CyberProof®
A UST Company

# A LOOK AT THE THREAT LANDSCAPE IN NUMBERS

Recent cyberattacks reflect new trends in cybersecurity. Here's some of what CyberProof's Cyber Threat Intelligence (CTI) team researched:

## 2400%

INCREASE IN THE NUMBER OF POSTS ON DARK WEB FORUMS ABOUT HOW TO EXPLOIT CHATGPT

The cybersecurity landscape has been significantly impacted by the deployment of AI by both defenders and adversaries. In January 2023, there were 120; in February 2023, there were 870; and in March, it peaked at 3,000.

## 135%

SURGE IN SOCIAL ENGINEERING ATTACKS

The emergence of AI tools facilitated a sharp increase in the number of social engineering campaigns between January and February 2023, when ChatGPT gained widespread adoption. AI's use has led to more sophisticated attacks and advanced defense mechanisms, sparking an arms race in cyberspace.

## 9.8%-46.5%

INCREASE IN CONFLICT-RELATED CYBER INCIDENTS IN EU

Russian Advanced Persistent Threat (APT) groups are actively targeting parties aligned with Ukraine.

## 11%

INCREASE IN HACKTIVIST ACTIVITY

In the first half of 2023, with geopolitical conflicts between Russia and Ukraine spilling into the digital domain, we've witnessed an increase in cyber proxy wars, hacktivism, and a marked rise in targeted attacks against critical infrastructure.

## 95%

INCREASE IN RANSOMWARE ATTACKS, HITTING AN ALL-TIME HIGH

The accessibility of Ransomware-as-a-Service also democratizes the tools required for complex cyberattacks, suggesting an escalation in both the frequency and sophistication of ransomware incidents.

## 2,700

ORGANIZATIONS WERE EXTORTED IN ONE CYBERATTACK

The Clop ransomware group conducted a far-reaching attack in 2023 that began with one compromised environment.

## 78%

OF ORGANIZATIONS ATTACKED BY RANSOMWARE FACED MULTI-FACETED EXTORTION

We can expect continued innovation of attack strategies, as adversaries leverage zero-day exploits and adapt to exploit new and existing vulnerabilities in increasingly interconnected IT and OT environments.

## ORGANIZATIONS MUST PRIORITIZE RESILIENCE AND ADAPTABILITY IN THEIR CYBERSECURITY STRATEGIES.

It is crucial to maintain vigilance, foster continuous learning, and embrace a proactive approach to cybersecurity. The digital threats we face will continue to evolve, but with collective effort and collaboration, we can fortify defenses and safeguard the integral systems that support our society.

Learn more about cyberattack trends!

DOWNLOAD THE REPORT →

CyberProof®
A UST Company