# Malicious software uses Gmail to receive commands and filter user data

An advanced version of the newly discovered backdoor ComRAT has the ability to use the Gmail web interface to receive commands from hackers and filter sensitive data.

The version of ComRAT v4 (the author of this malware called 'Chinch') uses a whole new code base and is much more complex than previous generations. According to ESET security researchers, the main purpose of ComRAT is to detect, steal, filter personal documents, sometimes even deploy the .NET implementation to interact with the MS database. SQL Server on the victim machine contains documents of the organization.
ComRAT v4's 'Mail' mode works to read valid email addresses and temporary files (cookies) stored at VFS (Virtual File System), connect to Gmail's basic HTML interface, analyze The syntax of the mailbox is on the HTML page and then the email subject list matches the file 'subject.str' on VFS.
For each email that meets the above criteria, ComRAT will download the available attachment and delete the email to avoid repeating it a second time. Whether containing the same format as the Word file (.docx) or Excel (.xlsx) in the name, the actual attachments are not document files but are encrypted binary data files containing specialized executables. especially reading / writing files, executing additional processes, collecting activity history, etc.
The results of the execution commands are then encrypted and stored as an attachment and sent in an email to the destination address available in the VFS file.
Based on one month's Gmail distribution patterns, ESET said the guys behind this campaign operate in the UTC + 3 or UTC + 4 time zone.
'ComRAT v4 was first discovered in 2017 and as of January 2020 is still active,' security expert at ESET company shared on THN. The company found that there were at least three targets targeted by the malware, including the Foreign Ministry of two Western European countries and a Caucasian parliament.
Backdoor ComRAT has long been used by the Turla APT team. The group, also known as Snake, has been operating for more than a decade with a 'track record' of offensive campaigns targeting embassies and military organizations from around 2004 or earlier.
Turla's espionage began with Agent.BTZ in 2007, later evolving into ComRAT - a remote control tool to add the ability to steal information from the local network. It was the early versions of Agent.BTZ that infiltrated the US military network in the Middle East in 2008. In the last few years, Turla was determined to be behind the attacks on the French Armed Forces (FAF) network. ) 2018 and the Austrian Foreign Ministry earlier this year.