# Malware hash cloud

**Ferreira, Paulo[1]; Gonçalo, Rui[2]; Pedrosa, Tiago[3]**

[1] a34960@alunos.ipb.pt, Instituto Politécnico de Bragança, Portugal
[2] a35937@alunos.ipb.pt, Instituto Politécnico de Bragança, Portugal
[3] pedrosa@ipb.pt, Instituto Politécnico de Bragança, Portugal

## Resumo

Atualmente, qualquer sistema na internet pode ser alvo de um ataque informático. Uma parte considerável desses ataques, incluindo a instalação de malware, contém determinados indicadores, designados por IOCs (Indicators of Compromise) que podem ser usados para detectar o mesmo ataque em outros sistemas (e.g., hash de um ficheiro malicioso). O objetivo deste trabalho foi construir uma solução responsável pela recolha e análise dos IOCs.

Numa primeira fase desta solução procedeu-se à pesquisa e recolha de fontes de informação abertas (OSINT - Open Source Intelligence), contendo IOCs relativos a malware, bem como os próprios malwares. Esta informação, por sua vez, foi submetida numa plataforma de gestão e análise designada por Viper, que facilita a organização da informação em vários aspectos cruciais para a uma investigação nesta área da cibersegurança.

Numa segunda fase, foram desenvolvidos módulos adicionais, designados por bots, usando a plataforma IntelMQ (responsável pela automatização do processo de correlação da informação). Estes bots permitiram recolher e correlacionar a informação previamente recolhida pelo Viper, com plataformas online (acesso via APIs) que possuem informações adicionais, como por exemplo, a data de criação de um domínio malicioso disponível no serviço Whois.

Por fim, toda a informação recolhida a partir de um IOC durante todo o processo é armazenada numa base de dados que serve como ponto central para a geração de blacklists que podem ser aplicadas nos sistemas de protecção de perímetro (e.g. firewall) de uma organização, bem como para o suporte na análise de incidentes de segurança.

**Palavras-Chave:** ioc; osint; malware; cyber-security; infosec.

# Malware hash cloud

**Ferreira, Paulo[1]; Gonçalo, Rui[2]; Pedrosa, Tiago[3]**

[1] a34960@alunos.ipb.pt, Instituto Politécnico de Bragança, Portugal
[2] a35937@alunos.ipb.pt, Instituto Politécnico de Bragança, Portugal
[3] pedrosa@ipb.pt, Instituto Politécnico de Bragança, Portugal

## Abstract

Nowadays, any system on the internet can be a target of cyber-attacks. Many of these attacks, including malware installation, have some specific indicators designated IOCs (Indicators of Compromise) that can be used to detect the same attack on other systems (e.g., hash of a malicious file). The objective of this project is to build a solution that collects and analyse these IOC's.

The first stage of the solution was to research and collect open sources of information (OSINT - Open Source Intelligence), with IOCs related to malware, and also the malware itself. This information was submitted, in turn, to a management and analysis framework designated by Viper, which allows better organization of the information about crucial aspects in a cyber-security research program.

In a second phase, some additional modules, designated by bots, were developed, using the IntelMQ platform (responsible for the automatization of the correlation of the information)". These bots allow us to collect and correlate the information previously collected in Viper, with online platforms (via API access) that have additional information, like the creation date of a malicious domain available in Whois service.

Finally, all the information collected from a IOC during the process is stored in a database that is a central point for blacklists generation, that can be used for perimeter protection (e.g. firewall) of an organization, and also for the support in security incident analysis.

**Keywords:** ioc; osint; malware; cyber-security; infosec.