

Deciphering Confucius' Cyberespionage Operations

By Daniel Lunghi, Jaromir Horejsi (words)

Published: 2018-02-13 · Archived: 2026-04-05 23:06:44 UTC

In today's online chat and dating scene, romance scams are not uncommon, what with [catfishersnews-cybercrime-and-digital-threats](#) and [West African cybercriminals](#) potently toying with their victims' emotions to cash in on their bank accounts. It's quite odd (and probably underreported), however, to see it used as a [vector](#) for cyberespionage.

We stumbled upon the Confucius hacking group while delving into [Patchwork's cyberespionage operations](#), and found a number of similarities. Code in their custom malware bore similarities, for instance. Confucius targeted a particular set of individuals in South Asian countries, such as military personnel and businessmen, among others.

Are Patchwork and Confucius the same group? The commands in their backdoors do resemble each other. The *config* files have a similar, custom structure, and both groups have infrastructure overlap. However, we construe them to be different groups, possibly within the same community, with different objectives and modi operandi. While Patchwork may be more straightforward with its predominantly malware-based attacks, Confucius' can be inferred to be more nuanced, relying heavily on social engineering.


Exploiting the human psyche with chat apps

Probing Confucius' infrastructure, we came across websites offering Windows and Android chat applications, most likely iterations of its predecessor, Simple Chat Point: Secret Chat Point, and Tweety Chat. We are admittedly uncertain of the extent — and success — of their use, but it's one of the ingredients of the group's operations.

While the chat applications indeed have real chat features (although the communication is not anonymous, as advertised), they have backdoor routines and file-stealing behaviors that get triggered when specific words are sent to the app: collecting and harvesting all SMS messages, contacts, and accounts. Tweety Chat's Android version can record audio, too. Its latest version can mute the device (i.e., take out the ringtone and vibration features) and sync call logs and SMSs.

We further tested Tweety Chat and saw red flags indicating their targets of interest: verification emails with a physical address whose postal code is assigned to a provincial capital that also appears (upon logging in) as a chat channel in Tweety Chat.



 [intel](#) Figure 1: Tweety Chat's interface (top), and code snippets showing the file types it steals (bottom)

Romance in cyberespionage

The user list, chat room names, and content of the applications were stored in a remote server without any authentication. The chat logs shed light on the social engineering used by the operators to persuade victims to




install the cyberespionage malware on their Android devices. The first user and chatroom were created on August 27, 2017, and were probably the app authors' testing ground. The succeeding users and chatrooms were created on October 31 and December 12 the latest.

A certain *hayat22* and *love* piqued our interest. *hayat22*, supposedly a female student, engaged in an online romance with a target whose handle was *love*, describing himself as living in South Asia working in garments manufacturing and wholesaling.

Over the course of their correspondence, *love* suggested using WhatsApp to communicate. *hayat22* declined, saying she felt safer using Tweety Chat. *love* refused, but when *hayat22* demurred and gave *love* an online cold shoulder, *love* tried installing Tweety Chat — and failed. He claimed that he wasn't able to install the app. *hayat22* quickly lost interest and stopped replying to him altogether. She also sent him a screenshot to show what Tweety Chat looked like.

We're not sure how *love* wound up in the chat room or how he met *hayat22*. He was probably either using the Windows version of Secret Chat Point or its web interface, which explains why *hayat22* was urging him to install Android Tweety Chat.

In an earlier chat group, an operator called *Heena* urged the members to install Secret Chat Point on other people's mobile devices to get perks like credits or the ability to "go invisible". In another chat room called "Maira's room", a target of interest disclosed he was a government officer traveling back from a northern city near the country's provincial capital. A few days after, the operator stopped answering in the chat room, and her user account was deleted from the server.

 [Figure 2: ByeBye Shell's interface showing Confucius' campaigns](#)  [Figure 3: Screenshot showing a group chat where the moderator is urging users to install Tweety Chat](#)  [Figure 4: Screenshot showing Tweety Chat promoted in social media](#)

A tangled web of malware

Confucius' operations include deploying bespoke backdoors and stealing files from their victim's systems with tailored file stealers, some of which bore resemblances to Patchwork's. The stolen files are then exfiltrated by abusing a cloud storage service. Some of these file stealers specifically target files from USB devices, probably to overcome air-gapped environments.

Compared to Patchwork, whose Trojanized documents exploit at least five security flaws, Confucius' backdoors are delivered through Office files exploiting memory corruption vulnerabilities [CVE-2015-1641](#) and [CVE-2017-11882](#). Their malware's resemblance to that of Patchwork's is also notable. The use of an exploit for a security flaw disclosed in December 2017 and their recent activities suggest Confucius is keenly trailing their targets.

Confucius has a miscellany of backdoors: *sctrls*, *ByeBye Shell*, *remote-access-c3*, and *sip_telephone*, to name a few. One of its file stealers, *swissknife2*, abuses a cloud storage service as a repository of exfiltrated files. At the time of research, there were around 60 victims whose data were uploaded to Confucius-owned cloud storage account. There were also a few thousand files in the account that were later deleted.

Our research, [Deciphering Confucius: A Look at the Group's Cyberespionage Operations](#), delves into the group's operations, the social engineering methods and gamut of malware it uses, and the countermeasures that

organizations can adopt to mitigate them. The list of indicators of compromise, which includes Trend Micro's corresponding detections and solutions, is in this [appendix](#).

Source: <https://blog.trendmicro.com/trendlabs-security-intelligence/deciphering-confucius-cyberespionage-operations/>