Cybercrime: an Internet By-product

Although hacking, identity theft and cybercrime in general have been around for years, with so many more people today being connected to each other and their personal information being stored on cloud servers, it was a logical expectation that cybercrime would be on the rise. In prior articles we have written about identity theft, viruses and hacking – things that can affect everyone at some time. But technological developments produce both good and bad results – depending on who's using it.

The term "Botnet" came into prominence when one nicknamed "Citadel" used **5 MILLION** computers to infect and steal information from normal individuals –a loss of half a billion dollars in 18 months. This "Botnet", operated by an Eastern European cybercriminal, constituted a network of zombie computers that recorded keystrokes, captured login passwords and personal ID numbers, spied on financial information, and logged people's most sensitive and personal information. These "zombies" reported back to their heads a person's mother's maiden name, where they banked and what password was used for several accounts. Next they were able to log into victims' favorite websites, steal their

savings, credit card numbers and even their identity by using personal data. The spread of the botnet army was rapid and produced costly results to innocent people.

In response, tech giants have collaborated with the FBI, Interpol and other policing agencies to combat this global threat. Microsoft, on whom the majority of the world's systems are based, has already set up its impressive Digital Crimes Unit….the CSI division of the tech world. Using its Cloud technology, imaging capabilities and tracking systems, Microsoft has launched a global initiative to cross all borders and surpass political boundaries to protect internet users. The forensics lab can detect via Microsoft's unique activation codes, in speeding time-lapse, where and when each zombie comes online and thus develop an accurate geographical map of where each is located. These same investigators have already discovered that **pirated and illegal software owners are more vulnerable to being affected by botnets** by the malware they emit. Microsoft's Cybercrime Center in Redmond, Washington is testament to their commitment to keep their customers safe from these types of intrusion, and a major reason why Windows 10 is to date the safest operating system they have produced.

This state-of-the-art lab is where a seasoned group of cybercrime investigators try to stay a couple of moves ahead of the world's Internet criminals in an effort to make the web a safer place. So love them or not, Microsoft is out to make money but recognizes that to keep their customers loyal, they need to protect them too.