techwell

Check Point®
SOFTWARE TECHNOLOGIES

Threat Intelligence Report

Email Attack Report

Emails Summary Data

- **78%** of malicious files are distributed by Email.
- **1** out of every **227** Email attachments is malicious
- **1** out of every **624** links in Emails is malicious.
- **1** out of every **555** malicious Emails is Sextortion email.

Major Email Attacks

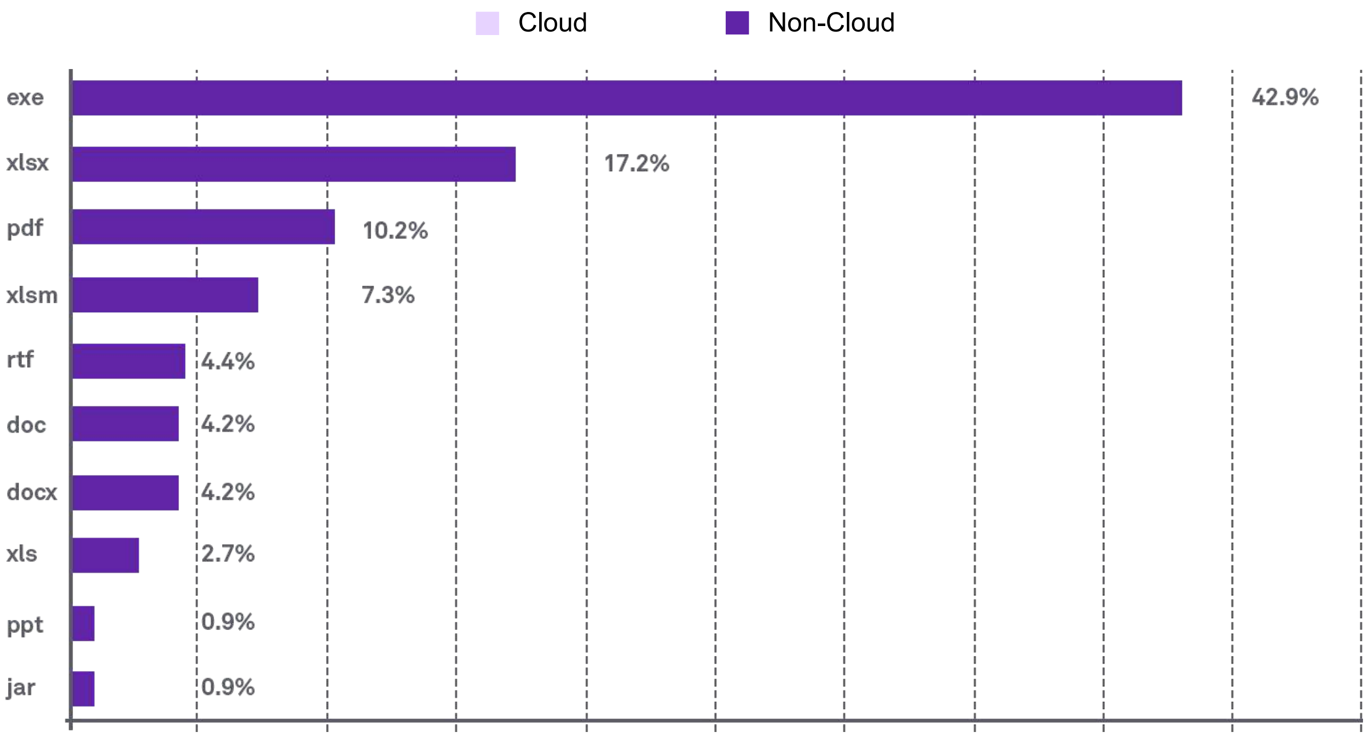
- 05-2021 - A spear-phishing campaign has been targeting travel and aerospace companies utilizing two RATs, RevengeRAT and AsyncRAT, deployed via a newly exposed malware loader. Spoofed email addresses are used in the phishing emails, as well as images posing as PDF files.
- 05-2021 - Three new malware families have been deployed as part of a spear-phishing campaign executed by the financially motivated cybercrime group referred to as UNC2529. Among them is a backdoor dubbed DoubleBack, which does not rely on hardcoded functionalities and is thus configured per target.
- 05-2021 - Hackers suspected to be linked to the Chinese government have deployed a new malware dubbed PortDoor in the systems of the design division of Marine Engineering, the engineering company in charge of the design of the Russian Navys submarines. The attack relied on spear-phishing
- 04-2021 - The 93rd Academy Awards were being abused by threat actors in a phishing campaign luring people into giving up credentials to stream the Oscar-nominated films.
- 04-2021 - Iranian APT group Charming Kitten, linked to the government, has launched a new phishing campaign targeting medical professionals from the fields of genetics, neurology and oncology in the United States and Israel. The campaign relies on emails delivering links to fake Microsoft 365 and OneDrive login pages.
- 03-2021 - Several members of the German Parliament have been hit by a targeted spear-phishing attack allegedly launched by the Russia-linked Ghostwriter threat group.

Top Malware Email Campaigns

MALWARE FAMILY	GLOBAL IMPACT	DESCRIPTION
Agenttesla	2%	AgentTesla is an advanced RAT (remote access Trojan) that functions as a keylogger and password stealer. Active since 2014, AgentTesla can monitor and collect the victim's keyboard input and system clipboard, and can record screenshots and exfiltrate credentials entered for a variety of software installed on the victim's machine (including Google Chrome, Mozilla Firefox and Microsoft Outlook email client). AgentTesla is openly sold as a legitimate RAT with customers paying $15 - $69 for user licenses.
Formbook	2%	First detected in 2016, FormBook is an InfoStealer that targets the Windows OS. It is marketed as MaaS in underground hacking forums for its strong evasion techniques and relatively low price. FormBook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to orders from its C&C.
Icedid	1%	IcedID is a banking Trojan which first emerged in September 2017. It spreads by mail spam campaigns and often uses other malwares like Emotet to help it proliferate. IcedID uses evasive techniques like process injection and steganography, and steals user financial data via both redirection attacks (installs a local proxy to redirect users to fake-cloned sites) and web injection attacks.
Qbot	1%	Qbot AKA Qakbot is banking Trojan that first appeared in 2008, designed to steal users banking credentials and keystrokes. Often distributed via spam email, Qbot employs several anti-VM, anti-debugging, and anti-sandbox techniques, to hinder analysis and evade detection.

Check Point SOFTWARE TECHNOLOGIES LTD techwell

Top Malicious Files



Check Point SOFTWARE TECHNOLOGIES LTD techwell