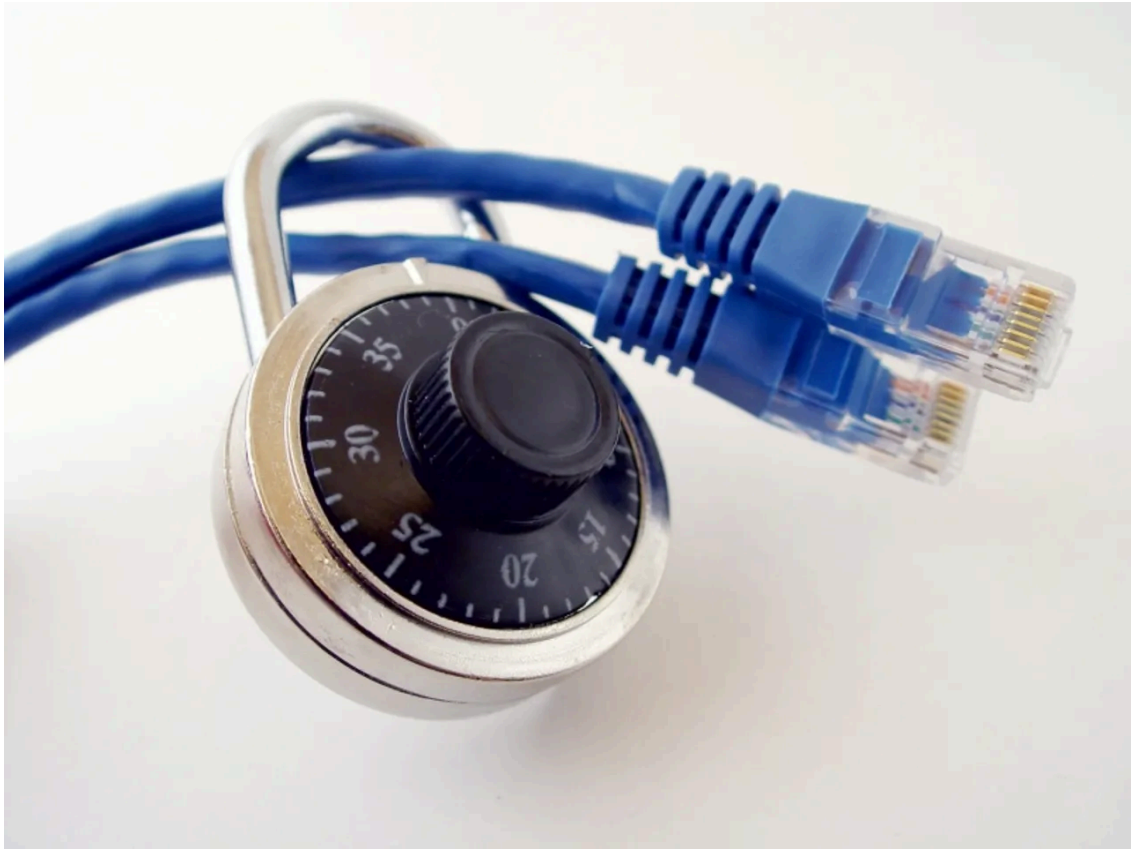
FireEye, Microsoft wipe TechNet clean of malware hidden by hackers

By Written by

Archived: 2026-04-05 16:56:51 UTC



FireEye and Microsoft have moved against Chinese hackers taking advantage of the TechNet forum to spread malware.

According to a new report released by cybersecurity firm FireEye, in late 2014, FireEye Threat Intelligence and the Microsoft Threat Intelligence Center discovered a command-and-control (C&C) obfuscation code hidden within Microsoft's TechNet web portal. A Chinese group dubbed APT17 -- also known as Deputy Dog -- used the TechNet forum in order to hide the C&C code, making it more difficult for security professionals to locate the true source of the attack infrastructure.

China tightens military control in fresh censorship wave

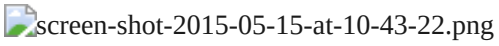
The researchers say Deputy Dog created profiles and posts in TechNet which embedded the encoded C&C for use with a variant of the BLACKCOFFEE malware, malicious code used in cyberespionage campaigns.

Comments left on particular pages contained the names of encoded domains, which systems infected with BLACKCOFFEE were forced to contact, as reported by IDG. The victim computer was then directed to the C&C server controlled by Deputy Dog. In other words, TechNet -- while not compromised itself -- became a go-between used to disguise the true address of the C&C.

As TechNet supports a vast amount of traffic and hosts an open forum where Microsoft software customers can ask and respond to questions, the platform was an excellent conduit for hiding hacking activities.

"This technique can make it difficult for network security professionals to determine the true location of the CnC, and allow the CnC infrastructure to remain active for a longer period of time," FireEye said.

"TechNet's security was in no way compromised by this tactic."



Deputy Dog is a well-known Chinese hacking group which has launched attacks against tech firms, mining companies, defense contractors, law firms and US government agencies. The group has also been linked to attacks on Japanese targets.

"By injecting encoded data onto some of the TechNet pages, the FireEye-Microsoft team was able to gain insight into the malware and the victims," FireEye explained. "Though the security community has not yet broadly discussed this technique, FireEye has observed other threat groups adopting these measures and expect this trend to continue on other community sites."

On Thursday, FireEye released Indicators of Compromise (IOCs) for BLACKCOFFEE and Microsoft released updated signatures for its anti-malware security products.

Read on: In the world of security

- Yahoo launches password-free logins
- Feds hot on the trail of JPMorgan hackers
- EquationDrug: Sophisticated, stealthy data theft for over a decade
- Symantec research highlights security failures in the connected home
- New CryptoLocker ransomware targets gamers

Editorial standards