Qualys Threat Research Unit (TRU) Launches 2023 TruRisk Research Report

March 28, 2023

Insights provide data-backed, actionable steps for security teams to decrease risk and increase the resilience of their organization

FOSTER CITY, Calif., March 28, 2023 /PRNewswire/ -- Qualys Inc. (NASDAQ: QLYS), a leading provider of cloud-based IT, security and compliance solutions, today released its 2023 TruRisk Research Report. The report traverses the global number of vulnerabilities detected by Qualys in 2022 – upwards of 2.3 billion. The findings of the report match the opportunistic behavior of threat actors who continue to be agile in modifying techniques to achieve successful exploits.

As digital transformation across businesses and governments is increasingly leveraged to accelerate productivity, new software tools to underpin these initiatives and programs is being developed quicker than ever. As technology continues to advance at a rapid pace, the number of software vulnerabilities surges, introducing significant levels of risk to organizations' environments.

Qualys' passion and vision for helping companies reduce their cyber risk has led the Qualys Threat Research Unit (TRU) to take a deep dive into the 13+ trillion events tracked by the renowned Qualys Cloud Platform. TRU mined anonymized detection statistics to uncover insights into the vulnerabilities found on devices, the security of web applications, misconfiguration of on-premises devices, and cloud security posture. Analysis of this extensive knowledgebase paired with TRU's unique visibility into threat actor activity – pre and post exploitation – yielded to five "Risk Facts."

Risk Fact #1: Speed is the key to out-maneuvering adversaries

On average, weaponized vulnerabilities are patched within 30.6 days while only being patched an average of 57.7% of the time. These same vulnerabilities are weaponized by attackers in 19.5 days on average. This means that attackers have 11.1 days of exploitation opportunities before organizations are able to patch.

Risk Fact #2: Automation is the difference between success and failure

According to the study, patches that could be automatically deployed were implemented 45% more frequently and 36% faster than manually deployed patches. Vulnerabilities where an automated patch could be applied have a mean time to remediation of 25.5 days while manually patched vulnerabilities took 39.8 days to be resolved. The patch rate for the automated set was 72.5% compared to 49.8% for the manual set.

Risk Fact #3: Initial Access Brokers (IABs) attack what organizations ignore

A growing trend in the threat actor landscape is a category called Initial Access Brokers (IABs) – sometimes called "affiliates." This report shows that while organizations are quicker at patching Windows and Chrome, threat actors – especially IABs – are forced to leverage vulnerabilities outside the "big two." IAB vulnerabilities have a mean time to remediation of 45.5 days, compared to 17.4 days for Windows and Chrome. The patch rates are also lower, patched at 68.3% compared to 82.9% for Windows and Chrome.

Risk Fact #4: Misconfigurations still prevalent in web applications

This study included anonymized detections in 2022 from the Qualys Web Application Scanner, which globally scanned 370,000 web applications and correlated data against the OWASP Top 10. The scans revealed more than 25 million vulnerabilities with 33% of them falling under the OWASP Category A05: Misconfiguration. These misconfigurations provided malicious actors with a gateway to spread malware in about 24,000 web applications.

Risk Fact #5: Infrastructure misconfigurations open the door to ransomware

TRU examined all controls failing more than 50% of their scans and the associated MITRE ATT&CK techniques linked to those specific controls. The top three techniques associated with failing controls for cloud misconfigurations were T1210: Exploitation of Remote Services, 1485: Data Destruction, and 1530: Data from Cloud Storage Object. This indicates misconfigurations in the cloud are exposing organizations to exploitation, encryption, and exfiltration. These three techniques describe exactly how ransomware operates today. These misconfigurations failed half of their scans with a pass rate of 49.4%. Failing misconfigurations are associated with enabling threat actors to move laterally within an organization.

"Adversaries make it their business to understand the vulnerabilities and weaknesses within their victims' environments, which can shift the balance of power in their favor," said Travis Smith, vice president of Threat Research Unit (TRU) at Qualys. "This report arms CISOs and security teams with unprecedented, data-backed insights for a holistic approach to understanding attack paths and threat actor behaviors to minimize risk."

Additional Resources

- Download the full report here
- Register for the 2023 TruRisk Research Report webinar here
- Learn more about the Qualys Threat Research Unit (TRU)
- Learn about the Qualys Cloud Platform
- Follow Qualys on LinkedIn and Twitter

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings.

The Qualys Cloud Platform leverages a single agent to continuously deliver critical security intelligence while enabling enterprises to automate the full spectrum of vulnerability detection, compliance, and protection for IT systems, workloads and web applications across on premises, endpoints, servers, public and private clouds, containers, and mobile devices. Founded in 1999 as one of the first SaaS security companies, Qualys has strategic partnerships and seamlessly integrates its vulnerability management capabilities into security offerings from cloud service providers, including Amazon Web Services, the Google Cloud Platform and Microsoft Azure, along with a number of leading managed service providers and global consulting organizations. For more information, please visit http://www.qualys.com.

Media Contact:
Jackie Dutton
Qualys
media@qualys.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/qualys-threat-research-unit-tru-launches-2023-trurisk-research-report-301783114.html

SOURCE Qualys, Inc.