ATTACK SURFACE ANALYSIS

LEBANON 2021 - SEMESTER 2

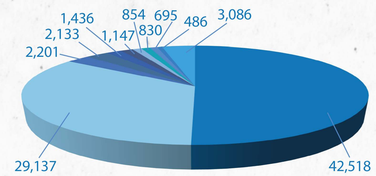
PERIMETER ANALYSIS

761 CRITICAL VULNERABILITIES

IP ADDRESSES **105,853**

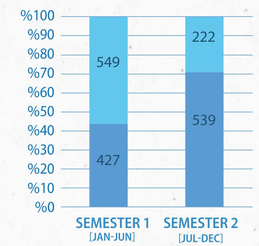
67,949 IP ADDRESSES WITH DOMAINS

DOMAINS **198,354**



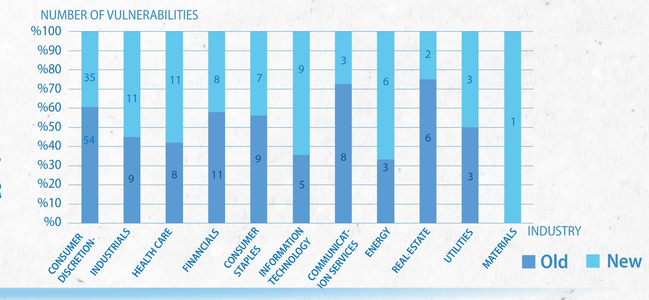
50% of the systems are hosted within the **Lebanon** territory

VULNERABILITY POSTURE



50 % OF THE VULNERABILITIES IDENTIFIED OVER THE PREVIOUS SEMESTER [OLD] ARE **STILL OPEN**

TOTAL OF 222 NEW VULNERABILITIES INCREASE OVER THE FIRST SEMESTER



WORLD KEY TRENDS

JUNE — **80,000 CUSTOMERS** COULD HAVE BEEN HIJACKED WITH THEIR SENSITIVE INFORMATION BEING LEAKED **OUT OF JIRA** AS PER CHECK POINT RESEARCH

JULY — **THE EUROPEAN BANKING AUTHORITY (EBA)** SUBJECTED A CYBER-ATTACK AGAINST ITS **MICROSOFT EXCHANGE** SERVERS. THE EBA TOOK ITS EMAIL SYSTEMS OFFLINE

JULY — **US CISA** REPORTS THAT THE ATTACKERS' FAVORITE NEW TARGETS ARE VULNERABILITIES PUBLISHED AFTER 2019 WITH **CITRIX ADC GATEWAY AND CISCO ASA** ON TOP EXPLOITED ONES

SEPTEMBER — **MERIS BOTNET** BREAKS DDOS RECORD **VIA DNS** WITH 21.8 MILLION RPS ATTACK AGAINST RUSSIAN YANDEX. ATTACKERS COMPROMISED 56.000 MIKROTIK RELATED DEVICES

OCTOBER — **SOPHOS RESPONSE TEAM** DISCOVERED A RANSOMWARE GROUP EXPLOITING **CONFLUENCE** VULNERABILITY TO DISRUPT ENDPOINT PROTECTION SOFTWARE

DECEMBER — **LOG4J CRITICAL FLAW** RATED 10.0 IMPACTING THE ENTIRE INTERNET LED TO MORE THAN 800.000 ATTACKS AFTER A WEEK OF PUBLISHING EXPLOIT

KEY OBSERVABLE VULNERABILITIES

Exchange — **Microsoft Exchange Server** Unauthenticated Remote Code Execution Vulnerability

citrix — Unauthenticated Remote Code Execution in **Critix ADC Gateway**

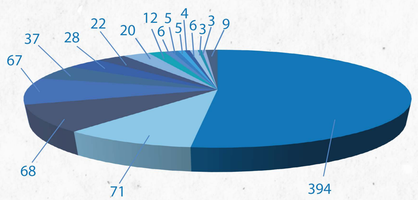
LOG4J — Unauthenticated Remote Code Execution Vulnerability in **Log4j**

Confluence — Unauthenticated Remote Code Execution in **Atlassian confluence Server**

JIRA — Unauthenticated Remote Code Execution in **Jira Service Management Data Center and Server**

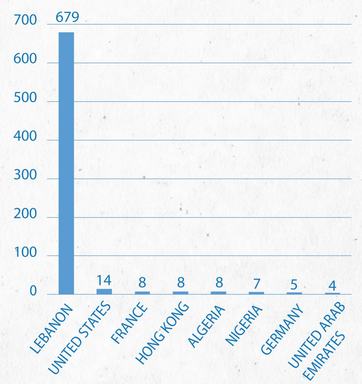
MikroTik — Unauthenticated Remote Code Execution in **Mikrotik router**

CRITICAL VULNERABILITIES

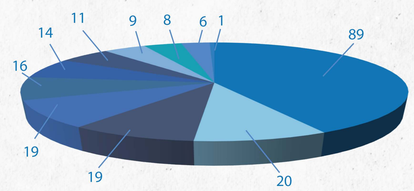


CRITICAL VULNERABILITIES ACTIVELY USED BY THREAT ACTORS FOR MORE THAN TWO YEARS [80%] **ARE STILL WIDELY OPEN IN LEBANON'S TERRITORY**

89% OF VULNERABILITIES ARE MAPPED TO ASSETS HOSTED WITHIN THE COUNTRY TERRITORY



INDUSTRY IMPACTED



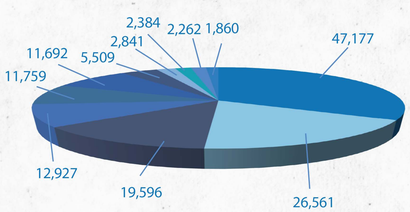
212 CRITICAL VULNERABILITIES CLEARLY ATTRIBUTED TO LEBANESE SECTORS

COSUMER DISCRETIONARY FOLLOWED BY INDUSTRIALS AND HEALTHCARE ARE THE MOST IMPACTED SECTORS

MANY VULNERABILITIES ARE PENDING REMEDIATIONS AFTER SEVERAL NOTIFICATIONS

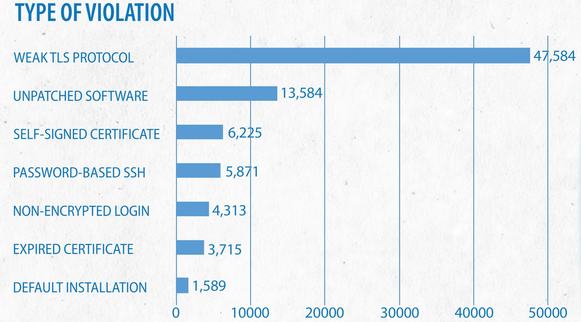
COMPLIANCE VIOLATION ANALYSIS

UNPATCHED VULNERABLE SOFTWARE



AGING UNPATCHED SECURITY ISSUES IN SOFTWARE **BEYOND TEN YEARS**

TYPE OF VIOLATION



VERY HIGH NUMBER OF SECURITY COMPLIANCE VIOLATIONS ESPECIALLY IN TERMS OF OLD CONFIGURATIONS AND UNPATCHED SOFTWARE

WHO WE ARE

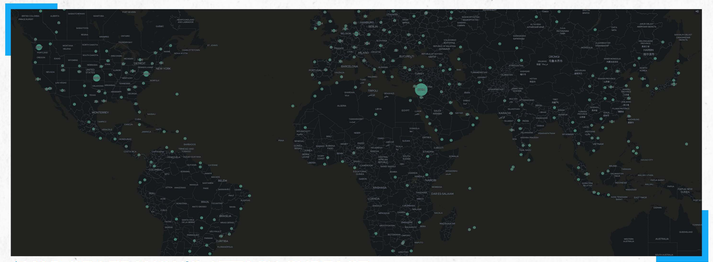
LEBANON CYBER EMPOWERING RESEARCH TEAM
A NON-PROFIT ORGANIZATION FOCUSED ON PROVIDING A MORE SECURE CYBER SPACE IN LEBANON

WHAT WE DO

WE CONSTANTLY MONITOR THE ATTACK SURFACE OF LEBANON, REGULARLY LOOKUP FOR NEWLY PUBLISHED VULNERABILITIES, AND INFORM ACCOUNTABLE OWNERS OF IMPACTED SYSTEMS

MORE DETAILS

- 00961 76 85 71 34
- info@lebanoncert.org
- https://lebanoncert.org



*MAP OF LEBANON'S ATTACK SURFACE