# New Phishing Campaign Abuses ConnectWise ScreenConnect to Take Ov

Data: 2025-08-29 06:38:18

Autor: Inteligência Against Invaders

A novel phishing campaign attempts to trick victims into downloading ConnectWise ScreenConnect remote monitoring and management (RMM) software, enabling attackers to take complete control over end-user devices.

A report by Abnormal AI found that the legitimate RMM tool is abused by the threat actors to achieve remote system control and facilitate follow-on attacks, including account takeovers and lateral phishing.

The researchers said the ongoing campaign represents a significant evolution in phishing tactics, which traditionally rely on victims giving up personal information such as credentials and financial details.

“The weaponization of a legitimate IT administration tool – one designed to grant IT professionals deep system access for troubleshooting and maintenance – combined with social engineering and convincing business impersonation creates a multi-layered deception that provides attackers with the dual advantage of trust exploitation and security evasion,” they wrote.

The campaign has so far targeted more than 900 organizations, impacting a broad range of sectors and geographies.

The use of ScreenConnect to support the campaign also demonstrates a more mature criminal ecosystem where dark web vendors operate like legitimate software providers, the researchers added.

“Cybercriminals can acquire ScreenConnect in numerous forms across forums, encrypted messaging apps and anonymous web pages,” they noted.

As well as focusing on deployment, some of these offerings are focused on resale. For example, vendors have been observed offering domain-admin level ScreenConnect access to networks in Germany, the UK and China, typically including control over 90–345 hosts.

*Read now: ConnectWise Confirms Hack, “Very Small Number” of Customers Affected*

## A Multi-Stage Attack Chain

The Abnormal AI report, published on August 26, observed that the multi-stage attack begins with a phishing email, which is designed to appear as routine business communications or friendly correspondence.

One commonly used lure is fake Zoom meeting invitations, using timely subject lines such as “Meeting Invite – 2024 Tax Organizer SID:80526353241,” tying in tax season relevance to make the message feel genuine.

The emails feature familiar branding and originate from compromised legitimate accounts to increase their credibility and avoid detection.

“In this particular instance, the attackers appear to have found a real Zoom notification email and modified only the call-to-action (CTA) to further enhance the illusion of authenticity,” the researchers noted.

In one case, the attackers hijacked an ongoing thread that already contained a genuine Zoom meeting invitation to insert a malicious link.

Other phishing lures involve invites to fake MS Teams calls.

Once a link is clicked, the target is redirected to a malicious site where the second stage of the attack is initiated.

This site prompts the user to download what appears to be an updated version of the relevant video conferencing platform. Instead, the file is the ScreenConnect RMM software.

Recipients whose organization already has ScreenConnect installed for legitimate purposes are immediately connected to a live ScreenConnect session controlled by the attackers. For targets without existing ScreenConnect installations, clicking these links triggers an automatic download prompt for the ScreenConnect client software.

“This technique exploits the fact that many organizations already have ScreenConnect installed for legitimate remote support purposes, allowing threat actors to bypass the installation process entirely,” the researchers said.

## Stealthy Post-Compromise Activity

Once downloaded, the threat actors are able to weaponize ScreenConnect’s intended functionality to achieve comprehensive system access equivalent to an IT administrator.

This allows for a wide range of post-compromise activities, including bypassing security controls, navigating file systems, achieving persistent access and exfiltrating sensitive data.

The attackers have also been observed pivoting to lateral phishing campaigns that leverage the compromised environment to compromise additional targets within the organization.

“They analyze communication patterns, identify high-value targets and craft phishing messages that appear to originate from trusted internal sources,” Abnormal AI wrote.

Many of these phishing emails ultimately aim for additional ScreenConnect deployments across the organization.

By sending phishing emails directly from the target’s account, they can bypass security controls that might flag external phishing attempts.

## How to Defend Against ScreenConnect Abuse

The Abnormal AI researchers urged organizations to take action to address growing abuse of legitimate RMM tools by threat actors.

This includes establishing comprehensive monitoring of these tools on the network, focusing on unauthorized installations and suspicious usage patterns.

Additionally, they advised organizations to updated training programs to make staff aware of legitimate software abuse, including during phishing attacks.

“This campaign serves as a critical reminder that modern threats increasingly weaponize trusted systems rather than circumvent them. As a result, defenders must fundamentally reconsider their approach to threat detection and response,” the researchers noted.

Abnormal AI told *Infosecurity* it has not had any communication with ConnectWise regarding the research.

*Infosecurity* has contacted ConnectWise for comment on the findings but has not received a response at the time of writing.