baseVISION TI Report #1

How threat actors are abusing Microsoft Teams to trick your employees, and what you can do about that

baseVISION

Cyber threats don't always come with the highest complexity to be effective. Most of the times, the simplest tactics are the most dangerous. As a matter of fact, social engineering remains the primary initial access method, with the majority of attacks (roughly 98%) relying on such techniques.

This number should not come as a surprise, as the human element remains the weakest link in the cybersecurity chain. Attackers have long recognized the value of exploiting this vulnerability, as people are often the easiest entry point for a successful attack, even in environments with highly robust and secure technical defenses.

Over the past months, a notable surge in phishing and voice phishing (vishing) attempts has been observed in multiple countries, including Switzerland, with email bombing and Microsoft Teams as the principal attack vector to target employees across companies in all sectors. Our monitoring efforts have also revealed a significant uptick in similar activities affecting our customer base. Here is a recap of the observed tactics and techniques, how they have been evolving throughout time and how you can safeguard your company against them.

98%

of cyberattacks rely on social engineering

700

social engineering attacks an average business organization faces every year.

Black Basta: The ransomware behind these operations

Who is Black Basta

Black Basta is a ransomware operator offering Ransomware-as-a-Service (RaaS) to a closed number of affiliates since 2022. Assessed to include current or former members of the Conti group, Black Basta adopts a double extortion technique, where in addition to demanding ransom for files decryption, victims are also threatened with the possibility their information could be leaked if the ransom is not paid.

Technique

Different Black Basta-related actors have been observed abusing Microsoft Teams since October 2024. The attack pattern appears to be the same independently from the operating group, and has been described in an advisory published by CISA. The same operations have also been detected in Switzerland, as reported by NCSC.

As per the initial access, users would firstly receive mass emails from outside the organization in a very short period of time. After flooding the user's mailbox with spam, a message or call via Teams from an alleged "Help Desk" would follow, with an external user offering assistance to solve the issue. This would happen by taking advantage of a default Microsoft Teams configuration, which allows external users to initiate chats or meetings with internal ones. Should the victim fall into the trap and call or message back, the threat actor would then attempt to convince the user in installing a tool for remote access, such as AnyDesk or Microsoft's Quick Assist. Once the user allows access and control, the threat actor runs malicious commands to download batch or ZIP files to deliver malicious payloads. In other cases, the attackers have been observed sharing a QR code with the targeted user, in an alleged attempt to bypass MFA after stealing a user's credentials. Once the phone call is concluded and access is established, the threat actor would perform further activities such as domain enumeration and lateral movement.

Microsoft Threat Intelligence attributed the activities to the financially motivated group tracked as Storm-1811, which has been observed delivering Black Basta malware since April 2024. In late January 2025, security researchers at Sophos have discovered a new threat cluster which has consolidated the previously observed operations, tiding those incidents to two separate threat actors. These have been tracked under the names STAC5777 (with overlapping techniques with Storm-1811) and STAC5143 (with possible connections to the financially motivated threat actor with Russian ties, known under various names such as FIN7, Sangria Tempest or Carbon Spider).

The interest in leveraging trusted platforms such as Microsoft Teams is a common topic, not only for adversaries but for security researchers and red teamers as well. As an example, a new interesting C2 infrastructure has recently emerged and dubbed as convoC2, and has been used by red teamers in legitimate operations by leveraging Microsoft Teams. Even though no adversary exploitation has been detected yet, it is worth noticing that a public proof of concept (PoC) is available. Attackers are able to embed commands into hidden span tags in Microsoft Teams messages, triggering out-of-bound requests to a C2 server. Even in this scenario, attackers do not need to be in the same organization as the victims. The monitoring is tricky because there is no direct communication between attacker and victim: the victim only sends http requests to Microsoft servers, and therefore the whole process is obfuscated to most antivirus solutions.

Cyber Threat Update: Storm-1811 & Microsoft Teams Exploits

Storm-1811 & Black Basta Ransomware

- **Who?** Storm-1811, a financially motivated cybercrime group.
- **What?** Spreading Black Basta ransomware since April 2024.
- New Developments (Jan 2025):
  - STAC5777 → Uses similar techniques as Storm-1811.
  - STAC5143 → Possibly linked to FIN7 / Sangria Tempest / Carbon Spider.

Microsoft Teams Exploited – A Growing Focus

- Both cybercriminals and security researchers are paying close attention to Microsoft Teams as a potential attack vector.
- **New Tool:** convoC2 – used by red teamers, but now a public PoC exists.
- How it Works:
  - Malicious commands hidden in Teams messages.
  - No direct attacker-victim communication → hard to detect.
  - Victims unknowingly send requests via Microsoft servers, evading security tools.

Key Takeaway: Teams exploitation is a rising concern. Monitor activity, stay alert, and enhance defenses!

Free Dark Web Report

Find out how popular you are on the dark web

Mitigations

Different are the measures that organizations can take in order to be protected against such threats. We at baseVISION offer a wide range of services to strengthen your defenses and reduce risks. Our experts can guide you through these strategies to ensure comprehensive protection for your organization. Some of the key recommendations include:

- Verify your Anti-Spam Inbound Policies, and submit the messages to Microsoft for analysis;
- As a further preventative measure, if possible, prevent chats with unmanaged Teams accounts;
- Even though adversaries keep changing their domains and senders, consider blocking the senders and domains;
- Consider raising awareness for this kind of attacks within the organization, warning users across the company not to be lured by the email bombing.

baseVISION

Indicators of Compromise (IOCs)

Here below you can find an extract of the most recent IoCs tracked for STAC5143 and STAC5777 activities. If you require additional Indicators of Compromise (IOCs), would like to explore further threat hunting services, or have any questions regarding our offerings, please don't hesitate to contact us. Our team is available to provide the support and expertise you need to strengthen your security posture.

Type	IOCs	Note
IPv4	109.107.170[.]2	STAC5143 – C2 IP address
IPv4	206.206.123[.]75	STAC5143 – C2 IP address
IPv4	207.90.238[.]52	STAC5777 – C2 IP address
SHA256	8abc8c92ebfe78f54e7488a467d1b6e90d28382067b49a954e31133691112eba	STAC5143 obfuscated RPivot tool component
SHA256	ea2b3bf32cc27e959e19c365fa2f6e5310ef2e76d3d0ed2df3fb5945f9afc9e7	STAC5777 winhttp.dll C2 backdoor
Account	helpdesk@llladminhlpll.onmicrosoft[.]com	STAC5777 abused M365 account

Want to know more about the XTI&H service?
Check out!