Top 10 per country	
Malware_Family_Name	**Description**
Nivdort	Nivdort is a Trojan family which targets the Windows platform. It gathers passwords and system information or settings such as the Windows version, IP address, software configuration and approximate location. Some versions of this malware collect keystrokes and modify DNS settings. Nivdort deploys its files in the Windows system files folder. The malware is spread via spam mail attachments or malicious websites.
Cryptowall	Cryptowall is a major ransomware Trojan which encrypts files on an infected machine and then asks users to pay for them to be decrypted. It spreads through malvertising and phishing campaigns. Cryptowall first appeared in 2014. There are four major versions, with the most recent iteration surfacing in the fall of 2015.
Nemucod	A malware dropper that once executed pulls a designated instance of malware from an online server, and then runs it on the infected machine. Nemucod has been in the business of dropping malware since at least late 2015, and possibly earlier. Its distribution vector has stayed constant throughout: Spam messages informing people about owed fines, failed payments, held baggage and various other mishaps that require the victim's immediate attention. Nemucod has been known to infect victims with various kinds of malware (such as TeslaCrypt ransomware) and adware (such as Boaxxe click-fraud).
Kelihos	The Kelihos botnet (aka Hlux) is a peer-to-peer botnet mainly involved in the theft of Bitcoins, Bitcoin mining and sending spam. It is spread by sending spam emails that have links to other malware. The botnet can also communicate with other PCs to exchange information about sending spam emails, steal sensitive information, or download and run malicious files. Later versions mostly propagate over social network sites, particularly Facebook.
Cerber	Cerber, also known as Zerber, which was first introduced in February 2016, is an offline ransomware, meaning that it does not need to communicate with its C2 server before encrypting files on an infected machine. It is spread mostly via malvertising campaigns which leverage exploit kits, but also through spam campaigns. The threat actors behind Cerber ask for a 1-bitcoin ransom for decrypting one's files, and according to some reports. Its business model is ransomware as-a-service, meaning that the author recruits affiliates to spread the malware for a share of the ransom payment.
Matsnu	Matsnu is a backdoor used to download and execute files or other code on an infected system. It can also encrypt files on the machine for ransom. When installed, Matsnu modifies the registry to run it after every Windows start and also

Pdf créé avec la version d'essai pdfFactory www.pdffactory.com

Top 10 per country	
Malware_Family_Name	**Description**
	adds itself to the authorized application list to enable its communication to bypass the firewall. It has anti-sandbox capabilities, such as checking if the strings "sand" or "-box" appear in its own file name before running. It also disables the registry editor and task manager, as well as the user's ability to start Windows in safe mode. Matsnu's communication with its Command and Control (C&C) servers is done using Domain Generation Algorithm (DGA), which generates a new domain name every predefined amount of time, thus making it more difficult to block its communication.
Peg	
Conficker	Conficker is a computer worm that targets the Windows OS. It exploits vulnerabilities in the OS and uses dictionary attacks on the admin passwords to enable propagation while forming a botnet. This infection allows an attacker to access users' personal data such as banking information, credit card numbers, or passwords. The worm originally targeted users of networking websites such as Facebook, Skype and email websites.
HackerDefender	HackerDefender is a rootkit for Windows 2000 and Windows XP, and may also work on later Windows NT based systems. The rootkit modifies several Windows and native API functions to remain undetected by security softwares. HackerDefender is widely deployed in the wild as it is publically available online and is easy to install.
RookieUA	RookieUA is an Info Stealer designed to extract user account information such as logins and passwords and send them to a remote server. The HTTP communication is done using an uncommon User Agent called RookIE/1.0.
Necurs	Botnet used to spread malware by spam emails, mainly Ransomware and Banking Trojans.

Pdf créé avec la version d'essai pdfFactory www.pdffactory.com