Different Hats on Hackers

Posted At : April 29, 2015 11:10 AM | Posted By : Admin
Related Categories: Security

Editor's Note: Hacking of computer systems sometimes appears to be a recent phenomenon. Back in the very early days of the Internet in 1988, a Cornell graduate student, Robert Tappen Morse created one of the first computer worms. It landed him in hot water and ultimately the first to be convicted under the comptuer fraud and abuse act. He eventually became a professor of computer science at MIT.

Today, there are different types of hackers exploiting vulnerabilities in computer systems and networks. This article discusses the differences among black hat, white hat and grey hat hackers..

Not all hackers are inherently bad. When used in mainstream media, the word, “hacker,” is usually used in relation to cyber criminals, but a hacker can actually be anyone, regardless of their intentions, who utilizes their knowledge of computer software and hardware to break down and bypass security measures on a computer, device or network. Hacking itself is not an illegal activity unless the hacker is compromising a system without the owner’s permission. Many companies and government agencies actually employ hackers to help them secure their systems.

Hackers are generally categorized by type of metaphorical “hat” they don: “white hat”, “grey hat”, and “black hat”. The terms come from old spaghetti westerns, where the bad guy wears a black cowboy hat, and the good guy wears a white hat. There are two main factors that determine the type of hacker you’re dealing with: their motivations, and whether or not they are breaking the law.

Black Hat Hackers

Like all hackers, black hat hackers usually have extensive knowledge about breaking into computer networks and bypassing security protocols. They are also responsible for writing malware, which is a method used to gain access to these systems.

Their primary motivation is usually for personal or financial gain, but they can also be involved in cyber espionage, protest or perhaps are just addicted to the thrill of cybercrime. Black hat hackers can range from amateurs getting their feet wet by spreading malware, to experienced hackers that aim to steal data, specifically financial information, personal information and login credentials. Not only do black hat hackers seek to steal data, they also seek to modify or destroy data as well.

White Hat Hackers

White hat hackers choose to use their powers for good rather than evil. Also known as “ethical hackers,” white hat hackers can sometimes be paid employees or contractors working for companies as security

specialists that attempt to find security holes via hacking.

White hat hackers employ the same methods of hacking as black hats, with one exception- they do it with permission from the owner of the system first, which makes the process completely legal. White hat hackers perform penetration testing, test in-place security systems and perform vulnerability assessments for companies. There are even courses, training, conferences and certifications for ethical hacking.

Grey Hat Hackers

As in life, there are grey areas that are neither black nor white. Grey hat hackers are a blend of both black hat and white hat activities. Often, grey hat hackers will look for vulnerabilities in a system without the owner's permission or knowledge. If issues are found, they will report them to the owner, sometimes requesting a small fee to fix the issue. If the owner does not respond or comply, then sometimes the hackers will post the newly found exploit online for the world to see.

These types of hackers are not inherently malicious with their intentions; they're just looking to get something out of their discoveries for themselves. Usually, grey hat hackers will not exploit the found vulnerabilities. However, this type of hacking is still considered illegal because the hacker did not receive permission from the owner prior to attempting to attack the system.

Although the word hacker tends to evoke negative connotations when referred to, it is important to remember that all hackers are not created equal. If we didn't have white hat hackers diligently seeking out threats and vulnerabilities before the black hats can find them, then there would probably be a lot more activity involving cybercriminals exploiting vulnerabilities and collecting sensitive data than there is now.