Notorious botnet TrickBot stopped working, redirected to another form of malicious code that could be more dangerous

TrickBot, one of the most active and damaging botnets ever recorded worldwide.

TrickBot, one of the most active and most damaging botnets ever recorded worldwide, was shut down after key developers switched to the Conti ransomware gang. This is believed to be the necessary move for them to focus their development on the stealthy malware families BazarBackdoor and Anchor which are also extremely dangerous.

TrickBot is a notorious malware on Windows. Since it was first discovered in 2016, this malicious code has always held a strong position in the list of the most dangerous and damaging malware strains. TrickBot's main method of spreading is via phishing, malicious email or other software. Therefore, the objects most affected by this malicious code are usually organizations and businesses.

Trickbot is not a simple piece of malware that can be detected by any free anti-virus software. It is dangerous in that it is constantly evolving and effectively hiding within the infected device.

After spreading and silently running on the victim's computer, the malicious code will download various modules on its own to conduct data theft and bad behavior. TrickBot is often distributed through spam emails containing malicious links or files. Once installed, this malicious code will secretly run on the victim's computer, downloading other components to serve various malicious purposes.

These modules help the malware perform a wide range of malicious activities, including stealing the domain's Active Directory Services database, spreading it horizontally across the network, locking the screen, and stealing cookies and passwords. browser, as well as stealing OpenSSH keys.

TrickBot also has a long association with ransomware activities. In 2019, TrickBot Group partnered with the Ryuk ransomware gang to provide initial access for this ransomware to networks. In 2020, the Conti ransomware group, which is said to be Ryuk's new brand, also partnered with TrickBot for the same purpose.

Despite the efforts of global law enforcement agencies, TrickBot has successfully rebuilt its botnet and continues to terrorize Windows users.

In 2021, TrickBot tried to launch its own ransomware operation called Diavol, but without success. This can be an important reason why the operations team made the decision to transform the operating model.

TrickBot stopped working

Over the past year, Conti has become one of the most versatile and profitable ransomware operations, responsible for numerous attacks on well-known victims and hundreds of millions of dollars in ransoms.

TrickBot is mainly used by Conti, the ransomware gang that has slowly taken control of the botnet's operations. However, Conti did not recruit these "elite developers and managers" to take over TrickBot, but rather to work on the BazarBackdoor and Anchor malware strains with even better stealth capabilities. .

According to experts, this change is inevitable because TrickBot is now too easily detected by popular security software. TrickBot Group has now closed all infrastructure for the operation of this malware.

In general, TrickBot's shutdown does not make much sense in terms of network security, because its attackers are essentially just moving on to develop another more dangerous strain of malicious code.

BazarBackdoor has increased its email distribution over the past 6 months, but with TrickBot shutting down, we are likely to see it become more common in breaches targeting corporate networks. Global.