CLOUD OFFICE SECURITY

INCREASED SECURITY FOR MICROSOFT 365 APPLICATIONS

Millions of companies across the globe are moving their daily operations to the cloud. As Windows remains the most popular platform, it is only natural that many of those organizations decide to use Microsoft 365 applications when moving away from on-premises software. Despite Microsoft's efforts invested into the security of the suite, there are still threats that manage to slip through the cracks.

That's where ESET Cloud Office Security (ECOS) enters the scene, providing Microsoft 365 applications with additional layers of protection.

ECOS' detection technology is based on ESET's 30 years of threat-fighting experience and development and offers reliable spam filtering, anti-phishing and antimalware scanning. Any suspicious activity detected in Exchange, OneDrive, SharePoint and Teams is immediately reported to the security staff via an easy-to-use cloud console.

THREATS DETECTED BY ESET CLOUD OFFICE SECURITY

In just the first half of 2021, ESET Cloud Office Security has blocked thousands of threats that bypassed native protection included in Microsoft 365. While the majority were phishing and spam messages, infostealers, downloaders and other types of dangerous malware were also detected. Some of the most severe threats are described below.

Downloaders

Emotet

Detected as a variant of PowerShell/ TrojanDownloader.Agent

Emotet was a notorious modular trojan, used primarily to download further malware—such as banking trojans, infostealers and ransomware—onto the compromised machines. Before its takedown in January 2021, Emotet had formed one of the largest and most prolific botnets, launching large-scale malspam campaigns containing malicious Office and PDF documents, spreading some of the most unscrupulous ransomware families such as Ryuk, Conti, BitPaymer and DoppelPaymer.

Learn more

Nemucod

Detected as variants of JS/TrojanDownloader. Nemucod and JS/Danger.ScriptAttachment

Nemucod is a notorious downloader family that spreads via malicious attachments in emails. Its main goal is to download further malware to the affected device. This malware family has fueled many large-scale malspam campaigns in the past, most notably those that distribute botnets such as TrickBot or delivering final payload such as GandCrab and Avaddon ransomware.

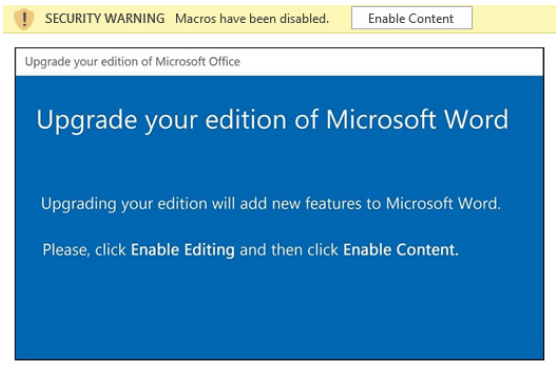
Learn more

Malicious VBA macros

Detected as variants of a variant of VBA/ TrojanDownloader.Agent

VBA/TrojanDownloader.Agent is a detection that typically covers malicious macros embedded into compromised Microsoft Office files. These are attached and sent in spam campaigns, disguised as important information relevant to the recipient. If enabled by the victim, the malicious macro downloads and executes additional malware. This technique is employed by multiple downloader and botnet families, including Qbot, Trickbot and Dridex as well as the now defunct Emotet.

Learn more



Document templates used to spread malicious macros by the now-defunct Emotet botnet

Infostealers

Agent Tesla

detected as variants of MSIL/Kryptik and MSIL/GenKryptik

Agent Tesla is a remote access trojan that became extremely popular due to its malware-as-a-service business model and easy-to-use interface. The capabilities of this powerful infostealer include harvesting login information from various credential-storing apps, keylogging and taking screenshots of the victim's desktop. It is typically spread via malspam, abusing legitimate, hacked email accounts for distribution. It uses sophisticated techniques to evade detection.

Learn more

Win32/Agent.ADAT trojan

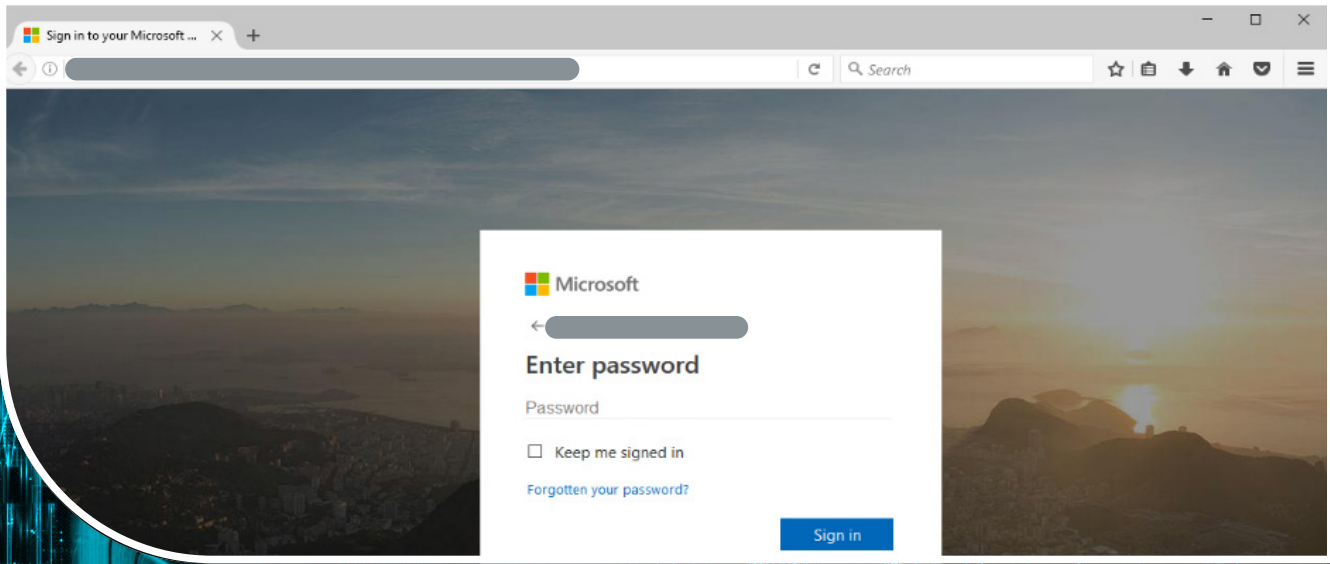
Win32/Agent.ADAT is the detection name for a file named "tax_invoice.com". Using this financial ruse, this file drops several other malicious files and executes them without the victim's knowledge. The code inside one of the malicious executables lays ground for a process injection, the initial stage of further compromise. A similar attack path has been seen in cases where Formbook was used as the payload. The primary aim of the Formbook malware family is to harvest and steal sensitive information such as browser history and stored passwords.

Learn more about Formbook

Phishing

HTML/Phishing.Microsoft

HTML/Phishing.Microsoft is the detection for a phishing threat distributed mostly as an email attachment. To hide the malicious purpose of the file, attackers use the ruse of unpaid invoices and payment orders, or try to lure victims with intriguing filenames such as "New Fax Received" or "AudioMessage". After opening the attachment, victims are redirected to a fake login website designed to harvest their Office 365 credentials.



ESET Cloud Office Security

Advanced preventive protection for Microsoft 365 applications against malware, spam and phishing attacks via an easy-to-use cloud management console.

LEARN MORE | FREE TRIAL

ESET Cloud Office Security
is included in your purchase of
ESET PROTECT Complete

INCLUDED COMPONENTS

- Cloud-based console
- Endpoint protection
- File server security
- Full disk encryption
- Cloud sandbox
- Mail security
- Cloud app protection

LEARN MORE

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services, delivering instant, comprehensive protection against evolving cybersecurity threats for businesses and consumers worldwide.

ESET is privately owned. With no debts and no loans, we have the freedom to do what needs to be done for the ultimate protection of all our customers.

www.eset.com

ESET IN NUMBERS

110m+ users worldwide

400k+ business customers

200+ countries & territories

13 global R&D centers

CYBERSECURITY EXPERTS ON YOUR SIDE

20210830