

Appendix: Additional attack scenarios

Contents

Attacks inside the organization	03
Attacking other organizations.....	05
Spam and phishing campaigns	06
Business email compromise (BEC)	07

Attacks inside the organization

There are several other attack scenarios that can be efficiently executed against an organization using Power Automate framework.

Its ability to automate access to email, SharePoint, and Teams while bundling it with external communication allows for other types of living-off-the-land (LOTL) approaches to malicious automation. Some examples include:

- The automation of access persistence
- The creation of backdoor flows that are triggered upon the receipt of a magic email, message or file in SharePoint
- SharePoint can be populated with malicious office documents that can later be distributed to other organizational employees for lateral movement

Below, we lay out many other attack scenarios broken down by category:

Lateral movement

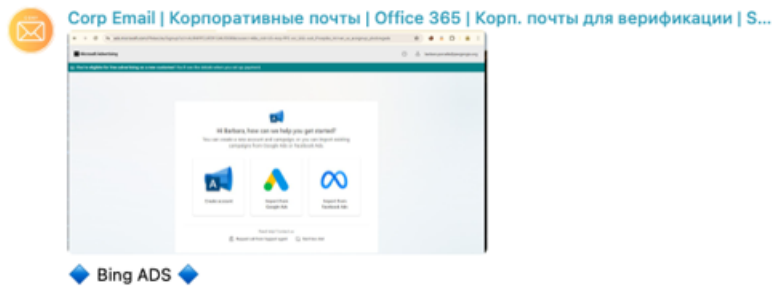
There are multiple scenarios in which the Power Automate framework may be used for lateral movement. For example, attackers could use it to automate the enumeration of the organizational structure, then use those identities to spread laterally through the organization via traditional phishing techniques (like the distribution of messages with links to phishing pages) or to distribute malicious office documents.

Extortion and attacks that can affect reputation

The Power Automate framework's abilities to process content, post, and initiate other activities on behalf of a user can create a variety of options for extortion. Notably, Power Automate incorporates AI-enabled features for processing documents that may introduce an additional layer of risk, considering there have been reports of AI models exhibiting unexpected behavior like blackmail.^{1,2}

Attackers could use Power Automate to send an offensive email to an external person on behalf of an executive of the company, providing them with significant extortion leverage over the target. Additionally, the ability to send messages with sensitive or offensive content from an executive's account, whether addressed to employees or released publicly, can significantly affect the reputation of the person or the company they work for. In the case of publicly traded companies, this could even lead to changes in the stock price.

Also, the advertising capabilities linked to corporate Office 365's infrastructure may give an attacker the ability to post advertisements on behalf of the company. They can leverage this to spread false narratives, manipulate public opinion, conduct phishing, and distribute malware. Figure 1 shows a post on a criminal forum on how to use corporate Office 365 accounts to start advertising campaigns.



📧 Напоминаем вам, что наши Corp Emails идеально подходят для Bing Ads.

- ✅ Вам не нужно будет принимать коды на почту.
- ✅ Достаточно просто войти в Office365 с помощью наших почтовых ящиков, и вы сразу попадете в Ads. Этим вы экономите свое время на создание аккаунтов и ожидание кодов на вашу почту.

⚡ Также доступна выборка по:

- Рабочему домену.
- Проверка компании США по вашему запросу.
- Адресу и номеру телефона.
- High Rep.
- Правильному адресу на сайте.
- Исключению школ и университетов.
- Правильному имени в самой почте с указанием имени и фамилии (без лишних слов).

А также другие ваши запросы, которые обсуждаются индивидуально.

ENG 🇺🇸 🇬🇧 🇫🇷

📧 Reminder that our Corp Emails are perfect for Bing Ads.

- ✅ You won't need to receive codes to your email.
- ✅ Simply log in to Office365 using our mailboxes, and you'll immediately access Ads. This saves your time on creating accounts and waiting for codes on your email.

⚡ We also offer:

- Work domain selection.
- USA company verification upon your request.
- Address and phone number.
- High Rep.
- Correct website address.
- Exclusion of schools and universities.
- Correct name format in emails with first and last name only.

And we're open to discussing other specific requests you may have.

📧 Contact: @ [redacted]

Figure 1. Post about the advertisement capabilities of Office 365 corporate accounts

Attacking other organizations

Access to Office 365 and Power Automate in organizations also opens the door for malicious actors to initiate attacks against other organizations by leveraging the infrastructure and trust relations between business entities, as shown in Figure 2.

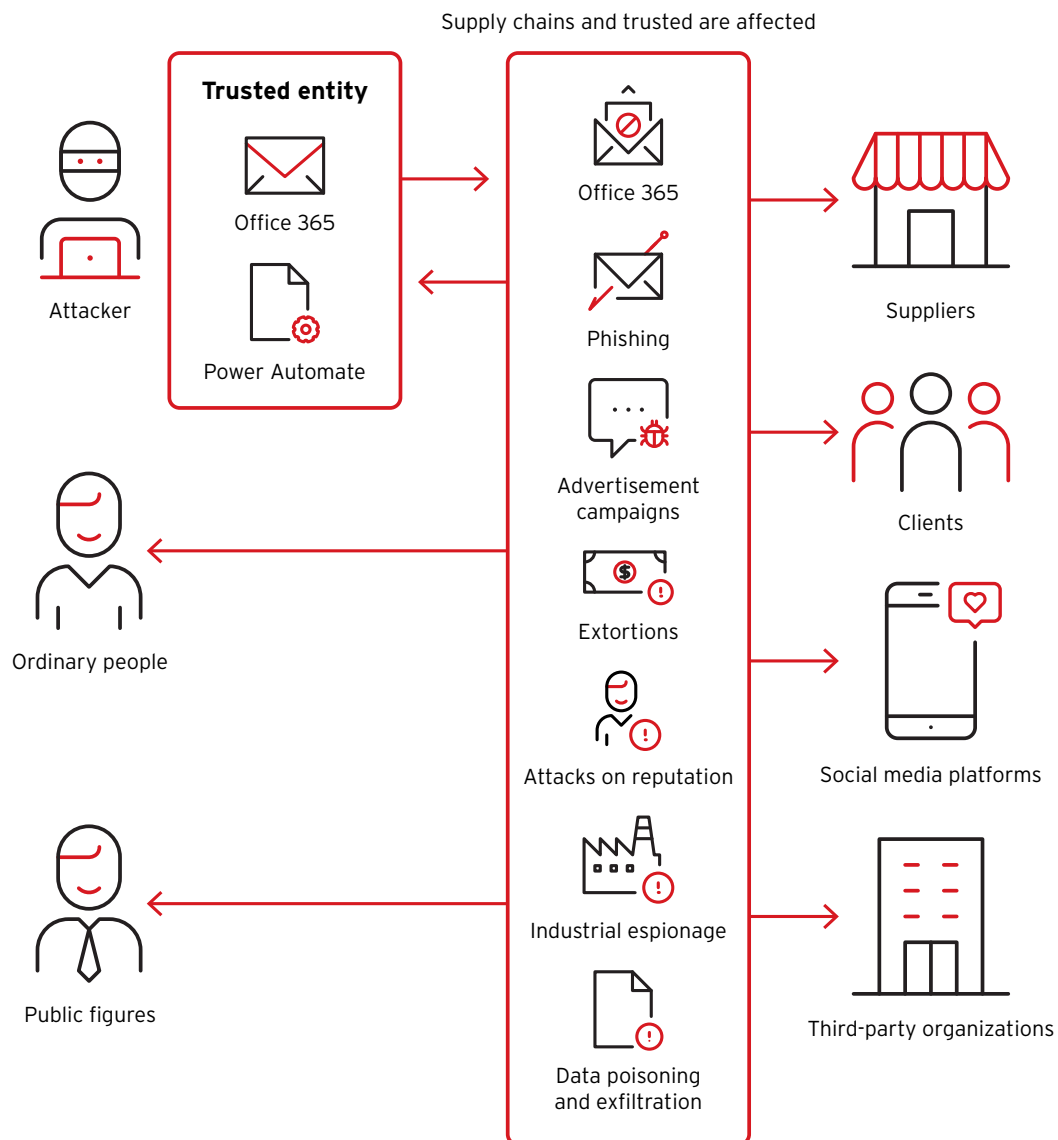
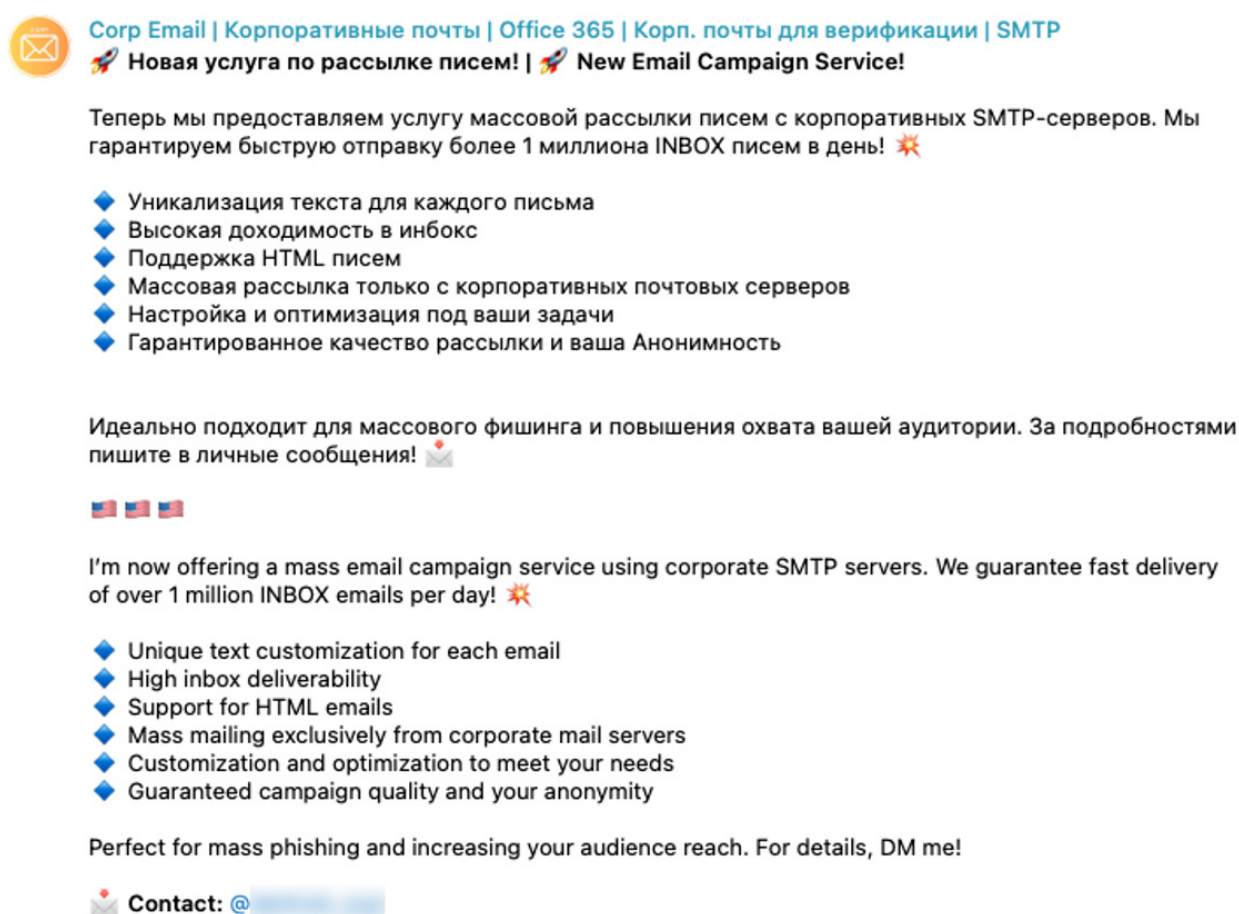


Figure 2. Interactions between a compromised trusted entity and their partner network

Spam and phishing campaigns

Power Automate can implement triggers to send emails for a variety of scenarios³ that empower existing criminal business processes related to mass emailing. Through the use of connectors, it is also possible to automate the sending of SMS, further extending these attack scenarios.⁴

In Figure 3, we can see an advertisement for a service carrying out mass email campaigns, claiming up to one million emails successfully delivered per day and sent exclusively from corporate mail servers. The service is advertised as a perfect option for mass phishing campaigns and spamming campaigns, since it uses the reputation of victimized companies as a trusted sender.



The advertisement is presented in two versions: Russian and English. Both versions feature a yellow envelope icon with a red 'X' and a rocket icon. The Russian text is in Cyrillic, and the English text is in Latin script. Both versions claim to offer a mass email campaign service using corporate SMTP servers, guaranteeing fast delivery of over 1 million INBOX emails per day. The services listed include text customization, high inbox deliverability, HTML email support, exclusive mass mailing from corporate mail servers, customization and optimization to meet needs, and guaranteed campaign quality and anonymity. The Russian version includes a contact instruction to write in private messages, while the English version includes a contact instruction to DM.

Corp Email | Корпоративные почты | Office 365 | Корп. почты для верификации | SMTP
🚀 Новая услуга по рассылке писем! | 🚀 New Email Campaign Service!

Теперь мы предоставляем услугу массовой рассылки писем с корпоративных SMTP-серверов. Мы гарантируем быструю отправку более 1 миллиона INBOX писем в день! 🚀

- ◆ Уникализация текста для каждого письма
- ◆ Высокая доходимость в инбокс
- ◆ Поддержка HTML писем
- ◆ Массовая рассылка только с корпоративных почтовых серверов
- ◆ Настройка и оптимизация под ваши задачи
- ◆ Гарантированное качество рассылки и ваша Анонимность

Идеально подходит для массового фишинга и повышения охвата вашей аудитории. За подробностями пишите в личные сообщения! ✉️

🇷🇺 🇺🇸 🇬🇧

I'm now offering a mass email campaign service using corporate SMTP servers. We guarantee fast delivery of over 1 million INBOX emails per day! 🚀

- ◆ Unique text customization for each email
- ◆ High inbox deliverability
- ◆ Support for HTML emails
- ◆ Mass mailing exclusively from corporate mail servers
- ◆ Customization and optimization to meet your needs
- ◆ Guaranteed campaign quality and your anonymity

Perfect for mass phishing and increasing your audience reach. For details, DM me!

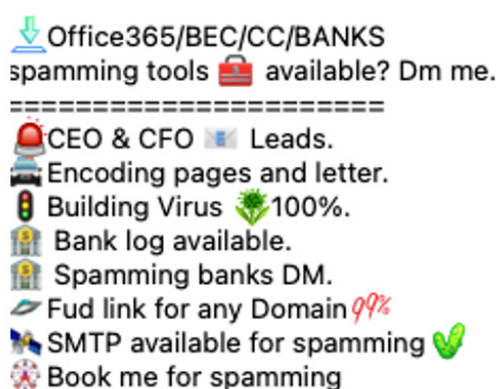
✉️ **Contact:** @ [redacted]

Figure 3. Example of a mass email campaign service, which leverages corporate Office 365 accounts

Business email compromise (BEC)

Power Automate may also empower business email compromise (BEC) attacks through its ability to trigger automatic actions. An attacker could set up necessary flows and triggers within the organization, such as creating an event or sending an email based on incoming email parameters. They might even automate the auto-update of all invoice documents with the attacker's own banking information. In addition to being used to trigger BEC attacks against other trusted organizations, this scenario is also especially powerful for internal BEC attacks, due to the extra level of access to the office document and messaging environment the attackers have.

The screenshot in Figure 4 below shows an advertisement for BEC-related services which are leveraging victim Office 365 infrastructure.



Office365/BEC/CC/BANKS
spamming tools available? Dm me.
=====

- CEO & CFO Leads.
- Encoding pages and letter.
- Building Virus 100%.
- Bank log available.
- Spamming banks DM.
- Fud link for any Domain 99%
- SMTP available for spamming
- Book me for spamming

Figure 4. BEC related services, which are leveraging Office 365 infrastructure advertised

Other discussions on criminal forums indicate a capability to spoof invoices on Office 365 platforms. This is a key part of the criminal business process related to BEC.

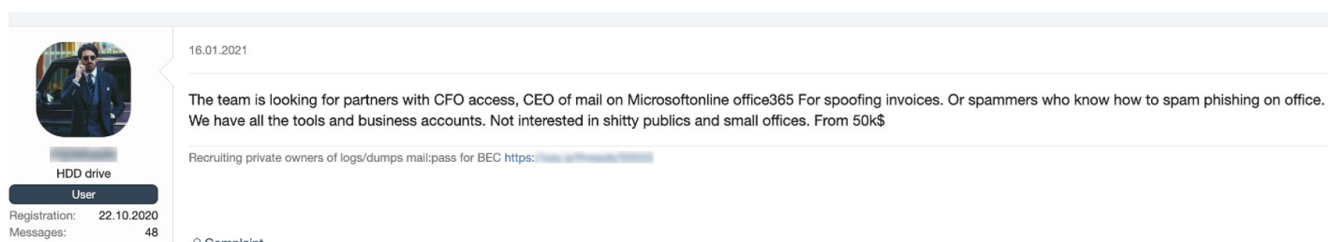


Figure 5. Request to supply corporate Office 365 accounts to monetize through invoice spoofing on Telegram

Other discussions indicate a similar approach, leveraging Office 365 capabilities to send emails which include fake invoices.

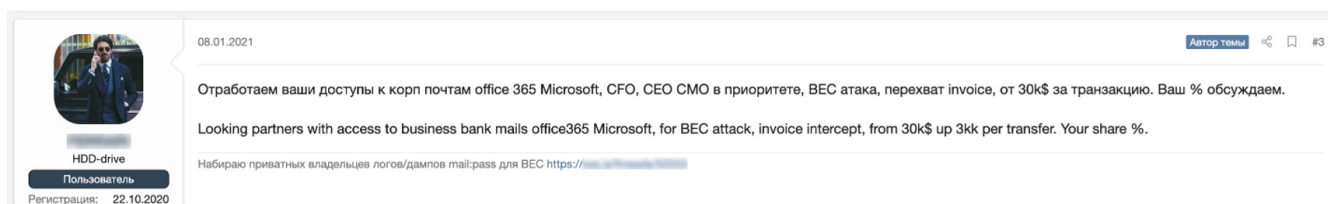


Figure 6. Forum thread discussing access monetization for Office 365 platform using fake invoices

In addition to a range of financial criminal business models, the capability to manipulate invoices can also create extortion opportunities. For example, creating an invoice that includes a sanctioned entity and luring the victim to transfer funds to this entity, and then following with a threat to reveal this activity to the relevant regulating body.

Endnotes

- 1 Liv McMahon. (May 23, 2025). *BBC*. "AI system resorts to blackmail if told it will be removed." Accessed on July 2, 2025, at: [Link](#).
- 2 Anthropic. (May 2025). *Anthropic*. "System Card: Claude Opus 4 & Claude Sonnet 4." Accessed on July 2, 2025, at: [Link](#).
- 3 Microsoft. (June 25, 2025). *Microsoft*. "Create flows for popular email scenarios." Accessed on August 13, 2025, at: [Link](#).
- 4 Microsoft. (n.d.). *Microsoft*. "SMSAPI." Accessed on August 13, 2025, at: [Link](#).