Malware delivered via Microsoft Teams

Malware Downloader delivered via Microsoft Teams

Background

Recently, Avanan released a blog post mentioning the interest of adversaries in Microsoft Teams as a launchpad for their malicious attacks. Attackers have always targeted online collaboration tools like Slack and Discord for malware distribution and phishing. While this is probably not the first time that teams have been used for infecting users, this trend has been on the rise with increasing popularity of Teams.

Campaign overview

Hackers are targeting Teams platform for sharing malicious trojan files at scale to infect unwitting users. They are using various means to get access to user's emails which in turn is used to get into Teams and subsequently share malicious files with more users to infect them. Files shared over Teams are executable files which can take control over the system.

Hackers get the added benefit of attacking over Teams or any other similar service if they use SSL encryption which can automatically bypass some security tools which are oblivious to things happening under SSL. Furthermore they are taking advantage of the trust between the compromised user and the target users as they are more likely to open the files coming from a known contact.

There is a **caveat,** Attackers can't just share files on teams, they must first get access to a Teams account to be able to share any files with other users.

What can you do to protect yourself?

- Route all traffic through Zscaler Internet Access, which will provide the right visibility to identify and stop malicious activity from compromised systems/servers.
- Ensure you are inspecting all SSL traffic.
- Advanced Threat Protection to block all known malware and command-and-control activity.

- Use Advanced Cloud Sandbox to prevent unknown malware delivered as part of a second stage payload.
- Security awareness training to spot and report suspicious attachments over chat and collaboration tools

Zscaler coverage:

Zscaler can protect against these or in fact any unknown threats by inspecting SSL encrypted traffic at scale and detonating files in Advanced Cloud Sandbox.

We have ensured coverage for the known payloads via advanced threat signatures as well as advanced cloud sandbox.

Malware protection

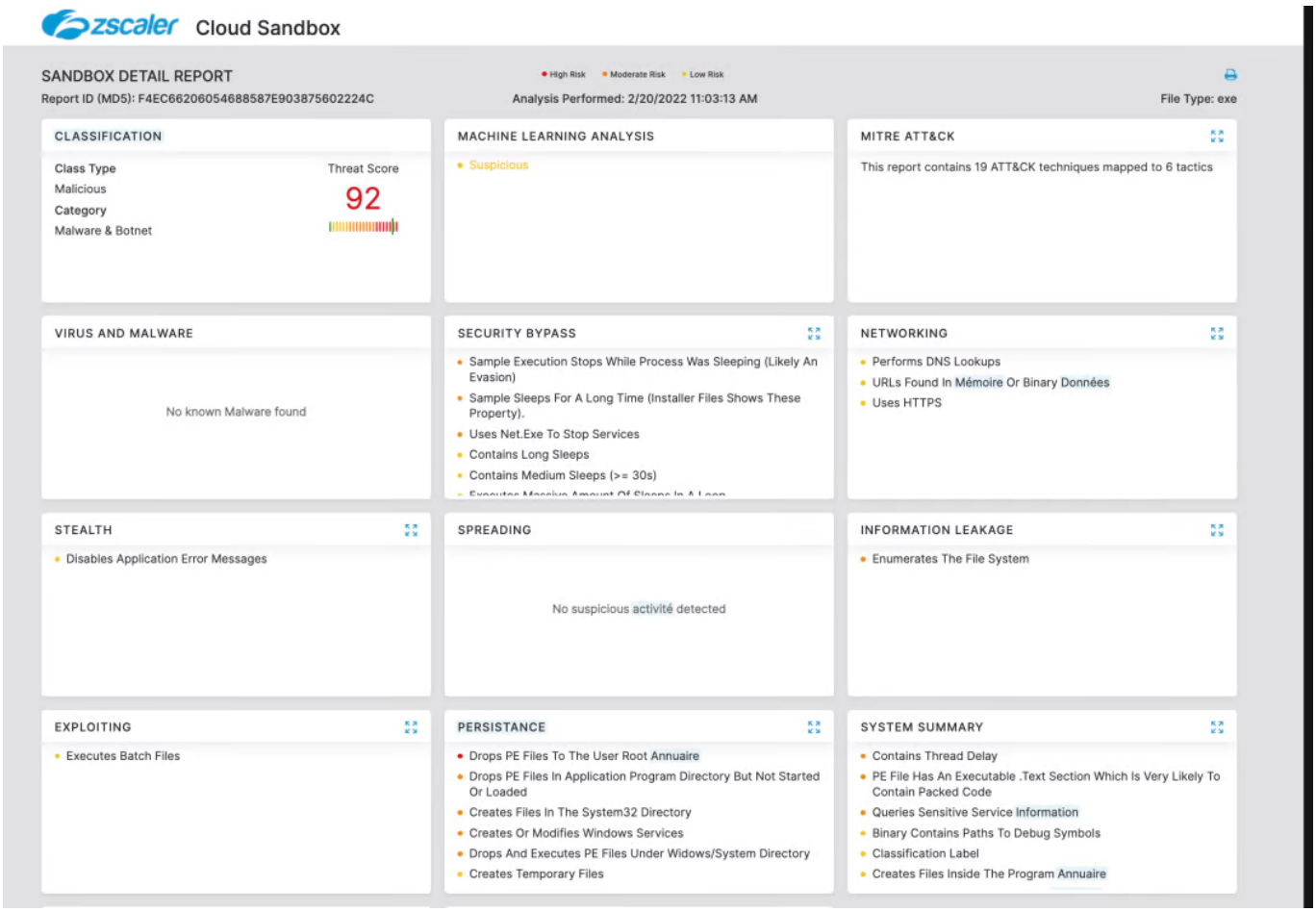
W32/Trojan.BEIE-5677

Advanced Cloud Sandbox

Win32.Trojan.Wincen

Advanced Cloud Sandbox Report

Zscaler's Cloud Sandbox detonates the payloads to reveal their actual behavior and plays a critical role in providing global protection against new payloads.



The Zscaler ThreatLabz team is actively monitoring this campaign and providing coverage for threats. More updates to follow.