Hello and thank you for allowing me to present you the Malicious Website Identification tool also known as Knight Cast.

The Malicious Website Identification tool was born due to the current increase in malicious websites linked to campaigns against Users and Companies, originally simply to automatically report those websites, and lately updated to a smarter and more proactive tool.

Malicious websites are seen on the rise through the use of phishing e-mails, and are used for different attacks, like Data harvesting of personal information And Targeted attacks to gain access to Users’ data

These websites are perfectly created to scam the victims, and steal information.

The attacker spoofs a well-known organization's domain name, then creates a fraudulent website that looks like the real deal, replicating the real website's design. They will then send emails with the spoofed domain; making it appear as if the victim is receiving an email from a legitimate company.

On the fake website the attacker might’ve added a malware, a spyware, or a form to collect victim’s data and credentials, that can be then used against the victim or for other illegal purposes.

Domain names are unique, so the phisher can only mimic the organization's address. They do so by using character substitution like 'r' and 'n' together for 'rn' instead of 'm', or by creating domains that look like the original one, in the hopes that the victim would fall for it.

This not only ruins people's lives but damages the Companies' image.

Scammers and fraudsters are getting faster at creating these types of malicious websites, using toolkits and templates that are widely available on the web, or simply by copying the HTML of the website and adding their own code.

These problems require a proactive approach to prevent any further damage, and to block them from happen completely.

Knight|Cast is an innovative project that builds upon the foundation of the BEP project.

Most of BEP systems are ‘reactive’, meaning that they require an alert to be generated to which the user can react to a potentially malicious website; Knight|Cast works on a proactive solution.

It automatically recognizes malicious websites from a list of newly registered ones based on keywords, triggered by the User, or triggered by notifications of possible threats, and through the validation of the domain and its content, and through cross-reference with Data Platform, it will automatically recognize its threat level and report it to the User.

Of course, final reports can be automated, in the sense of reports of threats being sent directly to the abuse email, or to Clients; this can be decided later with the team.

Using an algorithmics approach, through QUAD9 and VirusTotal databases, and through website analysis, and Data Platform cross-reference, Knight Cast can automatically identify the threat level within few minutes and send out the threat notification.

Let me show you an example.

\*\* PLAY VIDEO \*\*

I’ve executed the tool last Friday using the “DHL” keyword, as you can see from this video Knight Cast found different domains that include or are close to the keyword searched.

You can see the information that Knight Cast has retrieved from whois queries, and the queries against the VirusTotal and Quad9 databases.

The website used in this example is dhl-postal.com, this website was created the 28th of March and as you can see it’s clearly a clone of the DHL website.

This website requires the user to fill up the form adding private information including name, surname, address, credit card info, and more. In this case the form doesn’t have any data validation, so it allows anything to be written in, but more advanced ones have data validation, making them look even more real. Once that information is added and the payment button is clicked, the website shows a fake loading screen and after few seconds it redirects the user to the real DHL website. To an untrained eye it might seem a legit website, and few people might fall for this, losing their information and maybe even their money, although as all of us know this is a phishing website, created to steal user’s information, that at the same time ruins the trust the user has in DHL.

I have showed you a video because the website has been removed after I’ve reported it last Friday night.

Here you can see the whois records of the domain taken on Friday when it was discovered, as you can see there are clear information of the registrar, although it’s clearly false data, only the email is real and already appears in different threat reports on the web, and here you can see the current whois report and the threat detection from multiple known websites after the domain was reported.

Knight Cast will not only help to address new threats but used with the Data Platform and cross-referencing new domains and possible registrar info with our database, we will be able to report newly generated threats and block them before they could possibly generate problems or steal information, all in a matter of minutes.

By implementing Knight Cast we will save more than 45% of the time our current teams are using to identify malicious websites, and once we’ll build the trust in the tool, we can potentially save more than 65% of the time with automated reports, removing the manual overhead almost completely, but still giving the users the possibility to review reports.

Currently Knight Cast is not at 100% capability, the code needs to be updated for more robust web scraping and for the cross-reference with Data Platform, the latter can be completed later, and at the moment the tool using the free version of VirusTotal API, limiting the info that can be found.

By purchasing the professional license, we will be able to implement a more robust tool.

The public API for example is limited to 500 requests per day and a rate of 4 requests per minute, and cannot be used commercially, while the Premium API Allows to choose a request rate and daily quota allowance that best suits our needs. Enables to download submitted samples for further research, along with the network traffic captures they generate upon execution and their detailed execution reports.

Will return further details and context about the observables processed by VirusTotal, for instance: VBA code stream warnings for documents, source metadata, ExifTool output, IDS output for recorded network traces, domain popularity rankings, SSL certificates, etc.

Allows to perform reverse searches such as give me all samples that are detected with the following signature, give me all samples that are detected by more than 10 engines, etc. and allows to perform reverse searches such as give me all domains registered by the same attacker, give me all domains with a DNS A record TTL lower than 5 seconds, etc. these search modifiers can be combined to build complex requests.

The premium version starts at $10.000 a year and can go up depending on usage.