


# DarkGate malware delivered via Microsoft Teams - detection and response

---

 [cybersecurity.att.com/blogs/security-essentials/darkgate-malware-delivered-via-microsoft-teams-detection-and-response](https://cybersecurity.att.com/blogs/security-essentials/darkgate-malware-delivered-via-microsoft-teams-detection-and-response)

1. [AT&T Cybersecurity](#)
2. [Blog](#)

January 30, 2024 | [Peter Boyle](#)

## Executive summary

---

While most end users are well-acquainted with the dangers of traditional phishing attacks, such as those delivered via email or other media, a large proportion are likely unaware that Microsoft Teams chats could be a phishing vector. Most Teams activity is intra-organizational, but Microsoft enables External Access by default, which allows members of one organization to add users outside the organization to their Teams chats. Perhaps predictably, this feature has provided malicious actors a new avenue by which to exploit untrained or unaware users.

In a recent example, an AT&T Cybersecurity Managed Detection and Response (MDR) customer proactively reached out with concerns about a user who was external to their domain sending an unsolicited Teams chat to several internal members. The chat was suspected to be a phishing lure. The customer provided the username of the external user as well as the IDs of multiple users who were confirmed to have accepted the message.

With this information, the AT&T Cybersecurity MDR SOC team was able to identify the targeted users, as well as suspicious file downloads initiated by some of them. A review of the tactics and indicators of compromise (IOCs) utilized by the attacker showed them to be associated with DarkGate malware, and the MDR SOC team was able to head off the attack before any significant damage was done.

## Investigation

---

### Initial event review

---

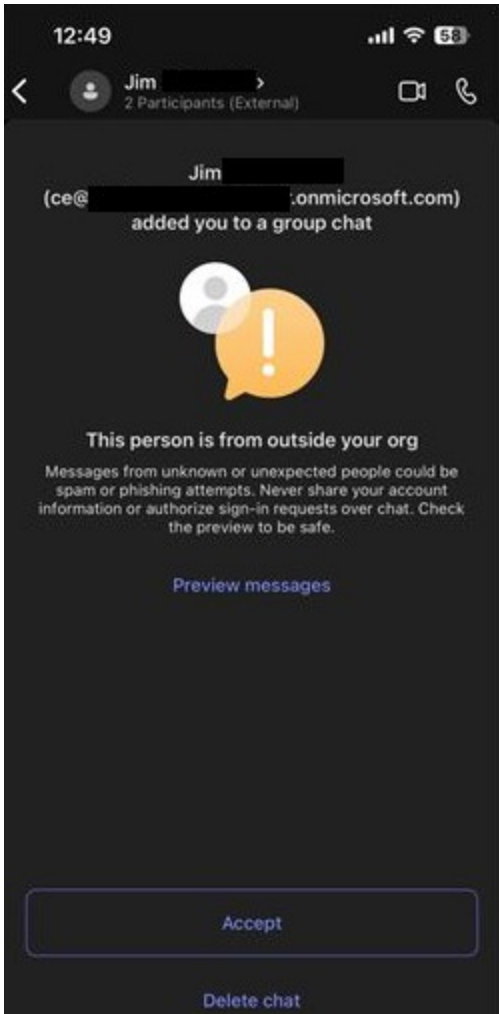
### Indicators of compromise

---

The customer provided the below screenshot (Image 1) of the message that was received by one of their users and which was suspected to be a phishing lure. An important detail to note here is the “.onmicrosoft.com” domain name. This domain, by all appearances, is authentic and most users would probably assume that it is legitimate. OSINT research on the domain

also shows no reports for suspicious activity, leading the MDR SOC team to believe the username (and possibly the entire domain) was likely compromised by the attackers prior to being used to launch the phishing attack.

**Image 1: Screenshot from customer of received message**



## Expanded investigation

---

### Events search

---

Performing a search of the external username in the customer's environment led the MDR team to over 1,000 "MessageSent" Teams events that were generated by the user. Although these events did not include the IDs of the recipients, they did include the external user's tenant ID, as displayed in Image 2 below.

**Image 2: Event log showing external user tenant ID**

```
{
  "AppAccessContext": {
    "IssuedAtTime": "2023-10-12T19:35:59",
    "UniqueTokenId": [REDACTED]
  },
  "CreationTime": "2023-10-12T21:30:06",
  "Id": [REDACTED],
  "Operation": "MessageSent",
  "OrganizationId": "[REDACTED]-acb0c8fbc13d",
  "RecordType": 25,
  "UserKey": "[REDACTED]",
  "UserType": 0,
  "Version": 1,
  "Workload": "MicrosoftTeams",
  "ClientIP": [REDACTED],
  "UserId": [REDACTED]onmicrosoft.com",
  "ChatThreadId": "19:725beb9ff23e413ebf65c402739a7374@thread.v2",
  "CommunicationType": "OneOnOne",
  "ExtraProperties": [],
  "MessageId": "1697146206921",
  "MessageVersion": "1697146206921",
  "ParticipantInfo": {
    "HasForeignTenantUsers": true,
    "HasGuestUsers": false,
    "HasOtherGuestUsers": false,
    "HasUnauthenticatedUsers": false,
    "ParticipatingDomains": [
      "[REDACTED]onmicrosoft.com",
      [REDACTED]
    ],
    "ParticipatingTenantIds": [
      [REDACTED]-acb0c8fbc13d",
      [REDACTED]-9798b197a0a3"
    ]
  }
},
"ResourceTenantId": [REDACTED]9798b197a0a3",
"ItemName": "19:725beb9ff23e413ebf65c402739a7374@thread.v2"
```

A Microsoft 365 tenant ID is a globally unique identifier assigned to an organization. It is what allows members of different companies to communicate with one another via Teams. As long as both members of a chat have valid tenant IDs, and External Access is enabled, they can exchange messages. With this in mind, the MDR SOC team was able to query events that contained the external user's tenant ID and found multiple "MemberAdded" events, which are generated when a user joins a chat in Teams.

**Image 3: "MemberAdded" event**

```
{
  "AppAccessContext": {
    "IssuedAtTime": "2023-10-13T06:33:54",
    "UniqueTokenId": "[REDACTED]"
  },
  "CreationTime": "2023-10-13T06:39:29",
  "Id": "[REDACTED]",
  "Operation": "MemberAdded",
  "OrganizationId": "[REDACTED]-acb0c8fbc13d",
  "RecordType": 25,
  "UserKey": "[REDACTED]",
  "UserType": 0,
  "Version": 1,
  "Workload": "MicrosoftTeams",
  "UserId": "[REDACTED]",
  "ChatThreadId": "19:e4ea144be56844839c10575a93b44210@thread.v2",
  "CommunicationType": "OneOnOne",
  "Members": [
    {
      "OrganizationId": "[REDACTED]-acb0c8fbc13d",
      "DisplayName": "[REDACTED]",
      "Role": 2,
      "UPN": "[REDACTED]"
    }
  ],
  "ParticipantInfo": {
    "HasForeignTenantUsers": true,
    "HasGuestUsers": false,
    "HasOtherGuestUsers": false,
    "HasUnauthenticatedUsers": false,
    "ParticipatingDomains": [],
    "ParticipatingTenantIds": [
      "[REDACTED]-acb0c8fbc13d",
      "[REDACTED]-9798b197a0a3"
    ]
  },
  "ResourceTenantId": "[REDACTED]-9798b197a0a3",
  "UserTenantId": "[REDACTED]-acb0c8fbc13d"
}
```

These events include the victim's user ID, but not the external user ID. In addition to the external tenant ID, the MDR SOC team was able to positively link these "MemberAdded" events back to the attacker via the "ChatThreadId" field, which was also present in the original "MessageSent" events. The customer was provided with a list of users who accepted the external chat and was then able to begin identifying potentially compromised assets and accounts for remediation.

## Event deep-dive

---

The MDR SOC team continued to drill down on the phished users to determine the precise nature of the attack. They subsequently discovered three users who had downloaded a suspicious double extension file. The file was titled "Navigating Future Changes October 2023.pdf.msi" (Image 4).

### ***Image 4: Suspicious double extension file download***

```

{
  "DestinationLocationType": 1,
  "Platform": 1,
  "Application": "chrome.exe",
  "FileExtension": ".msi",
  "DeviceName": [REDACTED],
  "MDATPDeviceId": [REDACTED],
  "Sha1": "1156ab27d8e65b92f5fe8842547eea941c93ac77",
  "Sha256": "92b65d3d0a6c6b8e5d73593a2f5a53eed851a1d139848a300e9f1f52592e5920",
  "EnforcementMode": 1,
  "TargetFilePath": "C:\\Users\\[REDACTED]\\Downloads\\Navigating Future Changes October 2023.pdf.msi",
  "FileSize": 1159168,
  "FileType": "Unknown",
  "Hidden": false,
  "ObjectId": "C:\\Users\\[REDACTED]\\Downloads\\Navigating Future Changes October 2023.pdf.msi",
  "UserId": "[REDACTED]",
  "ClientIP": [REDACTED],
  "Id": [REDACTED],
  "RecordType": 63,
  "CreationTime": "2023-10-12T20:08:05",
  "Operation": "FileDownloadedFromBrowser",
  "OrganizationId": [REDACTED],
  "UserType": 0,
  "UserKey": [REDACTED],
  "Workload": "Endpoint",
  "Version": 1,
  "Scope": 1
}

```

Double extension files are commonly used by attackers to trick users into downloading malicious executables, as the second extension, .msi in this case, is usually hidden by the filesystem. The user believes they are downloading a PDF for business use, but instead receives a malicious installer.

The MDR SOC team was able to provide the filename and associated hashes to the customer who in turn passed that information onto their endpoint detection and response (EDR) provider so the file could be added to the blocklist. The information about the file downloads also enabled the customer to begin identifying affected assets for isolation and remediation.

### Reviewing for additional indicators

The customer later provided the malicious file to the MDR SOC team for further analysis. Upon detonation in a sandbox, the file attempted to beacon out to the domain hgfdytrywq[.]com, which is a confirmed DarkGate command-and-control (C2) domain, according to Palo Alto Networks (<https://github.com/PaloAltoNetworks/Unit42-timely-threat->

[intel/blob/main/2023-10-12-IOCs-for-DarkGate-from-Teams-chat.txt](#)). The filename is also very similar to the files listed by Palo Alto Networks and the double-extension file is a known DarkGate tactic.

## Remediation

---

The MDR SOC provided the customer with a list of users who had received the message, users who were confirmed to have accepted the message, and users who were identified as having initiated a download of the malicious .msi file. The customer used this information to initiate password resets for the affected users and to determine which assets were infected so that they could be isolated and rolled back to a clean state. The DarkGate file hashes and paths were blocklisted by the customer's EDR solution and the C2 domain was blocked. The customer was also advised to consider disabling Teams External Access unless it was necessary for business use.

## Recommendations

---

Email phishing attacks have long been a threat to organizations, and they will continue to be, but phishing via Microsoft Teams is a relatively new phenomenon. This attack vector is a reminder of the need for constant vigilance and user training in the face of evolving threats.

Unless absolutely necessary for daily business use, disabling External Access in Microsoft Teams is advisable for most companies, as email is generally a more secure and more closely monitored communication channel. As always, end users should be trained to pay attention to where unsolicited messages are coming from and should be reminded that phishing can take many forms, beyond the typical email. Not everyone is on the same team!

## Share this with others

---

Tags: [malware research](#), [stories from the soc](#), [microsoft teams](#), [darkgate](#)