Top 10 per country	
Malware_Family_Name	**Description**
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 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.
Slammer	Memory resident worm targeted to attack Microsoft SQL 2000. By propagating rapidly, the worm can cause a denial of service condition on affected targets.
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.
Rig ek	Rig EK was first introduced in April 2014. It has since received several large updates and continues to be active to this day. In 2015, as result of an internal feud between its operators, the source code was leaked and has been thoroughly investigated by researchers. Rig delivers Exploits for Flash, Java, Silverlight and Internet Explorer. The infection chain starts with a redirection to a landing page that contains JavaScript that checks for vulnerable plug-ins and delivers the exploit.
Peg	
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.
Necurs	Necurs is a one of the largest botnet currently active in the wild, and it is estimated that on 2016 it consisted of some 6 million bots. The botnet is used to distribute many malware variants, mostly banking trojans and ransomware. Necurs botnet is usually spreading malware based on massive spam campaigns, with zip attachments containing malicious JavaScript code. On June 2016 the botnet mysteriously ceased operations for nearly

Top 10 per country	
Malware_Family_Name	**Description**
	a month, possibly due to a fault in its C&C function. Necurs is known as a prime distributor of Locky ransomware, one of the most prominent ransomware families of 2016, and Dridex, a sophisticated banking trojan responsible for the theft of millions of dollars from victims based mainly in the United Kingdom and the United States.
Business	A malicious program that targets the Windows platform and simulates the activity of AntiVirus software or operating system security modules.
Zeus	Zeus is a widely distributed Windows Trojan which is mostly used to steal banking information. When a machine is compromised, the malware sends information such as the account credentials to the attackers using a chain of C&C servers. The Trojan is also used to distribute ransomware. Zeus was first identified in July 2007 when it was used to steal information from the United States Department of Transportation. Over the next few years the malware compromised hundreds of thousands of machines, becoming one of the world's largest botnets. The malware was distributed mostly by email, using phishing attacks. In October 2010 the FBI arrested more than one hundred people on charges of conspiracy to commit bank fraud and money laundering, including the suspected master mind behind the botnet - Hamza Bendelladj, who was arrested in 2013. Currently, many cybercriminals use custom Zeus variants, which are typically spread via phishing and drive-by downloads.
Adwind	Adwind is a Backdoor that targets systems supporting the Java runtime environment. This malware sends out system information and accept commands from a remote attacker. Commands can be used to display messages on the system, open URLs, update the malware, download/execute files, and download/load plugins, among other actions. Downloadable plugins for the malware can provide considerable additional functionality including remote control options and shell command execution.
Ramnit	Ramnit is a worm that infects and spreads mostly through removable drives and files uploaded to public FTP services. The malware creates a copy of itself to infect removable and permanent drivers. The malware also functions as a backdoor, allowing the attacker to connect to the infected machine and communicating via C&C servers. The first variant, discovered in 2010, didn't have many capabilities beyond a basic ability to integrate itself into an infected machine. In 2011 it was modified by malicious actors to have the ability to steal web session information, giving the worm operators the ability to steal account credentials for all services used by the victim, including bank accounts, corporate and social networks accounts.