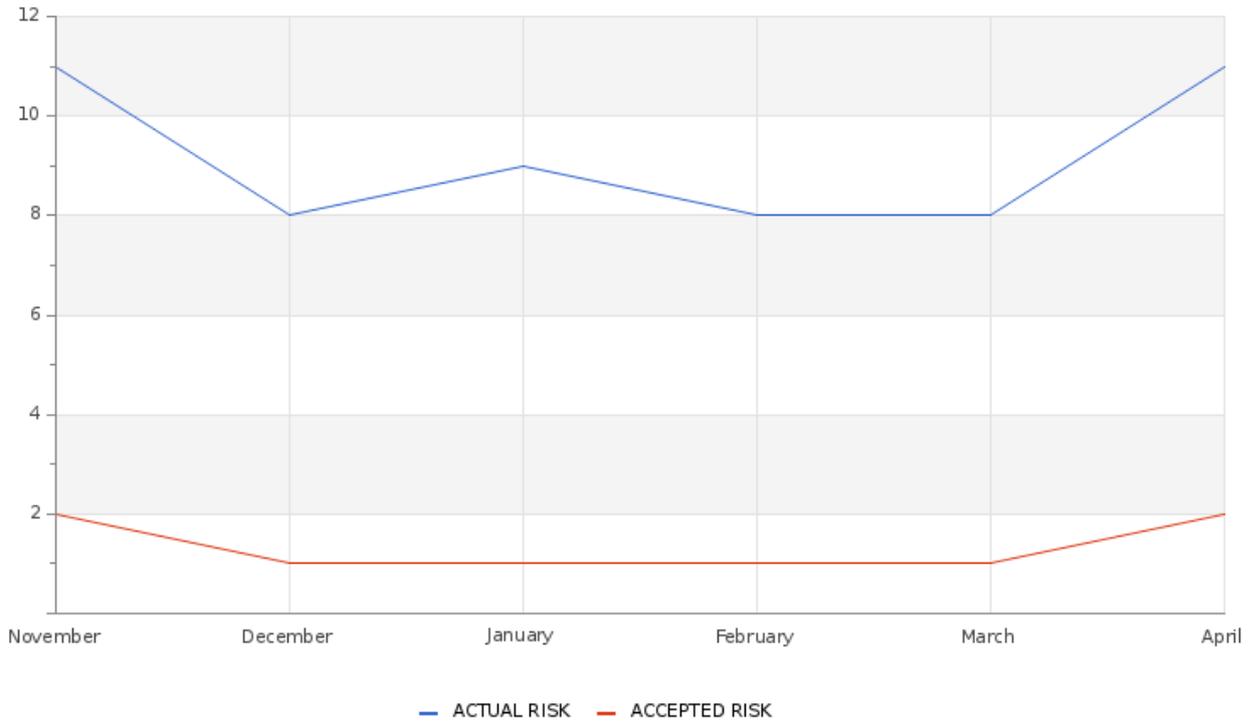
ABOUT THIS REPORT

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**11%****Accepted Risk****2%****Confidence****Medium**

GLESEC 05/21/2024

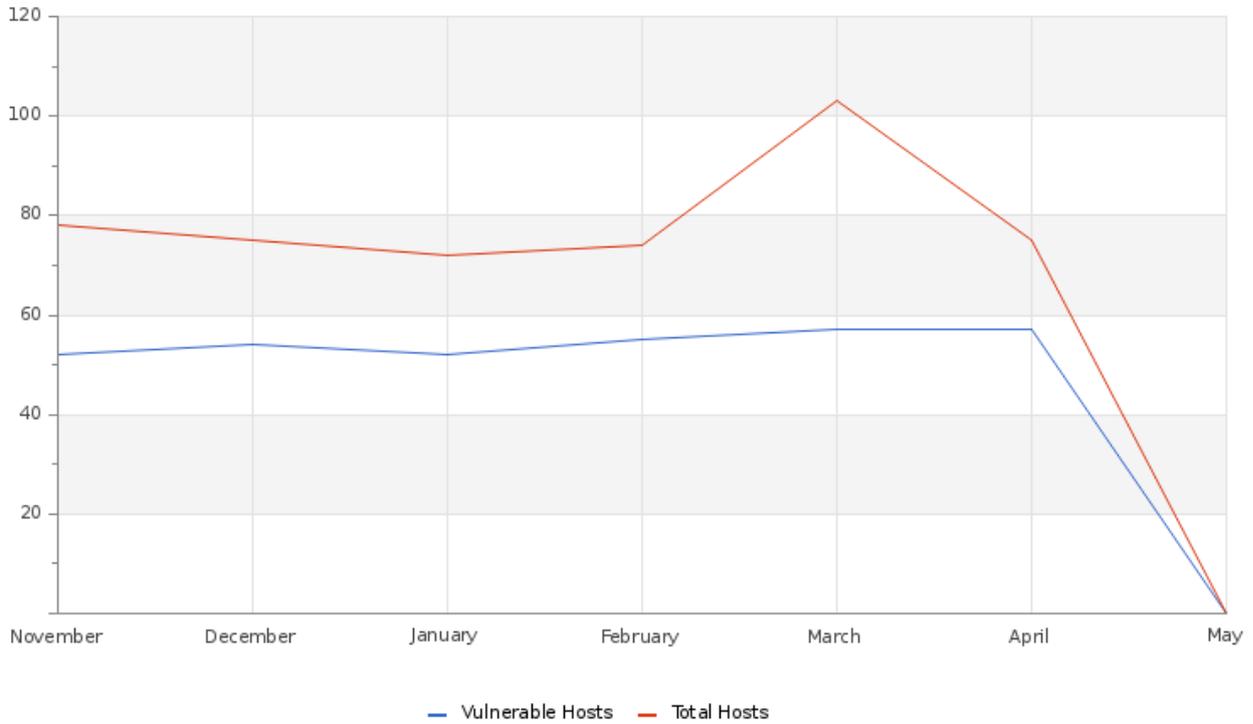
Accepted & Actual Risk



Over the course of this month, there has been a noticeable increase in the risk levels. The current risk now sits at 11%, and the accepted risk at 2%. This represents a significant rise from the previous month's figures, where the actual risk was recorded at 7% and the accepted risk at 1%.

GLESEC 05/21/2024

Hosts & Vulnerable Hosts In Last 6 Months



The graph illustrates a rise in the number of identified hosts coupled with a decline in vulnerabilities over the month, hinting at possible breaches in the security perimeter. Noteworthy among the high-risk vulnerabilities are several iterations of Adobe Acrobat, each with distinct vulnerabilities.

Total Attacks Successfully Blocked

18432

During the month, our systems identified and neutralized 18,432 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.

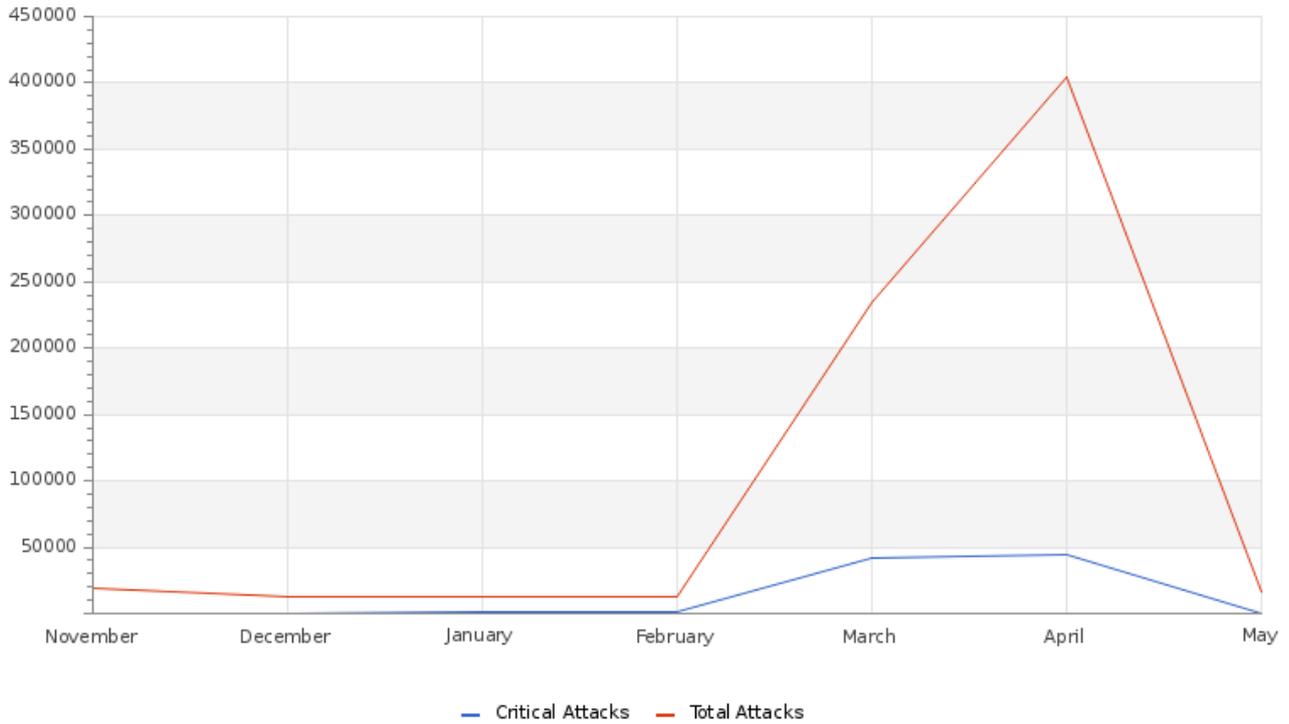
Critical Attacks Successfully Blocked

9

Throughout this month, we managed to maintain the number at 9 critical attacks, in contrast to 0 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.

GLESEC 05/21/2024

Attacks Successfully Blocked



The chart presents encouraging security outcomes, emphasizing the rise in successfully countered attacks. It proactively safeguards against emerging threats, including DDoS attacks, IoT botnets, advanced phishing methods, malware infiltrations, zero-day vulnerabilities, and complex DNS spoofing tactics.

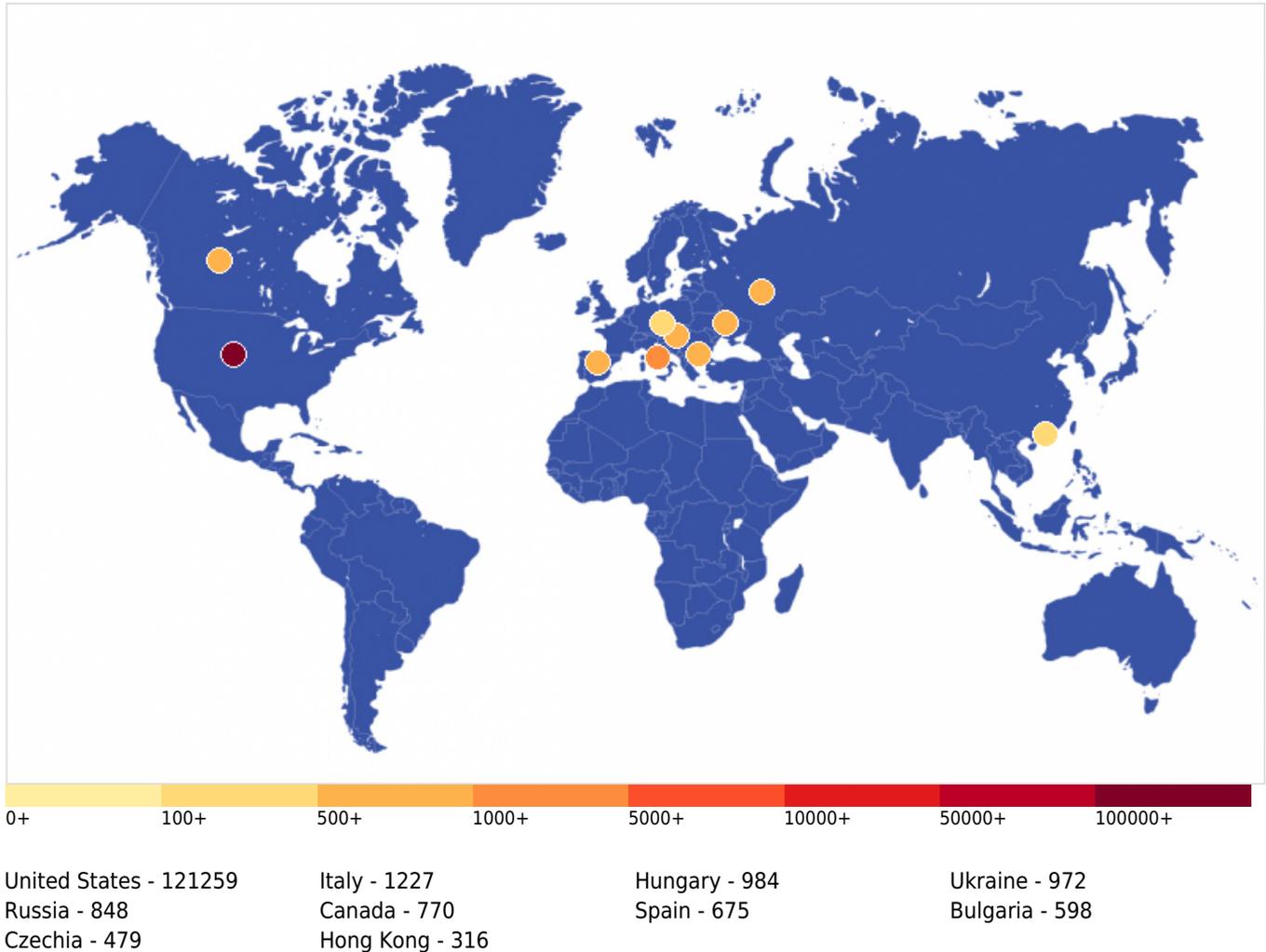
Vulnerability Metric

68

An analysis was conducted on 72 hosts based on their address range, revealing that 0 hosts are vulnerable. These vulnerabilities are categorized by severity, as outlined in the accompanying table. In this timeframe, we recorded 51 vulnerabilities of critical nature, 47 high-risk, 336 medium-risk, and 61 low-risk vulnerabilities. Based on these findings, your organization's vulnerability index is currently at 68%.

Critical Attacks Per Country In Past Week

GLESEC 05/21/2024



This graph displays the distribution of cyber attacks by country, highlighting the United States' dominance with 121,259 attacks. It is followed by the Italy with 1227 and Hungary with 984. Other countries like Ukraine, Russia, the Netherlands, Mexico, and India 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.**



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

HOW CAN WE HELP?

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

