Deciphering Confucius' Cyberespionage Operations

0

Posted on: February 13, 2018 **at 5:01 am** **Posted in:** Targeted Attacks
Author:
Trend Micro Cyber Safety Solutions Team

by Daniel Lunghi and Jaromir Horejsi

In today's online chat and dating scene, romance scams are not uncommon, what with catfishers 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.

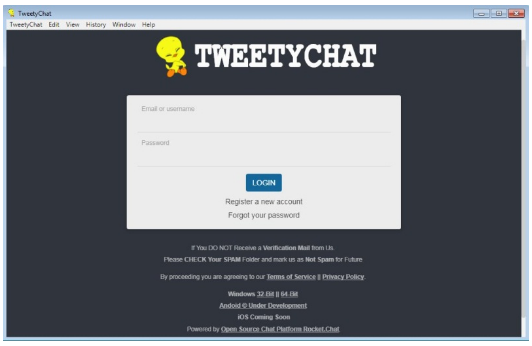
Are Patchwork and Confucius the same group? The commands in their backdoors do resemble each other. The *config* files have a similar, custom structure, and both groups have infrastructure overlap. However, we construe them to be different groups, possibly within the same community, with different objectives 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.



If You DO NOT Receive a **Verification Mail** from Us.
Please **CHECK Your SPAM** Folder and mark us as **Not Spam** for Future

By proceeding you are agreeing to our Terms of Service || Privacy Policy.

Windows 32-Bit || 64-Bit
Andoid © Under Development
iOS Coming Soon
Powered by Open Source Chat Platform Rocket.Chat

Featured Stories

- systemd Vulnerability Leads to Denial of Service on Linux
- qkG Filecoder: Self-Replicating, Document-Encrypting Ransomware
- Mitigating CVE-2017-5689, an Intel Management Engine Vulnerability
- A Closer Look at North Korea's Internet
- From Cybercrime to Cyberpropaganda

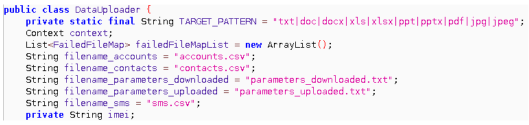
Security Predictions for 2018

- Attackers are banking on network vulnerabilities and inherent weaknesses to facilitate massive malware attacks, IoT hacks, and operational disruptions. The ever-shifting threats and increasingly expanding attack surface will challenge users and enterprises to catch up with their security. Read our security predictions for 2018.

Business Process Compromise

- Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Latest Ransomware Posts



```
public class DataUploader {
    private static final String TARGET_PATTERN = "txt|doc|docx|xls|xlsx|ppt|pptx|pdf|jpg|jpeg";
    Context context;
    List<FailedFileMap> failedFileMapList = new ArrayList();
    String filename_accounts = "accounts.csv";
    String filename_contacts = "contacts.csv";
    String filename_parameters_downloaded = "parameters_downloaded.txt";
    String filename_parameters_uploaded = "parameters_uploaded.txt";
    String filename_sms = "sms.csv";
    private String imei;
```

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

Romance in cyberespionage

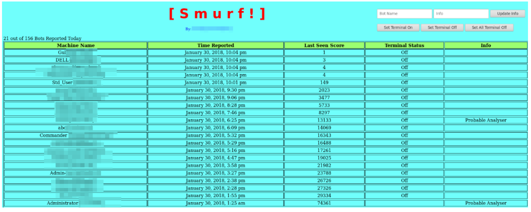
The user list, chat room names, and content of the applications were stored in a remote server without any authentication. The chat logs shed light on the social engineering used by the operators to persuade victims to install the cyberespionage malware on their Android devices. The first user and chatroom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

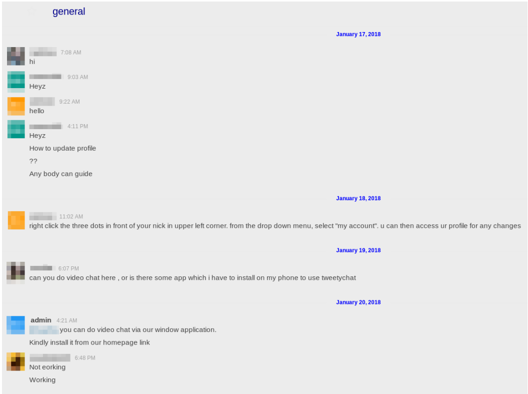


By: [redacted]

21 out of 156 Bots Reported Today

Machine Name	Time Reported	Last Seen Score	Terminal Status	Info
Gul[redacted]	January 30, 2018, 10:04 pm	1	Off	
DELL[redacted]	January 30, 2018, 10:04 pm	3	Off	
[redacted]	January 30, 2018, 10:04 pm	4	Off	
[redacted]	January 30, 2018, 10:04 pm	4	Off	
Std_User[redacted]	January 30, 2018, 10:01 pm	149	Off	
[redacted]	January 30, 2018, 9:30 pm	2023	Off	
[redacted]	January 30, 2018, 9:06 pm	3477	Off	
[redacted]	January 30, 2018, 8:28 pm	5733	Off	
[redacted]	January 30, 2018, 7:46 pm	8297	Off	
[redacted]	January 30, 2018, 6:25 pm	13133	Off	Probable Analyser
abc[redacted]	January 30, 2018, 6:09 pm	14069	Off	
Commander[redacted]	January 30, 2018, 5:32 pm	16343	Off	
[redacted]	January 30, 2018, 5:29 pm	16488	Off	
[redacted]	January 30, 2018, 5:16 pm	17261	Off	
[redacted]	January 30, 2018, 4:47 pm	19025	Off	
[redacted]	January 30, 2018, 3:58 pm	21982	Off	
Admin-[redacted]	January 30, 2018, 3:27 pm	23788	Off	
[redacted]	January 30, 2018, 2:38 pm	26726	Off	
[redacted]	January 30, 2018, 2:28 pm	27326	Off	
[redacted]	January 30, 2018, 1:55 pm	29334	Off	
Administrator[redacted]	January 30, 2018, 1:25 am	74361		Probable Analyser

Figure 2: ByeBye Shell's interface showing Confucius' campaigns



general

January 17, 2018

[redacted] 7:08 AM
hi

[redacted] 9:03 AM
Heyz

[redacted] 9:22 AM
hello

[redacted] 4:11 PM
Heyz
How to update profile
??
Any body can guide

January 18, 2018

[redacted] 11:02 AM
right click the three dots in front of your nick in upper left corner. from the drop down menu, select "my account". u can then access ur profile for any changes

January 19, 2018

[redacted] 6:07 PM
can you do video chat here , or is there some app which i have to install on my phone to use tweetychat

January 20, 2018

admin 4:21 AM
[redacted] you can do video chat via our window application.
Kindly install it from our homepage link

[redacted] 6:48 PM
Not eorking
Working

Figure 3: Screenshot showing a group chat where the moderator is urging users to install Tweety Chat

Digital Extortion: A Forward-looking View

qkG Filecoder: Self-Replicating, Document-Encrypting Ransomware

Bad Rabbit Ransomware Spreads via Network, Hits Ukraine and Russia

A Look at Locky Ransomware's Recent Spam Activities

Magnitude Exploit Kit Now Targeting South Korea With Magniber Ransomware

Recent Posts

- Tropic Trooper's New Strategy
- March Patch Tuesday Fixes 75 Security Issues, Drops Registry Key Requirement in Windows 10
- Detecting Attacks that Exploit Meltdown and Spectre with Performance Counters
- Campaign Possibly Connected to "MuddyWater" Surfaces in the Middle East and Central Asia
- Cryptocurrency-Mining Malware: 2018's New Menace?

Ransomware 101

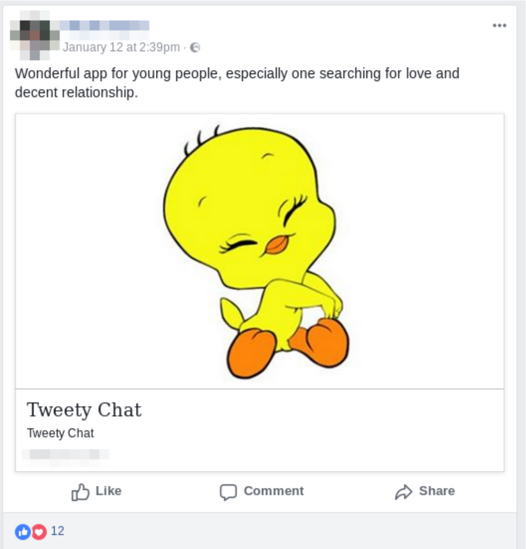
-

This infographic shows how ransomware has evolved, how big the problem has become, and ways to avoid being a ransomware victim. Check the infographic

Popular Posts

Homemade Browser Targeting Banco do Brasil Users

Vulnerabilities in Apache CouchDB Open the Door to Monero Miners



January 12 at 2:39pm ·

Wonderful app for young people, especially one searching for love and decent relationship.

Tweety Chat

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**.

Related Posts:

- **Untangling the Patchwork Cyberespionage Group**
- **ChessMaster Makes its Move: A Look into the Campaign's Cyberespionage Arsenal**
- **Cyberespionage Campaign Sphinx Goes Mobile With AnubisSpy**
- **Hacking Group Spies on Android Users in India Using PoriewSpy**

TREND MICRO Say **NO** to ransomware.
Trend Micro has **blocked over 100 million** threats and counting

Learn how to protect Enterprises, Small Businesses, and Home Users from ransomware:

ENTERPRISE » SMALL BUSINESS » HOME »

Tags: Confucius CVE-2015-1641 CVE-2017-11882 Patchwork Romance Scam

Comments for this thread are now closed. ×

0 Comments TrendLabs 1 Login

Recommend Share Sort by Best

This discussion has been closed.

Subscribe Add Disqus to your siteAdd DisqusAdd Privacy

Home and Home Office
|
For Business
|
Security Intelligence
|
About Trend Micro
Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
Latin America Region (LAR): Brasil, México
North America Region (NABU): United States, Canada
Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

Privacy Statement Legal Policies Copyright © 2018 Trend Micro Incorporated. All rights reserved.