# Microsoft has a group of 'elite' hackers that specialize in attacking Windows to keep the operating system safe

Their mission is to attack to find security holes on Windows, report to Microsoft to research and release patches before the crook takes advantage of them for bad purposes.

Microsoft owns an elite "red team" hacker to help keep Windows safe. Their mission is to attack to find security holes on Windows, report to Microsoft to research and release patches before the crook takes advantage of them for bad purposes.

"Red Team" - Red Team is the term for white-hat hacker groups to take on the attack to find security holes and help patch up in time.

Windows accounts for 90% of the market share of Laptop operating systems and desktop computers worldwide so it is certain that the safety protection will be at the top because the world will suffer extremely heavy consequences if Windows crashes. to dump.

Previously, Microsoft protected the Windows operating system by waiting for a large-scale attack to occur or waiting for someone to reveal to them a new attack technique, then embarked on research to fix it. This protection is very dangerous, the risk of the world's most popular operating system being knocked down is very high.

**Rally**

Therefore, 4 years ago David Weston - who is currently in charge of managing security groups at Windows, wants Microsoft to change the way it handles security issues for its products, especially Windows. . He wanted to proactively find out possible Windows errors, not passively respond to problems and vulnerabilities after they were found.

Weston embarked on a search for talent and set up an attack team on Windows to find vulnerabilities and fix them.

Members of the elite "red team" hackers of Microsoft include:

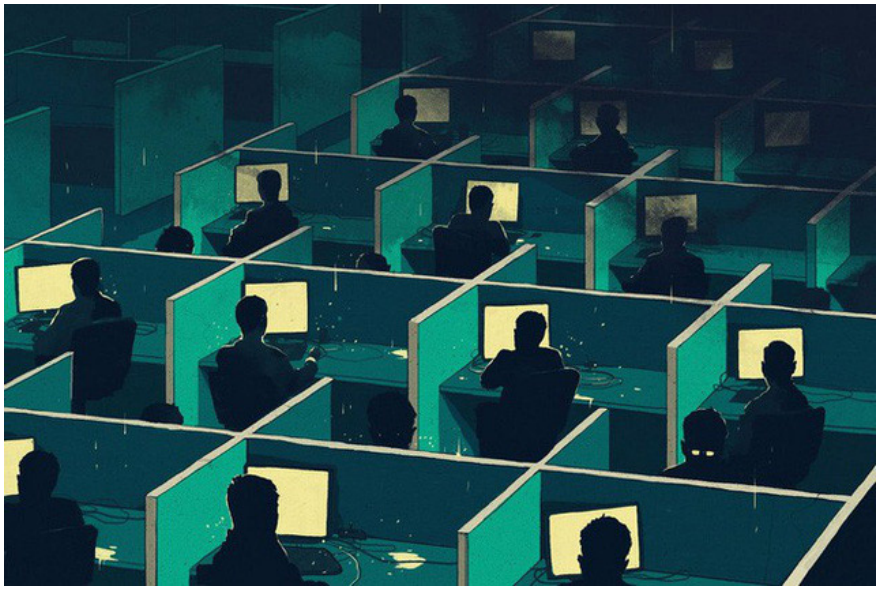
Jordan Rabet, a browser security expert for Microsoft, was invited to join the "red team" after launching a Nintendo 3DS unlocking video on YouTube in 2014. This guy also contributed greatly to help Microsoft. could quickly release a temporary patch in the Specter vulnerability.

Viktor Brange, who lives in Sweden, analyzes the operating system's native code and makes an assessment of the severity of his vulnerabilities that has contributed significantly to preventing the leak of hacking tools. Eternal Blue of NSA.

Adam Zabrocki, an important member of the red team, has lots of experience with the Linux operating system.

Jasika Bawa, who turns red team's findings into practical improvements makes Windows more secure.

In addition, the Red team of Microsoft also has two other members, but due to the more sensitive nature of the work, they decided to remain anonymous.



Each year, the red team (such as the sword) will develop a zero-day vulnerability to challenge the defensive capabilities of the blue team - as a shield, this is the Microsoft operating system protection team.

Every day, every month, every year they keep honing each other like that. And they will be the first to be called every time Microsoft's operating system has an urgent problem.

**Red code**

In fact, most major technology companies and corporations have one or more of their own red teams. Before the red team for Windows was founded, Microsoft had many "red" teams running but they only focused on problems during operation.

Redon's red team with Weston's attack on Windows has brought a lot of benefits to Microsoft, even to the computer industry. They not only helped overcome the problem that Specter and EternalBlue caused, but the army also discovered many more about security.

One of their most outstanding victories was to successfully prevent a series of phishing attacks performed by the Fancy Bear hackers. They used the attack method called Strontium, which targeted Win32k - a Windows kernel driver that was often exploited by hackers.

**Time**

The work of Red Team members does not have a fixed target and does not set a goal to fix all errors. The error will always exist and prioritize their work based on the trend of hackers and new features that are tested or easy to target.

Every time the work is done, the red team starts to press the time to have a relative view of the time needed to hack something. Hackers will be less interested in time-consuming and costly attacks.

However, attacks are their main job, not patches, so at times they are not happy with Microsoft. Mostly, it is time to overcome serious vulnerabilities that last for too long.

Windows will always be a target for top priority hackers, and Weston's red team is just a puzzle piece for Microsoft 's attempt to secure operating system security. However, considering that there are a lot of professional hackers, even sponsored by underground criminal organizations, we should probably feel lucky to know that there is at least one army in Redmond. are constantly protecting the operating system that we still use from the hands of the bad guys - even, surpassing them one step.

See more:

1. The way Hacker uses to remain anonymous
2. The story of "double bearer" Sabu: Anonymous traitor, the hero of the FBI
3. The white "monster master" hat hackers