GATEWATCHER

Cyber threats SEMESTER REPORT_

January - June 2023

Cyber threats decoded by Gatewatcher Purple Team

Executive Summary

Provide your security teams with greater visibility in an evolving cyber risk landscape.

THE ESSENTIAL

Ranking of the most utilised *malwares* by cyber attackers_

Emotet, previously a leading threat, has been displaced from the top three due to Microsoft's deactivation of Office macros, its primary attack vector, and is replaced by Qbot. Despite authorities' efforts, Mirai maintains overwhelming supremacy, supported by its numerous variants and multi-architecture infection capabilities. Payload, while secondary, remains more frequently employed in the infection chain. Cobalt Strike also reinforces its position.

Exploited files types by attackers and their evolution_

The ranking remains dominated by Windows binaries, HTML, and ELF, driven by cross-platform attacks against Linux, highlighting the rapid evolution of the cybersecurity threat landscape. The most notable evolution concerns the rise of portable executable files containing malicious DLL exploitation capabilities, contributing to fileless attacks.

Most active *threat actors*_

Analysis of tactics employed, with a focus on supply chain attacks through examples such as PyPI/W4SP, 3CX, MOVEit, and Jumpcloud, as well as the Russian Turla group.

Sectors particularly targered by threats_

Education consistently features in cyberattack headlines, ranking third among the most targeted sectors behind technology and energy: detailed analysis. Focus on new threats targeting Operational Technology (OT) systems in the context of Industry 4.0 growth.

Impact of *leaked identifiers*_

Latest novelty of this semi-annual report is a summary of leaked identifiers (email addresses + passwords) due to malwares, phishing, etc. Entrepreneurial domain names, technology companies, NGOs, and the education system lead the list. Special attention to vulnerabilities in public sectors.

EXPLORE THE TECHNICAL ANALYSIS PROVIDED BY OUR EXPERTS ON:

- The popularisation of legitimate tool hijacking by cybercriminals illustrated through the example of WMI.
- The increasing use of PowerShell by cybercriminals in intrusion scenarios.

To maintain the highest level of protection, our Purple Team experts actively monitor and analyse cyber threats based on the rich telemetry of Gatewatcher's #NDR and #CTI platforms.

Find out more about our teams' insights on major trends in cyber activity over the past six months in this third Cyber Threat Semester Report.

DOWNLOAD THE REPORT