TA505 Uses HTML, RATs, Other Techniques in Campaigns

By Hara Hiroaki, Loseway Lu (words)

Published: 2019-06-12 · Archived: 2026-04-05 21:21:37 UTC

TA505 is a prolific cybercriminal group known for its attacks against multiple financial institutions and retail companies using malicious spam campaigns and different malware. We have been following TA505 closely and detected various related activities for the past two months. In the group's latest campaign, they started using HTML attachments to deliver malicious .XLS files that lead to downloader and backdoor FlawedAmmyyopen on a new tab, mostly to target users in South Korea.

Figure 1. TA505’s latest infection chain

This blog post covers three main points involving TA505: their recent activity in specific regions, shifting tactics and payloads, and suspicious activity possibly associated with the group. We also touch on the latest TA505 developments, including an email stealer, their use of legitimate software and MSI Installer, and more.

Recent activity in Latin America and East Asia

As previously mentioned, TA505, first namedopen on a new tab by Proofpoint, is known for targeting financial enterprises. Since last December, TA505 has been very active and has been using legitimate or compromised RATs (remote access trojans) such as FlawedAmmyyopen on a new tab, FlawedGraceopen on a new tab, and Remote Manipulator System (RMSopen on a new tab).

While monitoring their activities, we found that the group is still updating their tactics, techniques, and procedures (TTPs). In April, TA505 targeted Latin American countries Chile and Mexico, and even Italy using either FlawedAmmyy RAT or RMS RAT as payload. By the end of April, we learned that the group started to go after targets in East Asian countries such as China, South Korea, and Taiwan using FlawedAmmyy RAT as its payload.

TA505 has also recently usedopen on a new tab LOLbins and legitimate Windows OS processes to perform malicious activities and deliver a payload without being detected. As the entry point of an attack, it delivers a sophisticated email containing a malicious Excel or Word file. The group notably abuses Excel 4.0 macro — a particularly old macro likely used to evade typical macro detection.

Figure 2. Korean language (left), simplified Chinese language (right) Microsoft Office instructions on how to enable macro

Figure 3. Excel 4.0 macro

This said macro executes a command to download the first stage payload using *msiexec.exe*, a Microsoft Installer tool that can download and run a Windows Installer file. The first stage payload is an MSI Installer that was created using an EXE to MSI converter.

Figure 4. MSI Installer payload that used EXE to MSI converter

The actual malicious payload is in the MSI Installer package. The payload can vary in each campaign, but it typically uses the FlawedAmmyy downloader, ServHelper, or RMS RAT launcher.

Payload as FlawedAmmyy downloader

The MSI Installer itself contains a FlawedAmmyy downloader, which is always signed.

Figure 5. FlawedAmmyy downloader

Figure 6. Digitally signed FlawedAmmyy downloader

The downloader will check if the infected machine is running in the Active Directory (AD) network. It then runs the “net group /domain” command and checks if “workgroup” is contained in the output result. (If it does not exist, it means that the PC is running in AD.) After performing the check, it downloads the RC4-encrypted FlawedAmmyy RAT, decrypts it, and executes it as the final payload.

We recently observed an instance where the FlawedAmmyy downloader was not digitally signed (FlawedAmmyy RAT payload is still signed, however). It could be a blip — perhaps a one-off — but it's still notable.

Payload as ServHelper

ServHelper is classified as a backdoor, but it can also workopen on a new tab as a downloader for FlawedGrace. If the MSI Installer package contains ServHelper as a payload, it will come with an NSIS (Nullsoft Scriptable Install System) installer.

Figure 7. NSIS Installer

NSIS is a legitimate tool that manages the installation for Windows, but some hacking groups also abuse it. TA505, for instance, abuses NSIS to install ServHelper. This NSIS installer has two files: (*nsExec.dll* and *repotaj.dll*) and *[NSIS].nsi*. The latter is a configuration file that handles files to install.

Figure 8. NSIS Installer sections

In this case, *repotaj.dll*, which is ServHelper, will be extracted to *%TEMP%* and execute with the "feast" parameter as its export function. Once ServHelper is executed, it runs a PowerShell script to get information from the infected machine.

Payload as RMS RAT

TA505 also uses RMS, a legitimate RAT, in their campaigns. If the MSI Installer package contains RMS RAT as its payload, it will include a self-extracting RAR.

Figure 9. SFXRAR

This SFXRAR extracts three files to *%TEMP%* and executes one of the files, where *exit.exe* is a launcher for *i.cmd*; *i.cmd* renames *kernel.dll* to *uninstall.exe*, then executes it with parameters.

Figure 10. Three files extracted from SFXRAR

Figure 11. Executed parameters

As indicated in the parameter above, *kernel.dll/uninstall.exe* is also SFXRAR, but password-protected. It will extract the following files (Figure 12) and execute *exit.exe*, where the said executable is also a launcher of *i.cmd* that registers *winserv.exe* (the actual RMS RAT) and executes it. The password used to extract from the RAR file will be passed by the parameter "-p", which is set in *i.cmd*.

Figure 12. Extracted files

Figure 13. RMS RAT is added to the startup registry and executed

Updates on TA505's tactics, techniques and procedures

Since the tail end of April through early June, we observed TA505 changing its tactics, techniques, and procedures (TTPs) in a variety of ways. The following is a quick rundown of the group's varying methods.

Using Amadey to distribute EmailStealer

On April 24, we detected an attack that used Amadey as its first stage payload. Amadey is a known downloader for another payload (FlawedAmmyy downloader) and EmailStealer, which steals email accounts or SMTP credentials from infected PCs.

In this particular attack, we discovered that the C&C server of EmailStealer had an open directory, allowing us to view the information that EmailStealer stole. We presume the information, primarily comprised of lists of email addresses, will be used in future attacks.

Using VBA macro

TA505 has been using Excel 4.0 macro for a while, but we recently observed the group using the usual VBA (Visual Basic for Applications) macro along with Excel 4.0 macro. However, they still hide the command and malicious URL in “UserForm” and not in VBA code.

Figure 14. Malicious command and URL hidden in UserForm

Avoiding the use of *msiexec.exe*

As previously mentioned, TA505 abuses *msiexec.exe* to install its first stage payload, but we recently observed the group just directly downloading the first stage payload binary and executing it. Like the VBA macro code, the group just executes the downloaded file *234.exe* by *cmd.exe*. This is possibly because endpoint security solutions easily detect *msiexec.exe*.

Using HTML as an attack entry point

TA505 has been using Excel file, Word document, or .WIZ filesopen on a new tab as its attack entry point. However, as mentioned earlier, the group has also started to attach an HTML link in emails to trick users into opening the Excel file.

Figure 15. Attached HTML

Opening this HTML link will redirect the user to a malicious URL that hosts the malicious Excel file. The Excel file still has the same style of VBA macro, which was described in the previous section. This could mean that the group is trying to change the entry point's file type to bypass macro detection.

In early June, for instance, we saw HTML in emails that used a friendly tone so recipients would download the Excel file. Some recent cases we observed even had the Excel file directly attached to the emails.

Figure 16. HTML shows a message before Excel download (Translation from Korean: Downloading ... ... will be taken to the download page after a while .... If you wait a while and continue to see this message, please click on <a href="<MALICIOUS_URL>"> link ! Thank you.)

Suspicious activity involving TA505

While analyzing TA505's activities, we encountered strange attacks that were very similar to TA505’s TTPs but with some differences. This section discusses a particular attack that, like the usual TA505 attack, distributes RMS

RAT via Excel and SFXRAR. But it also contains Kronos, a known banking trojan; and SmokeLoader, which is another payload downloader. While the attack shows characteristics that are similar those of TA505's attacks, we suspect that this could be a forged attack. As for the reason why we are dubious about this attack, another reportopen on a new tab has also since surfaced discussing that some threat actor was using similar tools to TA505's.

In this attack, the basic TTPs and tools used seem similar, but we found five interesting points that set them apart:

Using .rar or .zip as attachment

The TA505 group usually attaches a malicious file without any compression. But this attack sent an email with a .rar or .zip attachment. However, this may not be a significant difference.

Using a similar image on Excel but with different macro and attribution

The following image on Excel appears similar to the one TA505 has been using.

Figure 17. Display on Excel for this suspicious attack

But there are a few differences in this Excel file. For one thing, it has a different style of VBA macro. TA505 has been using Excel 4.0 macro and VBA macro without heavy obfuscation, but this particular Excel file was heavily obfuscated and had a different style.

Figure 18. VBA macro with heavy obfuscation

Another factor is its different codepage. Malicious Excel files that TA505 distributed had information harvesting capabilities. For example, the codepageopen on a new tab of Excel has always been "1251" Cyrillic (Windows), but the code page of this particular attack was "1252" Western European (Windows).

Figure 19. Information of Excel file used in this suspicious attack

Figure 20. Information of the usual Excel file distributed by TA505

Lacking the use of fast flux infrastructure

TA505 uses fast flux, a DNS technique used to mask botnets by quickly shifting among compromised hosts, which allows cybercriminals to delay or evade detection. The domains the group has been using to distribute payloads were usually resolved across a lot of IPs.

But in this attack, the domains used to distribute the payload only had one IP. It should be noted, however, that TA505 may have used different infrastructure for this instance, or another attacker may have performed malicious

activities under the guise of TA505.

Using Kronos and SmokeLoader (v2019)

TA505 previously used Amadey to distribute the FlawedAmmyy downloader before, so the use of Kronos and SmokeLoader can't be considered strong evidence of false attribution.

Using a different infrastructure to distribute spam

The strongest evidence that this attack might not come from TA505 is that this attack operator used a different spam infrastructure. Our daily monitoring of TA505's activities show that the group sends spam from specific IPs; this suspicious attack used different sender IPs. We couldn't find any of the IPs used in previous attacks.

We can't say for sure if this particular attack comes from TA505, another threat actor, an imitator, or perhaps just TA505 using another infrastructure. This reiterates the tricky business of attribution in cybersecurity, which calls for careful inspection. While it's easy to attribute similar incidents to certain threat actors, groups, or even countries, attribution should ultimately be based on technically provable information. After all, attributions can be used to operationalize appropriate incident response and remediation.

Defending against TA505's malicious activities

TA505 has been responsible for many large-scale attacks since at least 2014, using malicious email campaigns to distribute various banking trojans, ransomware, RATs, and backdoors. They had also targeted retail brandsopen on a new tab and even different financial companies across the world. TA505 has been focused on delivering downloaders, information stealers, and other malware — threats that can remain in affected systems if not prevented or remediated. With the group's use of email as an entry point for malicious activities, the threat has become more serious for unwitting users and organizations. Here are some best practices:

- Regularly update systems and applications.
- Incorporate multilayered security mechanisms such as firewallsopen on a new tab and intrusion detection and prevention systemsopen on a new tab.
- For system administrators, secure the email gatewayopen on a new tab to prevent it from becoming an attack entry point and proactively monitoropen on a new tab possible attack vectors.

To defend against spamopen on a new tab and threats from the TA505 group, businesses can consider Trend Micro™ endpoint solutions such as Trend Micro Smart Protection Suitesopen on a new tab and Worry-Free™ Business Securityopen on a new tab. 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™open on a new tab has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs.

Trend Micro™ Hosted Email Securityopen on a new tab 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 365open on a new tab, Google Apps, and other hosted and on-premises email solutions.

The list of indicators of compromise (IoCs) related to this threat can be found in this **appendix**open on a new tab.
