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

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

0

By: Hara Hiroaki and Loseway Lu (Threats Analysts)

Since our last research 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 FlawedAmmyy, 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 ***technical brief***.

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.

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

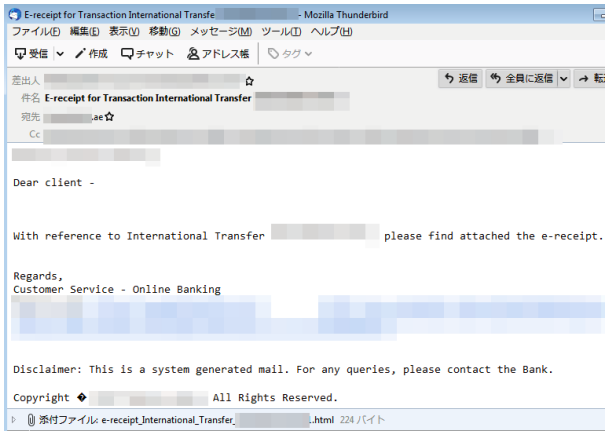


Figure 1. A sample spam email delivered to TA505's targets in the Middle East

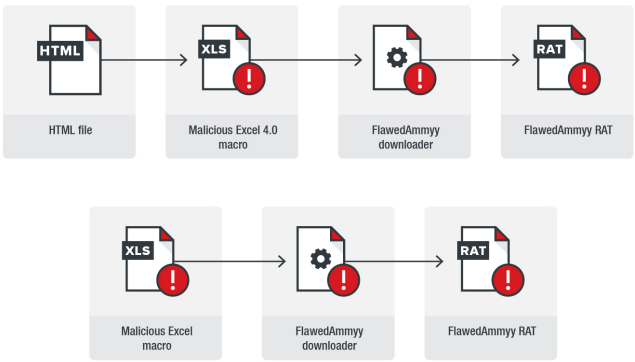


Figure 2. Infection chain of the spam emails with the FlawedAmmyy RAT

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.

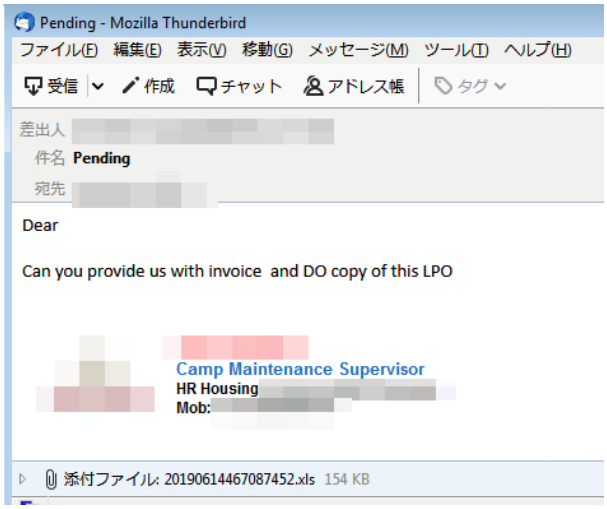


Figure 4. Sample spam email from a campaign observed on June 14

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).

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 sub-campaigns that targeted India and Italy with different email content.

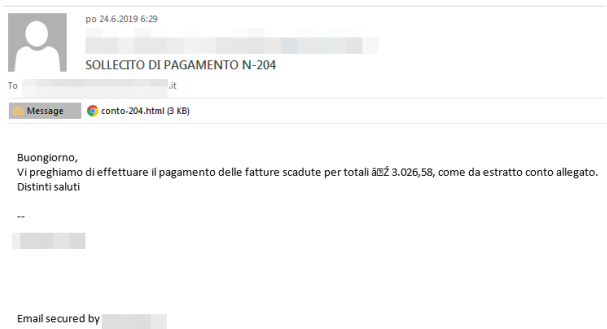


Figure 6. Screenshot of spam email from a sub-campaign observed on June 24 targeting Italy

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.

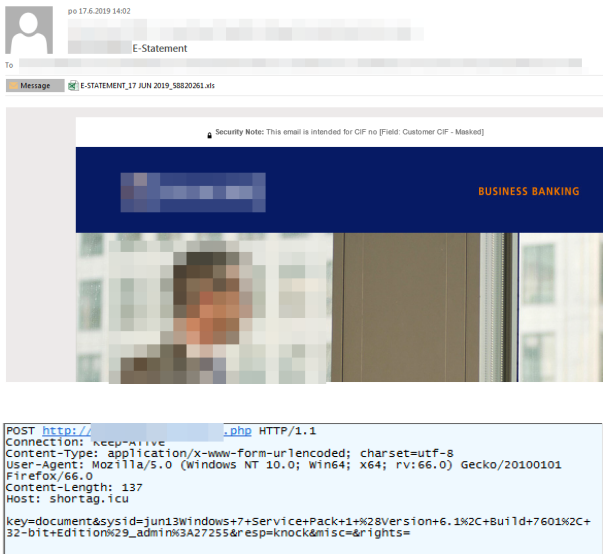
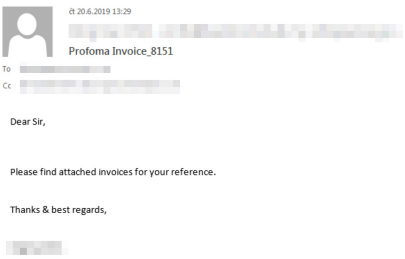


Figure 7. Sample spam email from a campaign observed on June 17 (top); the ServHelper-related command-and-control (C&C) traffic (center); and sample spam email from a similar campaign that used a mix of .html and .xls files to deliver the ServHelper loader

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.



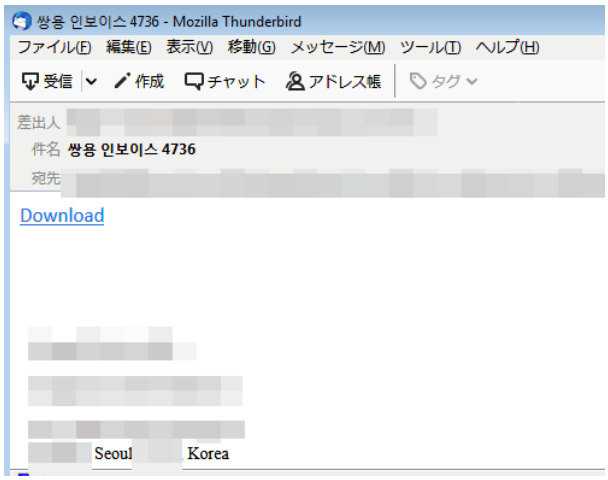


Figure 8. Screenshot of a spam email targeting Japan, the Philippines, and Argentina (top), and another that targets South Korea, which directly uses or embeds a malicious URL instead of an attachment (bottom)

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 AndroMut 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 ***technical brief***, 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 ***technical brief*** 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 ransomware 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 disclosed 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 best practices on thwarting messaging-related threats; enforce the principle of least privilege to mitigate further exposure; and regularly update systems (or use virtual patching for legacy systems) to prevent attackers from taking advantage of security gaps. Additional security mechanisms like enabling firewalls and intrusion detection and prevention systems 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 Trend Micro Smart Protection Suites and Worry-Free™ Business Security. Both solutions can protect users and businesses from threats by detecting malicious files and spammed messages as well as blocking all related malicious URLs. Trend Micro Deep Discovery™ has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs.

Trend Micro™ Hosted Email Security 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, Microsoft Office 365, Google Apps, and other hosted and on-premises email solutions.

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

With additional insights and analysis by Kawabata Kohei