Hacker Attacks on Microsoft Teams Threaten Business Collaboration

According to Microsoft, 270 million people worldwide actively use Microsoft Teams. More than just a messaging app, Teams provides an essential hub for connecting workers and driving efficiency. As such, it presents an increasingly attractive target for bad actors, and security groups have noticed a sharp rise in hacker attacks on Microsoft Teams.

Beginning in January 2022, bad actors posing as coworkers started inserting seemingly legitimate files into Teams chats. But when a user clicks the file, usually named UserCentric.exe, it installs DLL files and modifies the Windows registry. This opens the door for hackers to take over the computer remotely.

Business Email Compromise (BEC) Evolves

In these attacks on Microsoft Teams, hackers employ an evolved version of a business email compromise (BEC) attack. In a BEC scam, the attacker impersonates a trusted person, often a high-level executive, and tricks employees into taking harmful action. For instance, the employee may receive an email from the CEO instructing them to transfer money.

Threat actors have successfully used BEC scams through email for years. But now they have expanded their attacks. Instead of using just email, hackers have begun using stolen credentials to impersonate trusted employees in Teams chats. This broadens their attack surface and provides new inroads into the organization.

Hackers first compromise an employee's email account, often through a phishing campaign in a third-party organization. Then, using those stolen credentials, they can then access the Microsoft 365 environment and pose as a team member. In the recent attacks, they use that position of trust to trick coworkers into clicking on malicious files that install malware.

Exploiting End-user Trust of Popular Platform

Security awareness training has helped end users recognize the signs of a BEC scam through email. Unfortunately, however, users often fail to approach Teams with the same caution. Employees tend to trust the Teams environment, assuming that information shared in a Teams chat remains secure.

Additionally, while users may know to look carefully at a sender's email address to spot a fake, they do not always know how to recognize when someone has spoofed a Teams identity. They may interact with what appears to be a team member, not realizing they have received a file from a bad actor instead.

For instance, in a recent attack, hackers invited coworkers to a Teams meeting, posing as the CEO. Then, claiming a bad connection, they sent a SharePoint link through the chat. An employee, thinking the file contained important information about the meeting, clicked the link and activated a malicious file.

Multi-layer Security Counters Attacks on Microsoft Teams

As threat actors begin to launch more attacks on collaboration platforms like Teams, organizations need to update their security strategies. Default security tools in Teams do not provide enough protection on their own. Instead, companies need to take a multi-faceted approach.

To begin with, security awareness training needs to adapt to the new reality. Users need to learn to use more caution within Teams communications, double-checking the source of a file or request before clicking or responding.

Second, organizations cannot depend on the default security tools provided with Teams to provide adequate protection. Instead, they should implement comprehensive security measures that include protection for Teams communication. Those measures should include automatic inspection of all files shared through messaging to identify suspicious content.

eMazzanti Delivers Peace of Mind

The cybersecurity experts at eMazzanti Technologies stay abreast of emerging cyber-threats, as well as advancements in security technology. And with deep experience in Microsoft, our consultants will help your organization deploy a security solution designed for secure collaboration.