Turning Telegram toxic: ‘ToxicEye’ RAT is the latest to use Telegram for command & control

blog.checkpoint.com/2021/04/22/turning-telegram-toxic-new-toxiceye-rat-is-the-latest-to-use-telegram-for-command-control/

April 22, 2021

Remote access trojan exploits Telegram communications to steal data from victims and update itself to perform additional malicious activities

Research by: *Omer Hofman*

Telegram, the cloud-based IM platform has enjoyed a surge in popularity this year because of controversial changes to its rival, WhatsApp’s privacy settings. Telegram was the most downloaded app worldwide for January 2021 with more than 63 million installs, and has surpassed 500 million monthly active users. This popularity also extends to the cyber-criminal community. Malware authors are increasingly using Telegram as a ready-made command and control (C&C) system for their malicious products, because it offers several advantages compared to conventional web-based malware administration.

In this blog, we’ll explore why criminals are increasingly using Telegram for malware control, using the example of a new malware variant called ‘ToxicEye’ that we have recently observed in the wild.

Why hackers are turning to Telegram for malware control

The first use of Telegram as the C&C infrastructure for malware was the ‘Masad’ info-stealer back in 2017. The criminals behind Masad realized that using a popular IM service as an integral part of their attacks gave them a number of operational benefits:

- Telegram is a legitimate, easy-to-use and stable service that isn't blocked by enterprise anti-virus engines, nor by network management tools
- Attackers can remain anonymous as the registration process requires only a mobile number
- The unique communications features of Telegram mean attackers can easily exfiltrate data from victims' PCs, or transfer new malicious files to infected machines
- Telegram also enables attackers to use their mobile devices to access infected computers from almost any location globally.

Since Masad became available on hacking forums, dozens of new types of malware that use Telegram for C&C and exploit Telegram's features for malicious activity, have been found as 'off-the-shelf' weapons in hacking tool repositories in GitHub.

ToxicEye, a new remote access trojan

Over the past three months, Check Point Research (CPR) has seen over 130 attacks using a new multi-functional remote access trojan (RAT) dubbed 'ToxicEye.' ToxicEye is spread via phishing emails containing a malicious .exe file. If the user opens the attachment, ToxicEye installs itself on the victim's PC and performs a range of exploits without the victim's knowledge, including:

- stealing data
- deleting or transferring files
- killing processes on the PC
- hijacking the PC's microphone and camera to record audio and video
- encrypting files for ransom purposes

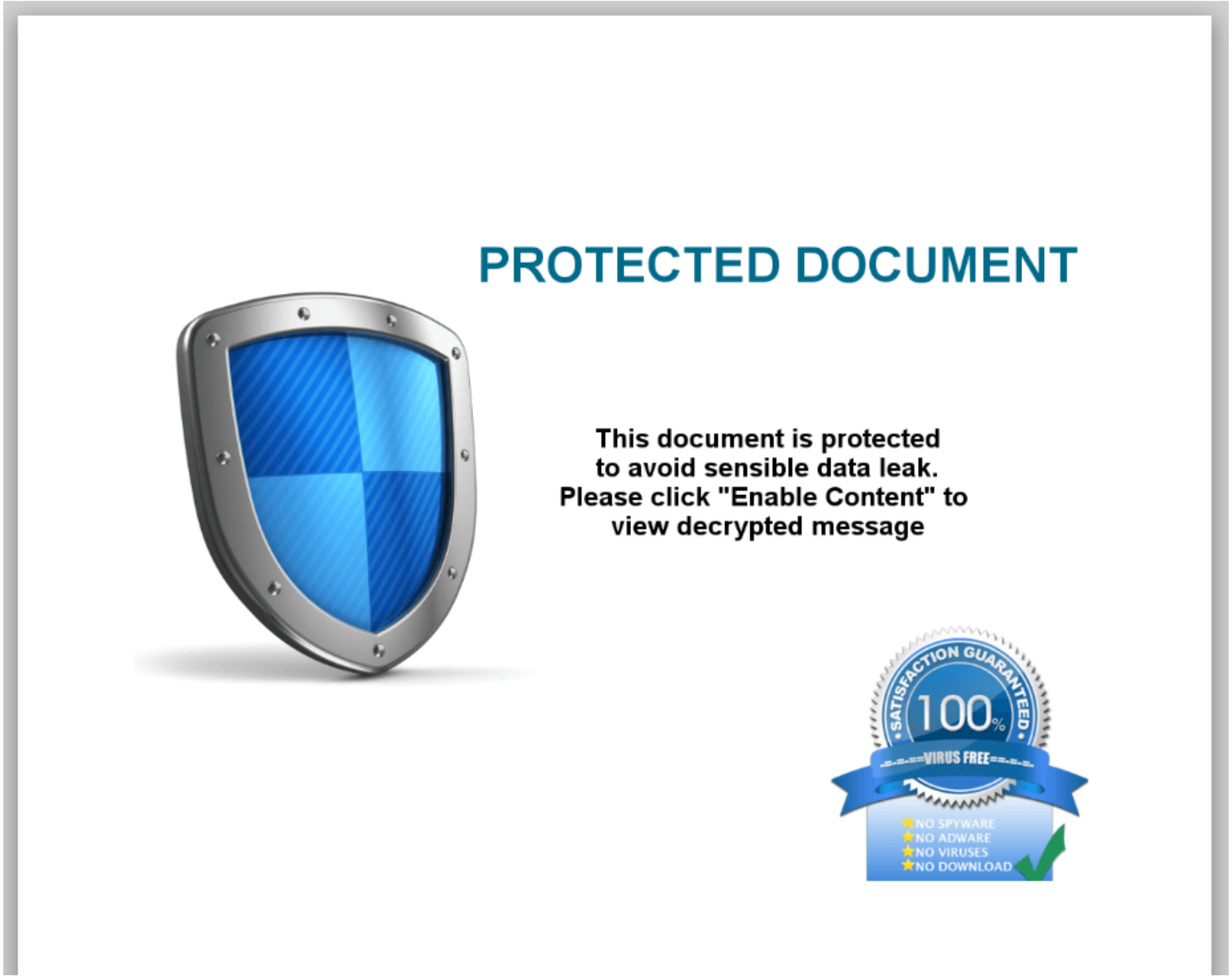
ToxicEye is managed by attackers over Telegram, communicating with the attacker's C&C server and exfiltrating data to it.

ToxicEye's infection chain

The attacker first creates a Telegram account and a Telegram 'bot.' A Telegram bot account is a special remote account with which users can interact by Telegram chat or by adding them to Telegram groups, or by sending requests directly from the input field by typing the bot's Telegram username and a query.

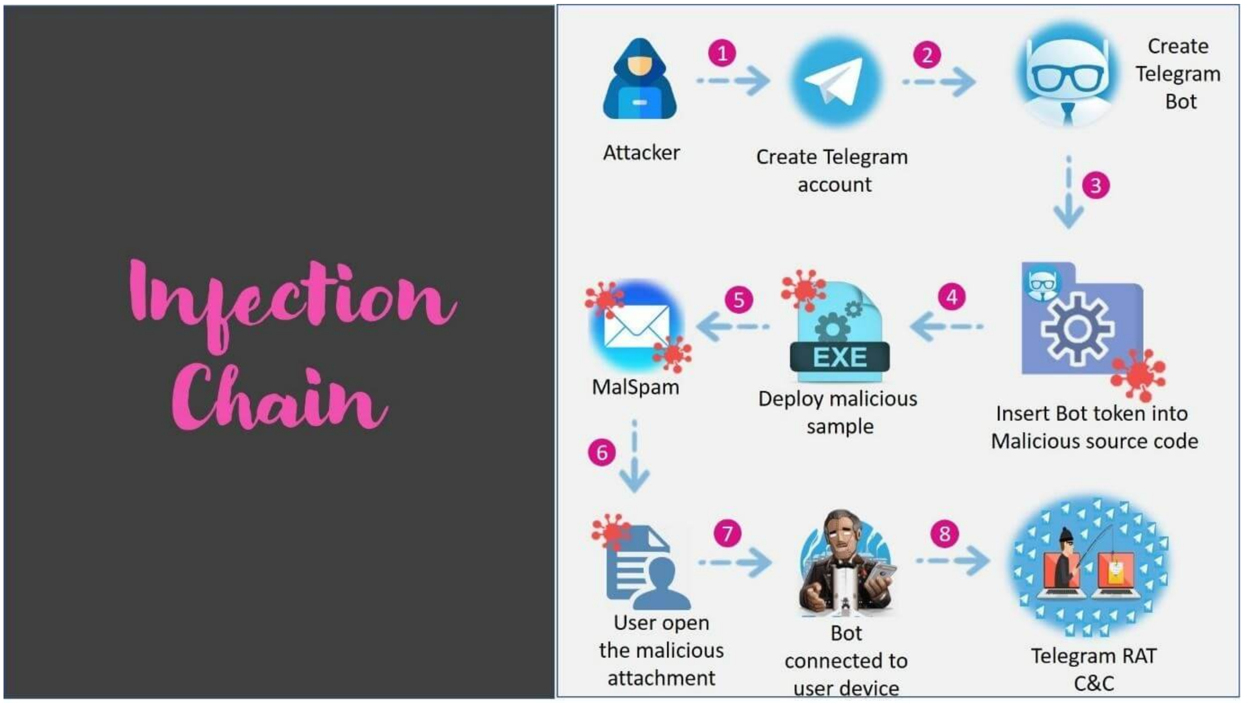
The bot is embedded into the ToxicEye RAT configuration file and compiled into an executable file (an example of a file name we found was 'paypal checker by saint.exe'). Any victim infected with this malicious payload can be attacked via the Telegram bot, which connects the user's device back to the attacker's C&C via Telegram.

In addition, this telegram rat can be downloaded and run by opening a malicious document seen in the phishing emails called solution.doc and by pressing on "enable content."

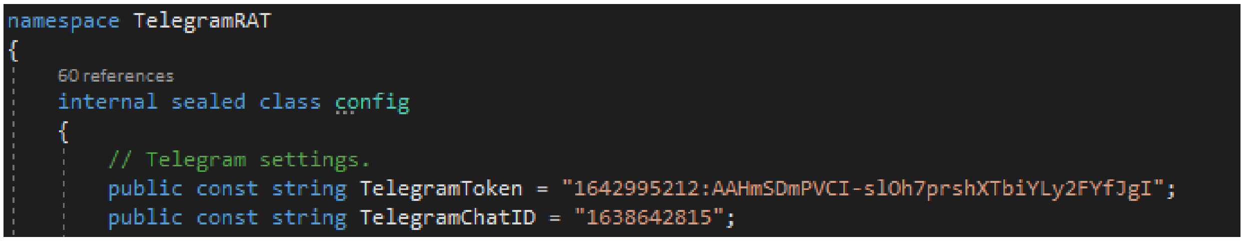


PROTECTED DOCUMENT

This document is protected
to avoid sensible data leak.
Please click "Enable Content" to
view decrypted message



The ToxicEye infection chain



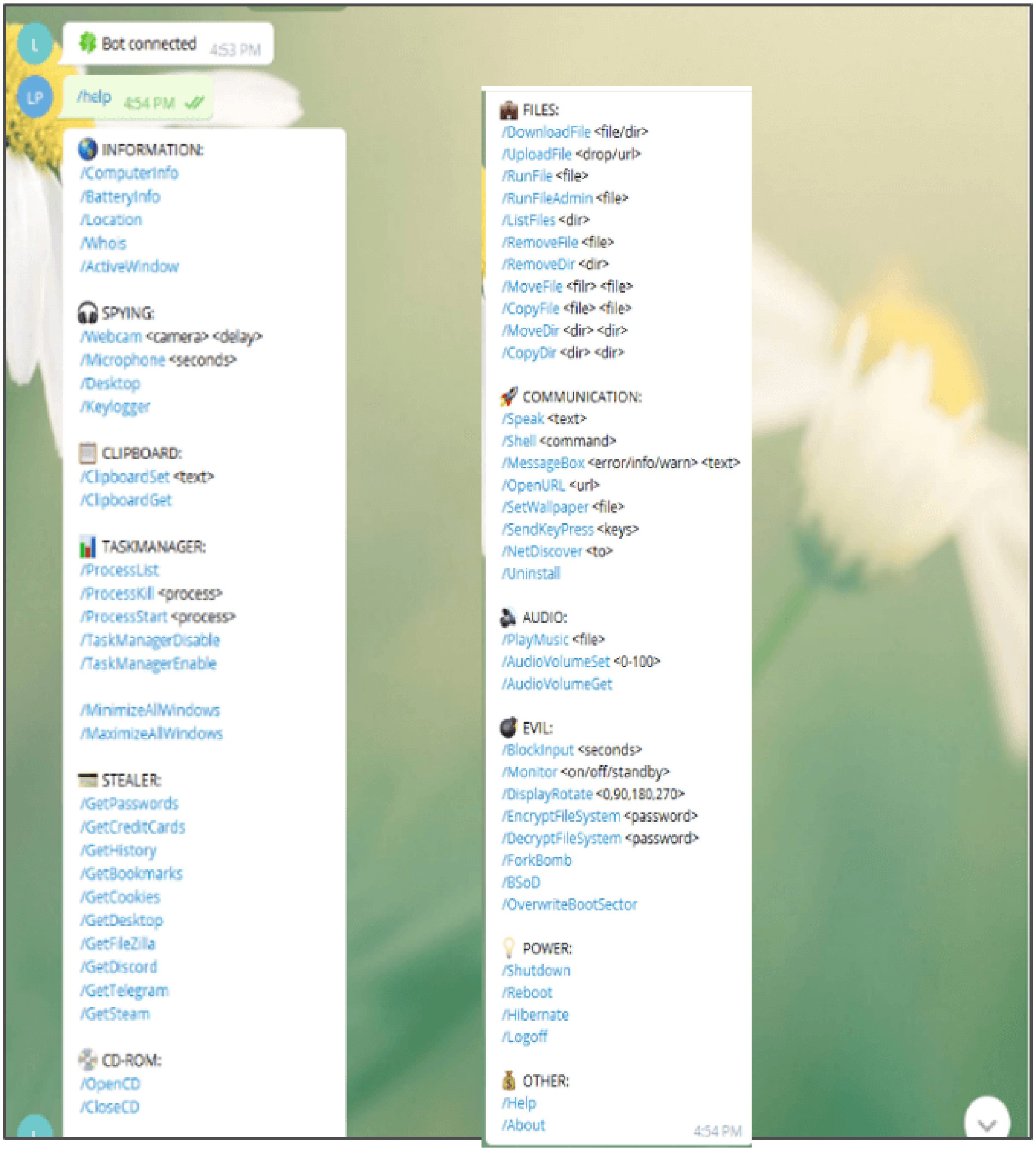
```
namespace TelegramRAT
{
    60 references
    internal sealed class config
    {
        // Telegram settings.
        public const string TelegramToken = "1642995212:AAHmSDmPVCI-slOh7prshXTbiYLy2FYfJgI";
        public const string TelegramChatID = "1638642815";
```

Code snippet example from open source telegram RAT repositories

Telegram RAT functionality

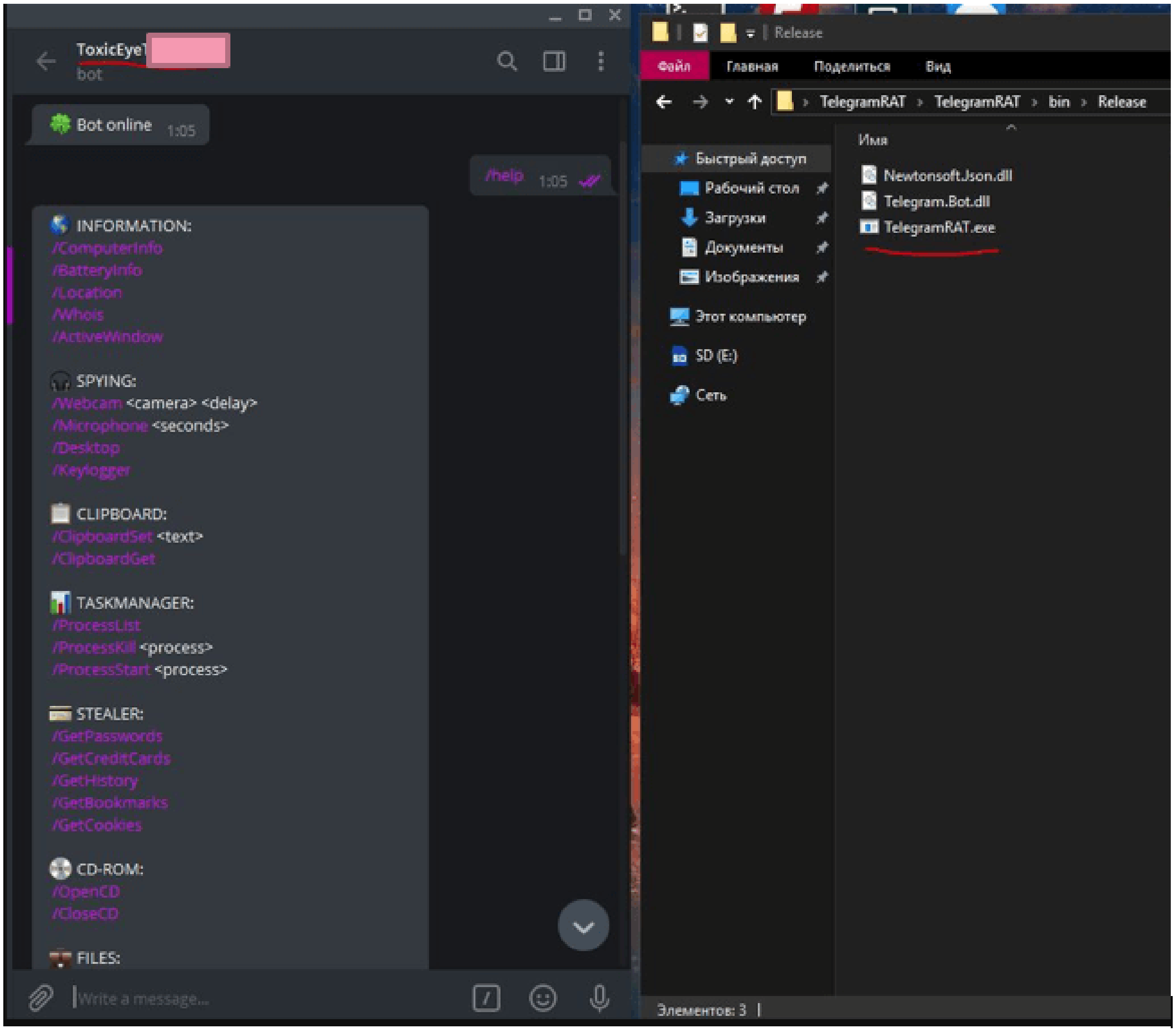
Obviously, every RAT using this method has its own functionality, but we were able to identify a number of key capabilities that characterize most of the recent attacks we observed:

- Data stealing features – the RAT can locate and steal passwords, computer information, browser history and cookies.
- File system control – Deleting and transferring files, or killing PC processes and taking over the PC's task manager.
- I/O hijacking – the RAT can deploy a keylogger, or record audio and video of the victim's surroundings via the PC's microphone and camera, or hijack the contents of the clipboard.
- Ransomware features – the ability to encrypt and decrypt victim's files.



```
L  Bot connected 4:53 PM
LP /help 4:54 PM

INFORMATION:
/ComputerInfo
/BatteryInfo
/Location
/Whois
/ActiveWindow

SPYING:
/Webcam <camera> <delay>
/Microphone <seconds>
/Desktop
/Keylogger

CLIPBOARD:
/ClipboardSet <text>
/ClipboardGet

TASKMANAGER:
/ProcessList
/ProcessKill <process>
/ProcessStart <process>
/TaskManagerDisable
/TaskManagerEnable

/MinimizeAllWindows
/MaximizeAllWindows

STEALER:
/GetPasswords
/GetCreditCards
/GetHistory
/GetBookmarks
/GetCookies
/GetDesktop
/GetFileZilla
/GetDiscord
/GetTelegram
/GetSteam

CD-ROM:
/OpenCD
/CloseCD

FILES:
/DownloadFile <file/dir>
/UploadFile <drop/url>
/RunFile <file>
/RunFileAdmin <file>
/ListFiles <dir>
/RemoveFile <file>
/RemoveDir <dir>
/MoveFile <filr> <file>
/CopyFile <file> <file>
/MoveDir <dir> <dir>
/CopyDir <dir> <dir>

COMMUNICATION:
/Speak <text>
/Shell <command>
/MessageBox <error/info/warn> <text>
/OpenURL <url>
/SetWallpaper <file>
/SendKeyPress <keys>
/NetDiscover <to>
/Uninstall

AUDIO:
/PlayMusic <file>
/AudioVolumeSet <0-100>
/AudioVolumeGet

EVIL:
/BlockInput <seconds>
/Monitor <on/off/standby>
/DisplayRotate <0,90,180,270>
/EncryptFileSystem <password>
/DecryptFileSystem <password>
/ForkBomb
/BSoD
/OverwriteBootSector

POWER:
/Shutdown
/Reboot
/Hibernate
/Logoff

OTHER:
/Help
/About
4:54 PM
```

A functionality snippet example from chosen Telegram Rat project



ToxicEye[redacted]
bot

Bot online 1:05

/help 1:05

INFORMATION:
/ComputerInfo
/BatteryInfo
/Location
/WhoIs
/ActiveWindow

SPYING:
/Webcam <camera> <delay>
/Microphone <seconds>
/Desktop
/Keylogger

CLIPBOARD:
/ClipboardSet <text>
/ClipboardGet

TASKMANAGER:
/ProcessList
/ProcessKill <process>
/ProcessStart <process>

STEALER:
/GetPasswords
/GetCreditCards
/GetHistory
/GetBookmarks
/GetCookies

CD-ROM:
/OpenCD
/CloseCD

FILES:

Write a message...

After installing the executable file, the attacker can hijack the computer through the bot (Source)

How to spot if you’ve been infected and tips to remain protected

1. ***Search for a file called C:\Users\ToxicEye\rat.exe*** – if this file exists on your PC, you have been infected and must immediately contact your helpdesk and erase this file from your system.
2. ***Monitor the traffic generated from PCs in your organization to a Telegram C&C*** – if such traffic is detected, and Telegram is not installed as an enterprise solution, this is a possible indicator of compromise
3. ***Beware of attachments containing usernames*** – *malicious* emails often use your username in their subject line or in the file name of the attachment on it. These indicate suspicious emails: delete such emails, and never open the attachment nor reply to the sender.
4. ***Undisclosed or unlisted recipient(s)*** – if the email recipient(s) has no names, or the names are unlisted or undisclosed – this is a good indication this email is malicious and / or a phishing email.

5. ***Always note the language in the email*** – Social engineering techniques are designed to take advantage of human nature. This includes the fact that people are more likely to make mistakes when they're in a hurry and are inclined to follow the orders of people in positions of authority. Phishing attacks commonly use these techniques to convince their targets to ignore their potential suspicions about an email and click on a link or open an attachment.
6. ***Deploy an automated anti-phishing solution*** – Minimizing the risk of phishing attacks to the organization requires AI-based anti-phishing software capable of identifying and blocking phishing content across all of the organization's communication services (email, productivity applications, etc.) and platforms (employee workstations, mobile devices, etc.). This comprehensive coverage is necessary since phishing content can come over any medium, and employees may be more vulnerable to attacks when using mobile devices. Check Point email security solution will help you prevent the most sophisticated phishing and social engineering attacks, before they reach users.

Conclusion

The developers who publish these tools disguise their true purpose by defining them as "Remote Administration Tool" or "for educational purpose only", although some of their characteristics are often found in malicious Trojans.

Given that Telegram can be used to distribute malicious files, or as a C&C channel for remotely controlled malware, we fully expect that additional tools that exploit this platform will continue to be developed in the future.

Check Point protections

Telegram RAT project	Samples (sha1)	Protection
Telegram Rat 2020	173542ba9f3a6b6da172572668b8d105f16eef48 e3a2b905d8d5587d2a123b5b4097df574e9d22c5 ed013c93d22c5c36a425f2aa58c6b7a4c8175c7f	RAT.Win.TelegramRat.A
Toxic eye 2020	2f452f001efd48f76a67c2f880d926e040775048 3de600dfcc588de8b4a190bc421dd854e29722c5 46396bab68ee8940b35e00840da95d3eac12a1d5	RAT.Win.ToxicEye.A RAT.Wins.ToxicEye.B
Rat via Telegram 2019	11cb873cfea6055966ddf78bd3e0c1194586ddac	RAT.Win.TelegramRat.B

Teleshadow3 2019	75f737f1291552a5d44204d30809831e2c29e44f	RAT.Win.TelegramRat.C
MASAD 2017	42c30dc551a3cb3bc935c0eae79b79f17942e439	RAT.Win.ChatC2.A