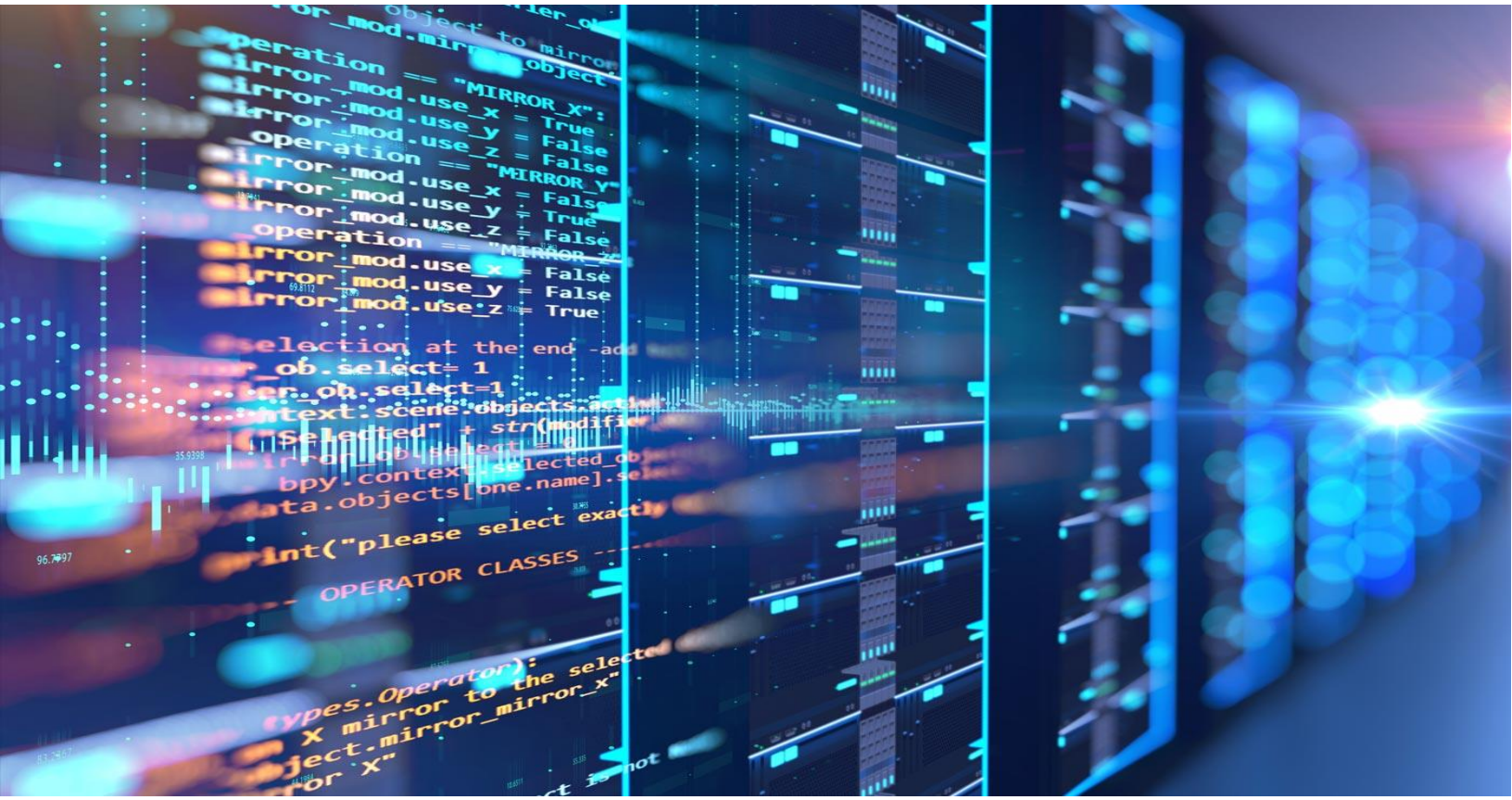
ADACOM
CYBER SECURITY



The Vulnerability Landscape of Greece™

Technical Report, November 2018

Legal notice

Notice must be taken that this publication represents the views and interpretations of ADACOM, unless stated otherwise. This publication should not be construed to be a legal action of ADACOM. This publication does not necessarily represent state-of the-art and ADACOM may update it from time to time. ADACOM is not responsible for the content of the external sources including external websites referenced in this publication. This publication is intended for information purposes only. It must be accessible free of charge. Neither ADACOM nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Contents

1 Foreword

The current report contains a statistical analysis of the security findings discovered by ADACOM Cyber Security during a period of three years and a sample of 200 security engagements of various types. The findings represent actual vulnerabilities discovered and/or exploited in a number of systems hosted/managed by organizations mainly established in Greece.

Our objective is to report on these findings with a contextual approach and provide an expert analysis on their source, as well as advise on their remediation.

Data contained in this report come from five (5) different types of assessments, notably:

- Infrastructure Security Assessment (ISA): assessing the security posture of networks, operating system and application servers;
- Web Application Security Assessment (WASA): assessing the security posture of web applications;
- Mobile Application Security Assessment (MASA): assessing the mobile application and the corresponding back end systems;
- WiFi Security Assessment (WISA): assessing threats against WiFi networks – although a different service, for the purposes of this report, the WiFi assessment results have been included into the infrastructure assessment results;
- Social Engineering Assessment (SEA): assessing the human element with regards to cyber security.

2 Demographics

2.1 Period of Performance

The data gathered refer to a period of almost three years, from January 2016 to October 2018, and correspond to 192 different engagements for 30 different organizations belonging to 12 different vertical markets.

Out of this number, the findings from retests have been eliminated on purpose, since they do not provide original vulnerability findings. Findings of subsidiary companies outside Greece were also eliminated, since the main purpose of this report is to present the vulnerability landscape of Greece. Same applied to data gathered from purpose-build assignments (i.e. check against a specific vulnerability).

2.2 Types of Projects

The following pie chart presents the percentage of the engagement types during the abovementioned time period.

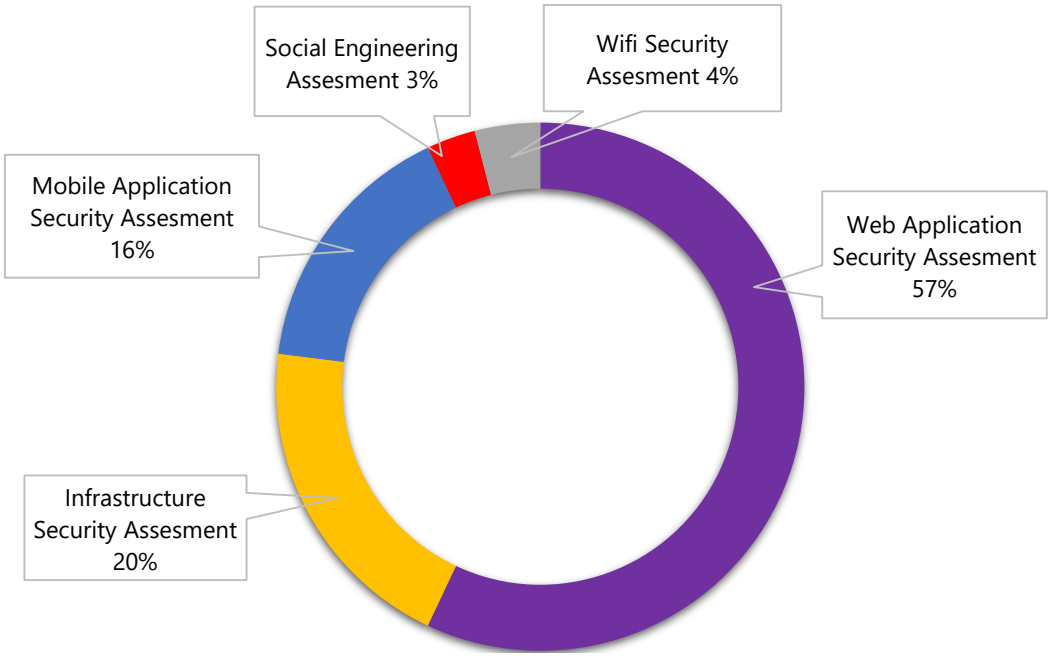


Figure 1: Engagement Types

The following figures represent data from the remaining 88 engagements, their split per year and assessment type[1].

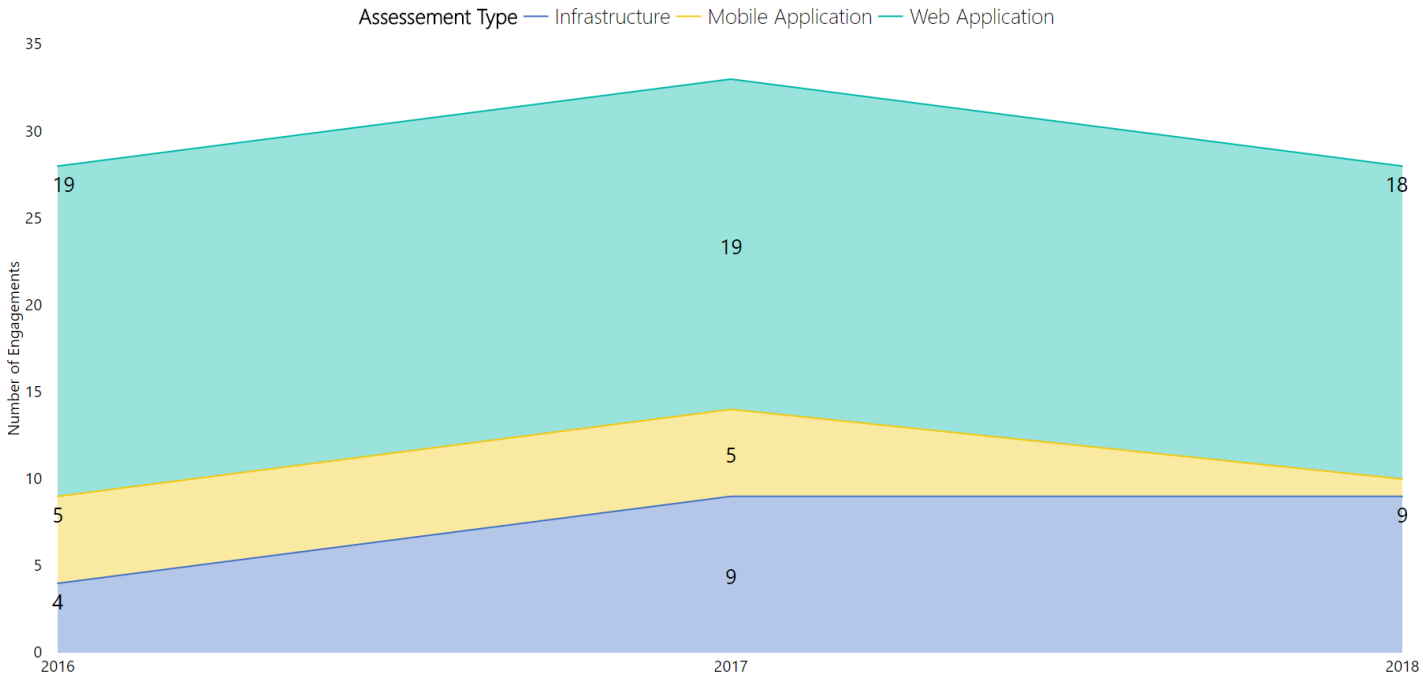


Figure 2: Number and Types of Valid Engagements per year

The organizations examined belong to a number of different verticals, representing a total of 30 unique entities:

Banking and Finance	Payments and Fintech
Management Consulting	Insurance
Manufacturing	Telecommunications
Transportation	Electronic Commerce
FMCG	Pharmaceutical
Private Sector (Other)	Public Sector

Table 1: Vertical Market

[1] For Year 2018, data are available for the period 01/01 – 31/10.

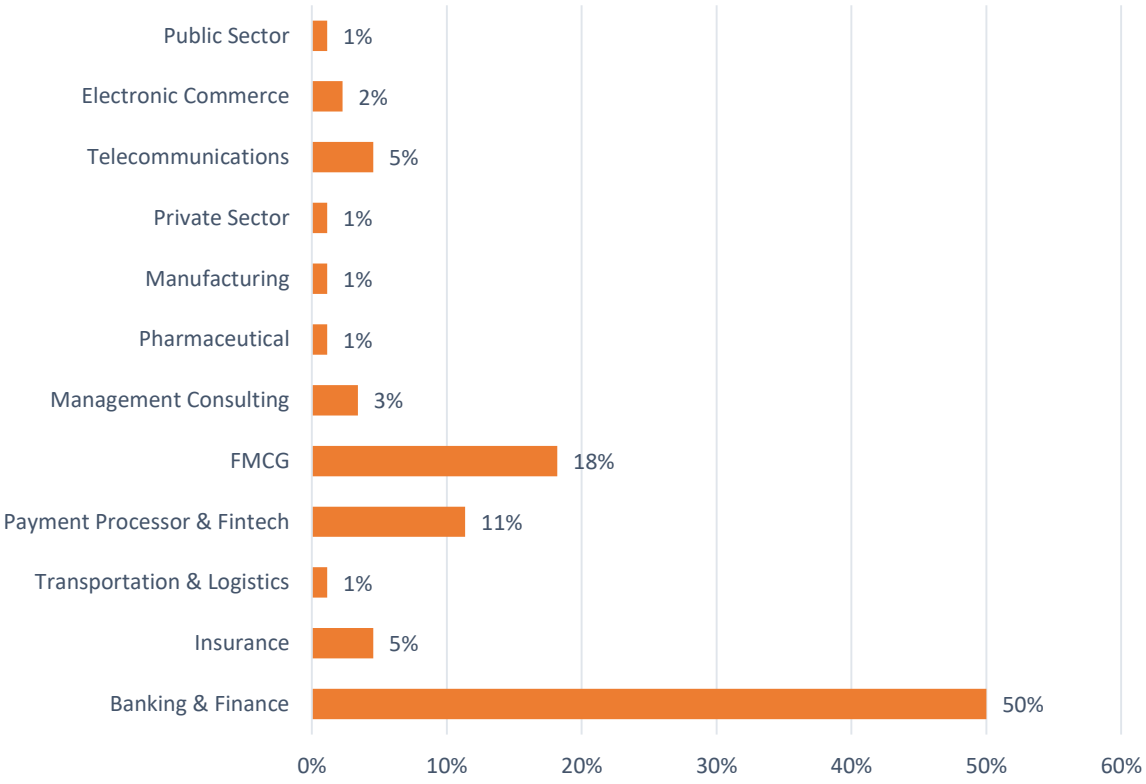


Figure 3: Percentage of Engagements per vertical market

3 Overview of Findings

3.1 Average Number of Findings and Risk Rating

Many of the findings identified during 2016 (the starting point for our analysis) may still be present, as detected by recent tests (so-called re-test).

In 2017, a number of cybersecurity breaches and critical findings were investigated, in the light of security assessment engagements. These breaches are the result of technical misconfigurations or insufficient patching of the affected systems.

Figure 4: Average number of findings per engagement

Figure 5: Critical Findings per engagement

The average number of findings per engagement was 30, while 6 out of these 30 findings (a staggering 20%) were classified as critical.

Our findings were also categorized per assessment type (infrastructure, web application and mobile application) and Threat Level, as per below chart:

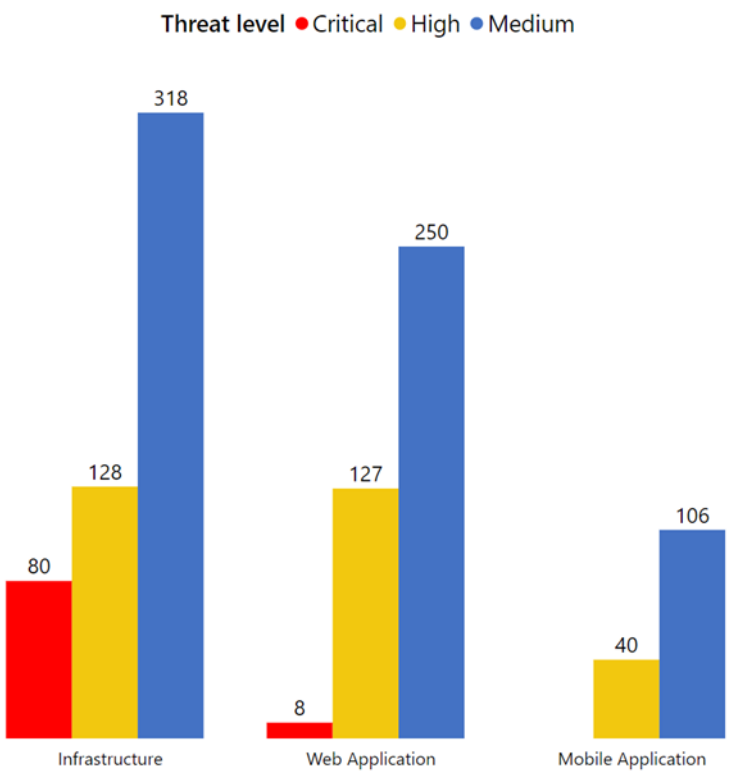


Figure 6: Summary of Findings per assessment type.

Overall, more than 1000 vulnerabilities were discovered. The following visualization represents their distribution per assessment category and their risk rating.

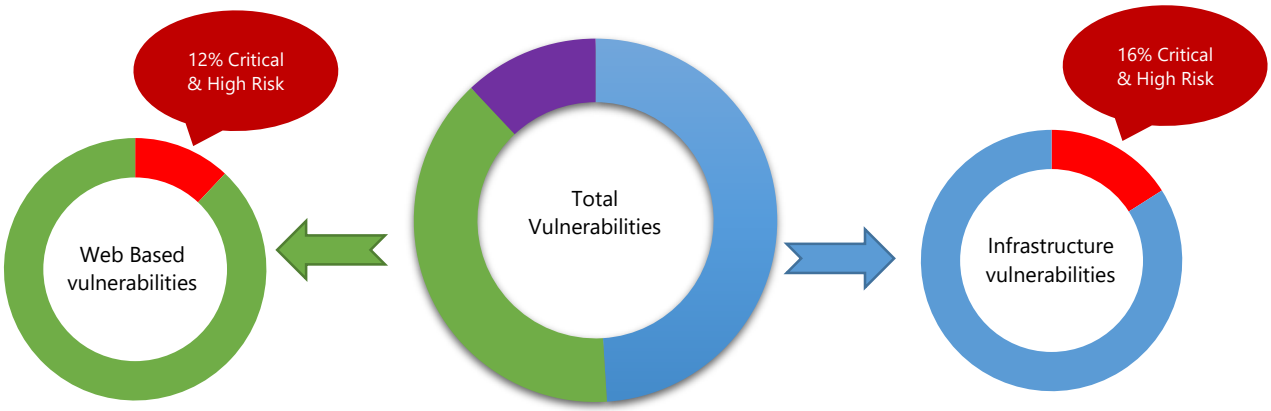


Figure 7: Summary of Vulnerabilities per assessment type and risk rating.

Finally, the consolidated number of findings per assessment type is presented in the following chart:

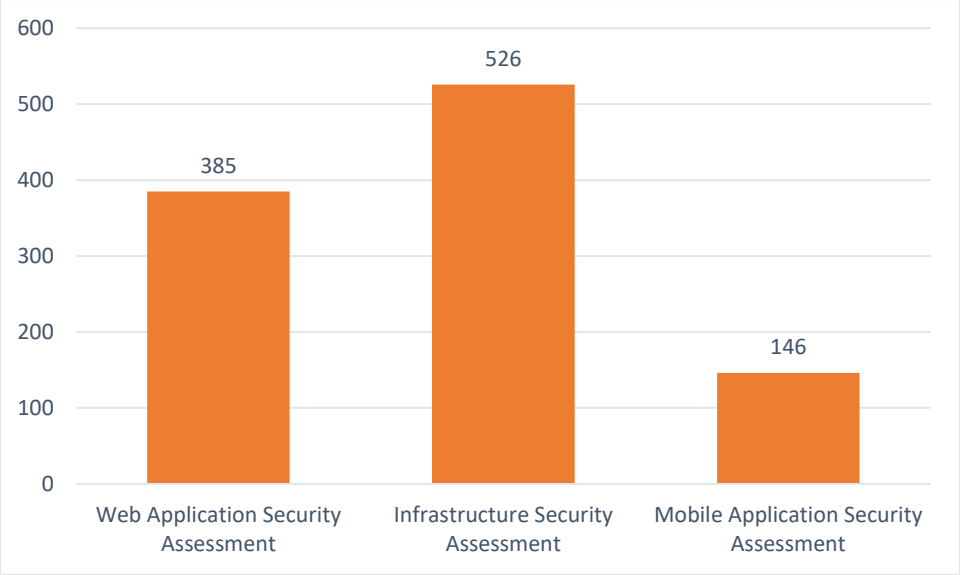


Table 2: Total Number of Discovered Findings per assessment type

3.2 Infrastructure Assessment

3.2.1 Summary

The following pie chart presents an overview of infrastructure assessment findings and their corresponding risk rating:

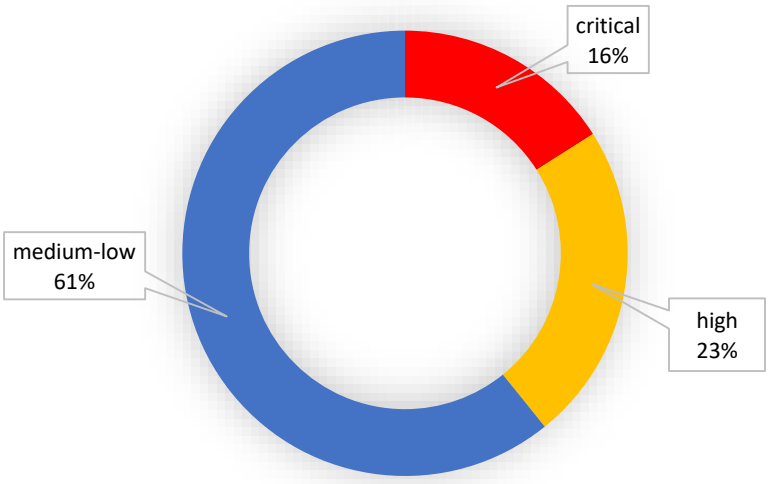


Figure 8: Infrastructure Assessment vulnerabilities risk rating

3.2.2 Findings

The following figure presents an overview of the categories of vulnerability types discovered in infrastructure assessments.

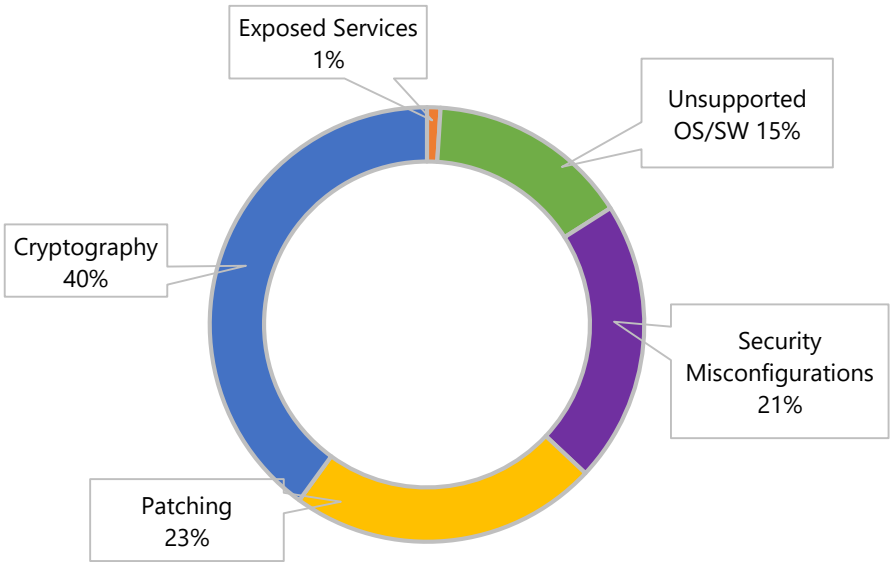


Figure 9: Types of Infrastructure Assessment Vulnerabilities

3.2.3 Commentary

Although usage of insecure or misconfigured cryptography seems to hold the major percentage (approximately 40%), **the vast majority of vulnerabilities originate from improper systems security maintenance** (approx. 59%), due to unsupported operating system and/or application software, improper patching and security misconfigurations. Is it worth noting that a hardened perimeter is a commonplace in Greek organizations, since only 1% of the findings were due to improperly exposed services.

The most common vulnerability finding in infrastructure security assessment was "***SSL Medium Strength Cipher Suites Supported*".**

Notably, the oldest vulnerability discovered was almost 20 years old (SNMP Agent Default Community Name, CVE-1999-0517).

3.3 Web Application Assessment

3.3.1 Summary

The following figure presents an overview of web application findings and their corresponding risk rating

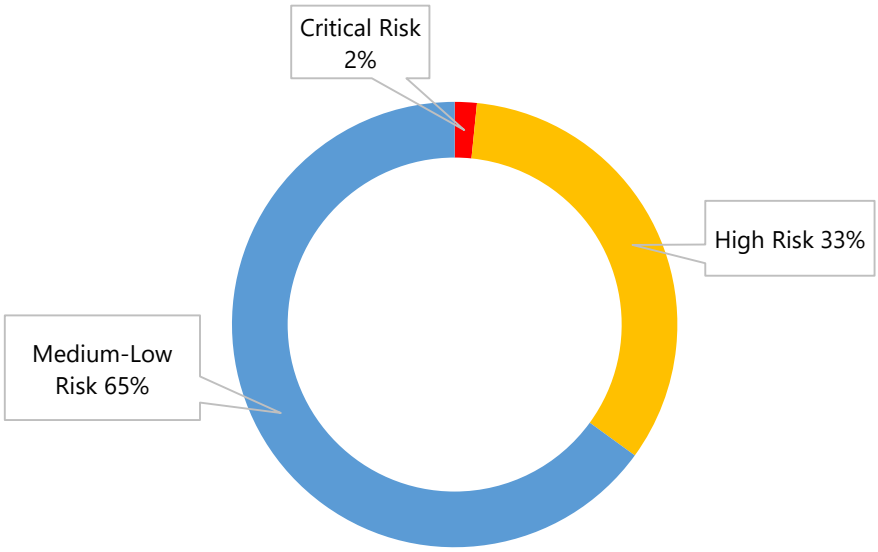


Figure 10: Web Application Assessment vulnerabilities risk rating

3.3.2 Findings

The following figure presents an overview of the categories of vulnerability types discovered in web application assessments.

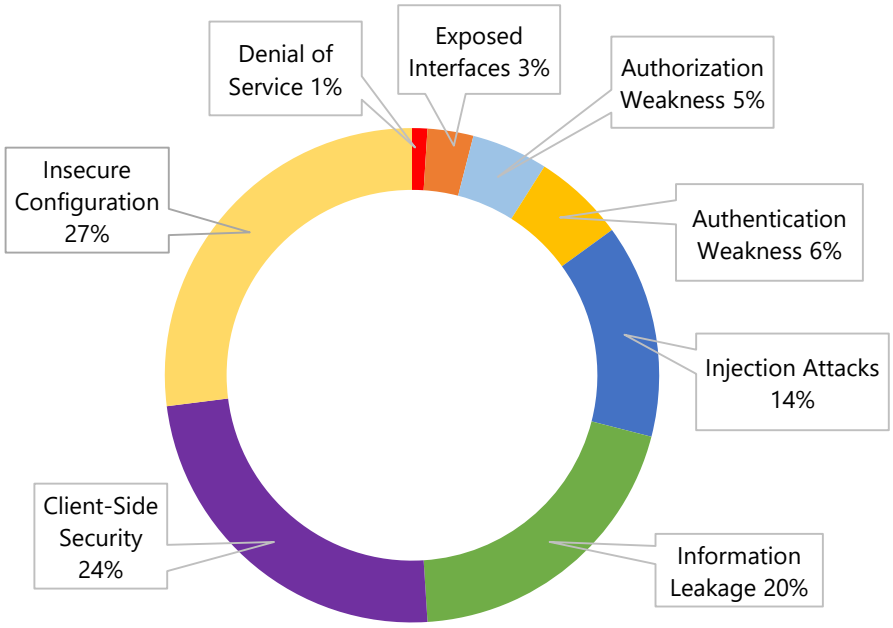


Figure 11: Types of Web Application Vulnerabilities

3.3.3 Commentary

The web application assessment findings originate from a number of different origins. The majority of those are due to insecure configuration of the web/application server (approximately 27%). However, it is worth considering that injection attacks, in combination with exposed information and authentication/authorization weaknesses are a result of insecure programming practices or non-properly testing protocols. It is worth noting that, from an availability point of view, only a tiny percentage of vulnerabilities can lead to Denial of Service.

The most common vulnerability category in web application assessment was "**Host Header Injection"**.

3.4 Mobile Application Assessment

3.4.1 Summary

The following figure presents an overview of mobile application findings and their corresponding risk rating.

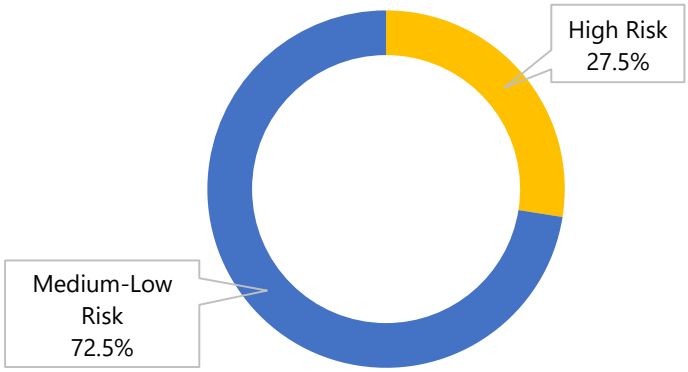


Figure 12: Mobile Application Assessment vulnerabilities risk rating

3.4.2 Findings

The following figure presents an overview of the categories of vulnerability types discovered in mobile application assessments.

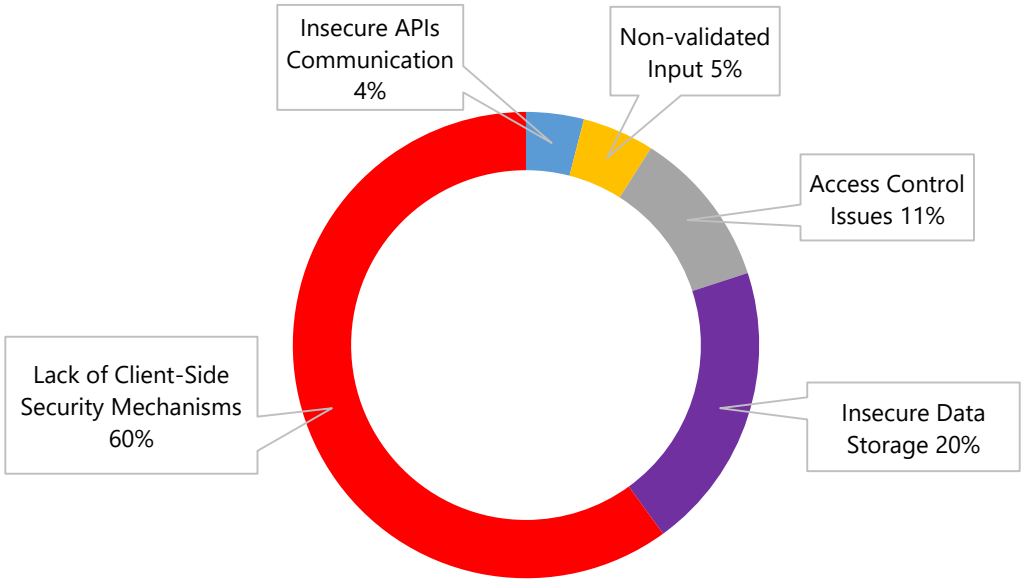


Figure 13: Types of Mobile vulnerabilities

3.4.3 Commentary

The most common vulnerability category in mobile assessment was "**Lack of Certificate Pinning**". The second category, according to findings numbers, concerns "**Insecure Data Storage**", a common issue that occurs due to insufficient storage protection of sensitive data. It is worth mentioning that "**Access Controls**" issues still exist in modern mobile applications, where the lack of enforcement pertaining to users or functions is the main characteristic.

As it derives from several Penetration Testing projects in Mobile Applications, a couple of "wrong" permissions would do the work for us. Careful development and deployment with APIs is highly suggested for constructing a "fortress" against Mobile Application attackers.

3.5 Social Engineering

3.5.1 Summary

Social Engineering is all about the exploitation of the human factor, and is therefore a human-centric attack. The main purpose is to identify personnel awareness related to cyber security, while also testing the readiness of the organization when such an attack occurs. The main stages of a social engineering attack are presented in the following figure.

Figure 14: Stages of a Social Engineering Attack

Most commonly, a phishing campaign is luring the victims to give away their credentials (via phone and/or email). In most occasions, social engineering attacks are combined with other assessment services; viz. infrastructure and web application assessments, as a means of lateral movement, privilege escalation etc.

3.5.2 Findings

The following figure presents an overview of the findings during social engineering attacks.

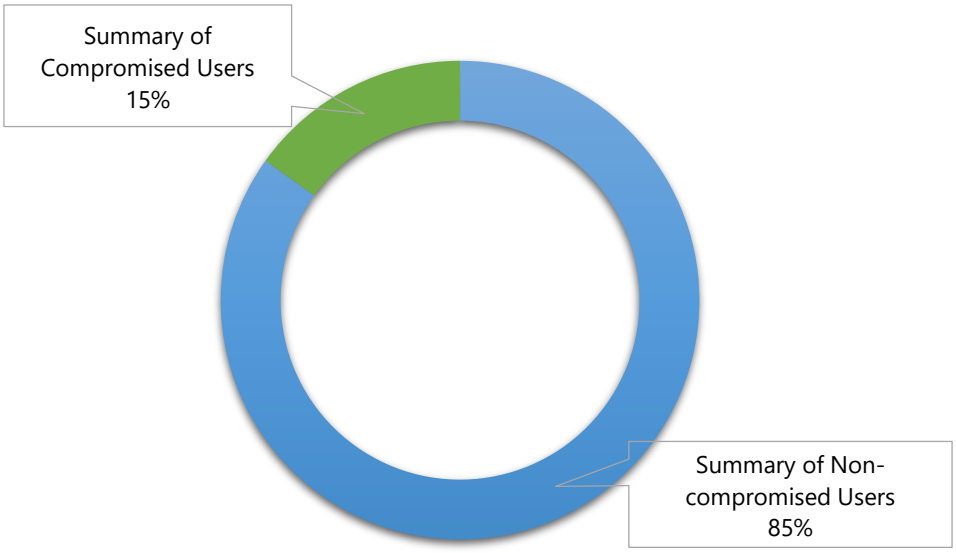


Figure 15: Social Engineering Attack Results

3.5.3 Commentary

As it can be observed from the chart above, a 15% of the users of an organization is prone to provide their credentials as a result of a social engineering attack. This number is considered high, taking into account that these users are providing real and active credentials that provide access to corporate applications.

4 Conclusions

The abovementioned findings analysis provides an initial insight to assessing the vulnerability state of Greek organizations. During our analysis we discovered that – on average – it is a matter of three (3) days for a skillful adversary to discover (and exploit) a critical vulnerability, thus gaining a foothold into the corporate network.

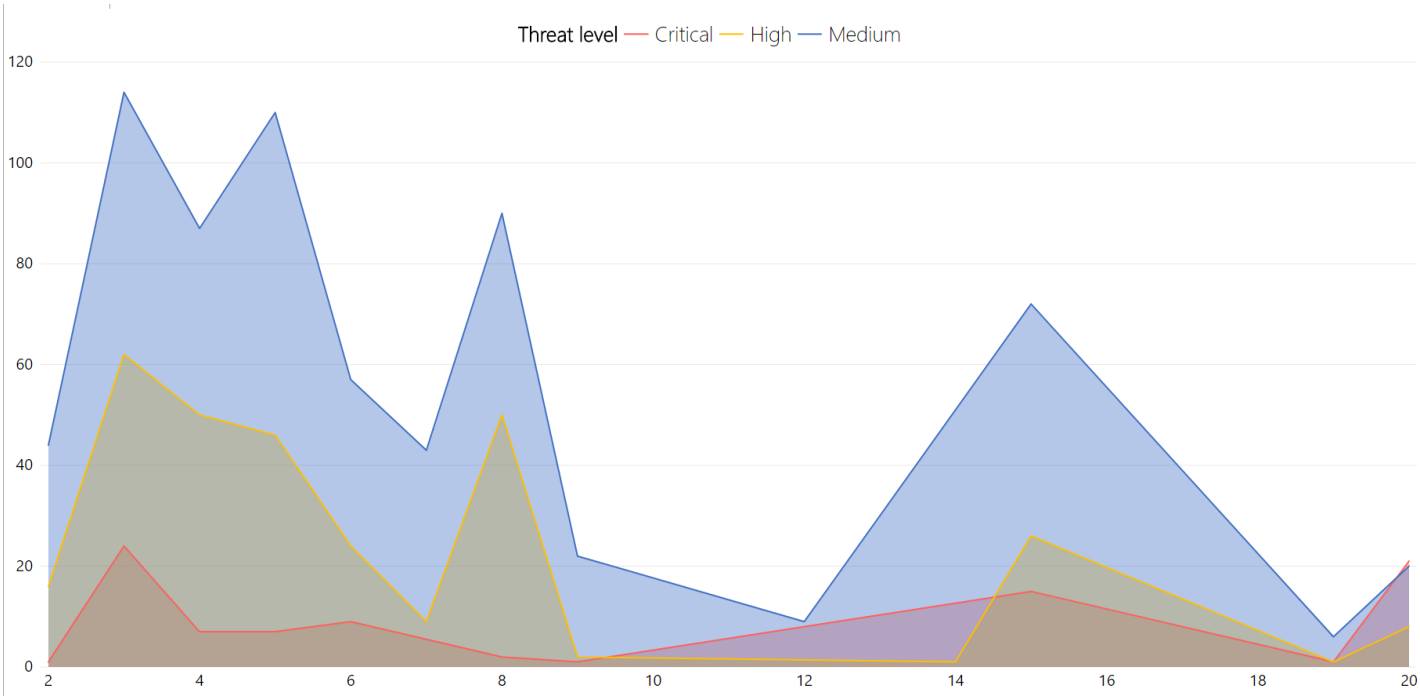


Figure 16: Findings per assessment duration and threat level

It is also worth noting that, after this period (and once an adversary is already in), the adversary can further exploit additional vulnerabilities.

In many occasions, adversaries were capable of exploiting vulnerabilities for a period of 20 days without being noticed. Furthermore, in two occasions, our team was second, discovering that someone else (perhaps an adversary) has already broke in, as evident by unauthorized programs and tools installed in systems and by observing abnormal system and application states.

The Top Threats (per count) discovered in Greek organizations, regardless of the type of assessment, indicate known issues to the security community. That is not to say that, if these threats were eliminated, then the Greek organizations would be immune to cyber threats; this means that organizations should place focus on practicing due care to their systems and applications, along with enforcing additional security controls to further strengthen their security posture. Additionally, this Top Threats list indicates that an adversary can identify and potentially exploit vulnerabilities without deploying extremely sophisticated methods and tools.

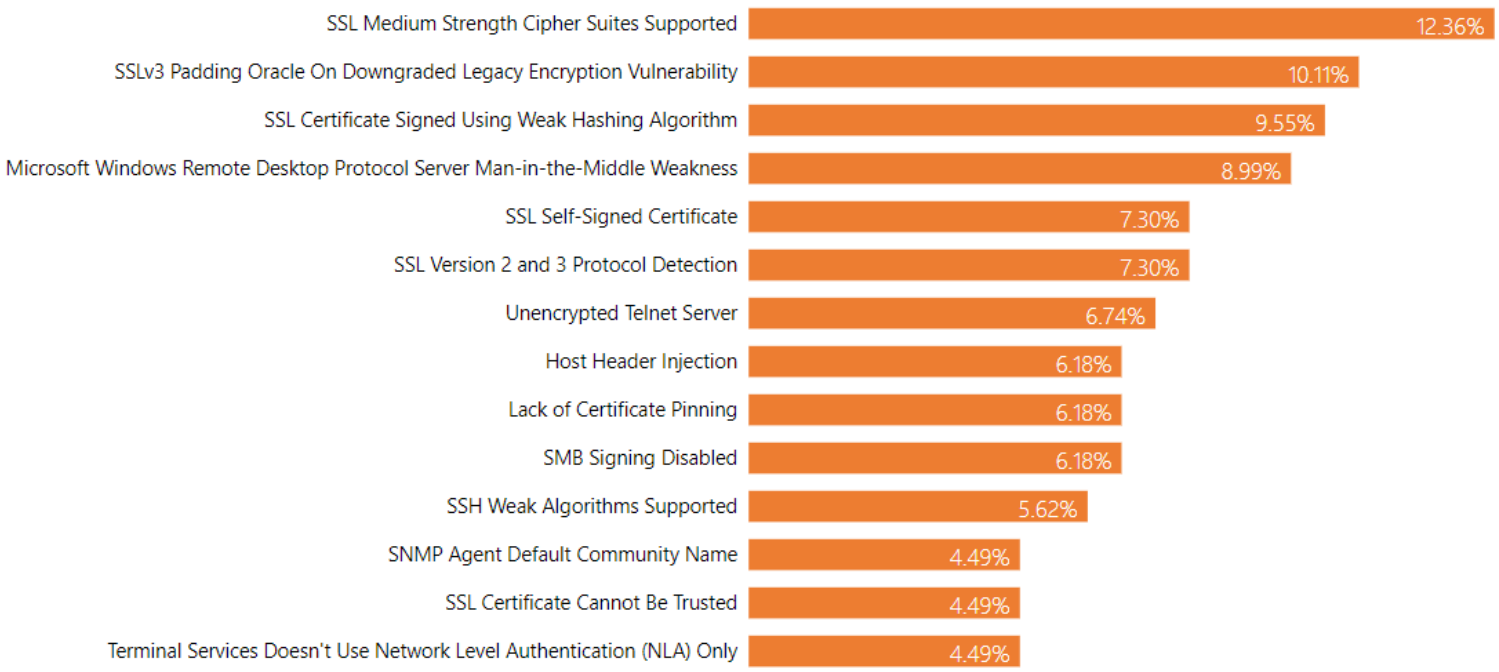


Figure 17: Top Threats (overall) in Greek Organizations (per count)

Finally, a list of additional controls that Greek organizations could deploy to strengthen their security posture and provide defense in depth, can possibly include the following:

- Establish security baselines, to provide a minimum set of security controls to enterprise systems, measure and improve these baselines;
- Replace insecure protocols like Telnet and SSL with secure protocols like SSH and TLS respectively;
- Develop a digital certificate management system, to manage weak ciphers, expired certificates, or certificates that support older versions of security protocols;
- Deploy a privileged account monitoring mechanism, to investigate abnormal privileged use of systems;
- Deploy an advanced Endpoint Detection and Response mechanism, to identify signs of intrusion to endpoints (since the majority of network traffic is encrypted, therefore network monitoring tools are limited in capability), as well as lateral movement;
- Consider a data leakage prevention solution, to defend against unauthorized exfiltration of corporate data;
- Consider encryption for data considered as "crown jewels";
- Develop a security awareness program to defend against social engineering attacks.

Greece
25 Kreontos St., 104 42 Athens
Tel: +30 210 51 93 740

Cyprus
7 Florinis Str. Greg Tower 2nd Floor 1065 Nicosia
Tel: +357 99318516

United Kingdom
88 Wood St., Barbican EC2V 7RS, London
Tel: +44 (0) 203 126 4590

Serbia
Omladinskih Brigada 90v, 11070 Airport City, Belgrade
Tel : +381 11 3219425