Cymulate

APT 36 Uses New TTPs and New Tools to Target Indian Governmental Organizations

Malvertising The malvertising aspect of APT-36 group has not been previously documented, so in this blog Analysts will shed some light on how the threat actor lures Indian government users to download backdoored Kavach multi-factor authentication (MFA) applications.

The threat actor routinely registered new domains and hosted web pages impersonating as the official Kavach application download portal. It then abused Google Ads' paid search feature, to push malicious attacker-registered fake websites to the top of the search results returned by Google for Kavach-related keywords such as "Kavach download" and "Kavach app," when searched from India.

Third party application stores In addition to this, Analysts also discovered that this threat group controls certain third party application stores which offer downloads for various applications. One such example is the acmarketsapp[.]com store. While at first this site seems benign and

Cymulate

The app store – acmarketsapp[.]com itself is pushed to the top in Google search results for certain search keywords from India by abusing the Google Ads paid search feature as described earlier.

By combining these techniques, it allows APT-36 to operate these third party app stores as a gateway to redirect unsuspecting users to their malicious sites hosting the latest backdoored variants of Indian government applications.

Technical analysis A new data exfiltration tool – LimePad Analysts recently identified a new and previously undocumented data exfiltration tool used by this APT group. It is distributed as a Python-based application packaged inside a VHDX file. Based on the unique strings present in the first iteration of this stealer, Analysts have named it LimePad.

Similar to some of the other malicious binaries used by the SideCopy APT group in the past, this new tool is a PyInstaller-based payload as well. Analysts found 2 unique examples of the new tool in-the-wild, both of which were distributed inside very large VHDX files with size greater than 60 MB, each.

The main purpose of this new tool is to constantly upload any new file of interest from the victim's machine to the attacker's server. It synchronizes this file stealing operation between the victim's machine and the attacker's server by maintaining a local custom SQLite database. This database holds the latest records of all the files which are uploaded, in queue or newly modified. It is done to ensure that any new files or modifications to existing local files are synced up with the remote server.

Time zone check Before starting any malicious activity, it checks whether the keyword "india" is present in the timezone config of the machine. Due to this, the payload will execute only on machines configured in India time zone.

Cymulate

early stages of development by the threat actor.

USERFILE defines the name of the local SQLite database which is used to keep track of the file sync operations. In the first version of this tool, it was configured as “Limepad.db” due to which Analysts have named this tool as “Limepad”

The fields, STARTDATA, LOCKDOORS, and DOORS are used to create a Windows URL Shortcut file which is used for the purpose of persistence. This URL shortcut file is placed in the Windows Startup directory with the name: “Limepad.dll” and it points to the local file path of the malicious payload as shown below.

[InternetShortcut] URL=file:///

A similar persistence mechanism was used by another tool in SideCopy APT’s arsenal in 2021.

SERVERS field is used to configure an array of attacker-controlled C2 servers. In both the identified samples, only one C2 server was configured each time. However, the code has support for multiple C2 servers and will cycle through them until it finds a working C2 server.

DUSSEN field contains a hex-encoded version of the string – “india”. This is what is used for the India time zone check in the main subroutine of Limepad before starting any malicious activity.

The fields – DBTABLES, DBTABLES_INDEXES and SYNC_RULES_CONFIG all correspond to the structure and configuration of the tables in the local SQLite database.

It is important to note that “SYNC_RULES_CONFIG” contains a set of rules which defines which files the attacker is interested in stealing.

Cymulate

legit browser communication.

Also, in each request to the server, an HTTP request header field called “Auth_Token” will be present. This is used to authenticate with the C2 server. This value is the same as the password which is also sent in the HTTP request. This 32 characters password is generated by base64-encoding the random value generated by os.random() using the following code.

password = base64.urlsafe_b64encode(os.urandom(30))[:32]

Server check

Sends a GET request to the file bind.php on the server. Once the server responds with “pong!”, it indicates the configured server is working well.

Registration of infected machine with the server

Sends a POST request to the file “information.php” on the server with the credentials used to register the infected machine. The username and password are sent as both – HTTP POST request body and HTTP request headers.

“Username” and “Auth_Token” fields in request headers correspond to the username and password respectively.

POST body format is: USERNAME=&PASSWORD=

This is followed by a GET request to “information.php” to confirm user registration.

Uploading files to the server

Each file upload request is in the form of HTTP POST request to the file “adjustfile.php” on the server. The local file path is included in the URL. The contents of the file are uploaded in plaintext

Cymulate

National Informatics Center(NIC) which is an Indian government department under the Ministry of Electronics and Information Technology.

On execution, the binary performs following operations:

1. Performs the time zone check and executes further only if the time zone matches Indian Standard Time (IST). 2. Extracts and drops the legit Kavach installer in the path “C:ProgramDataKavach-Auth”. The installer is extracted from the resource section of the binary. 3. Downloads and drops the Stage-2 payload from the URL “http://139.59.79[.]86/hardwell.mp3” in the path “C:ProgramDataKavach-Authhardwell.mp3” 4. Executes the dropped legit Kavach installer 5. Moves the dropped Stage-2 payload to the path “C:ProgramDataKavach-Autharchiveviewer.scr” 6. Executes the dropped Stage-2 payload

Stage-2: PyInstaller compiled binary The Stage-2 payload is a Python script compiled to an executable using PyInstaller. For analysis Analysts extracted the Python script which Analysts have included in the Appendix section.

The script on execution does following major operations:

1. Creates the directory “c:programdataWUDFHost” 2. Creates a log file in the path “c:programdataWUDFHostlogs.txt” which is updated according to the operations performed during further execution. 3. Performs the time zone check. 4. Downloads, drops and executes the next stage payload.

For the next stage payload, if the path “C:WindowsMicrosoft.NETFrameworkv4.0.30319” exists, then the payload is downloaded from the URL “http://139.59.79[.]86/WUDFHost45.zip” in the path “c:programdataWUDFHost45.zip” else it is downloaded from the URL “http://139.59.79[.]86/WUDFHost35.zip” in the path “c:programdataWUDFHost35.zip”

Cymulate

"c:\programdata\WUDFHost\oraclenotepad45.dll" 3. Creates a fake file in the path "c:\\programdata\\Expense_Account_Hierarchy.csv" and writes fake information to it. The information written is extracted from the resource section. 4. Pass the execution control to the loaded assembly

Stage-4: Backdoor The assembly loaded by the loader is the main backdoor of the infection chain. Similar to Python script. Analysts will not cover the full technical analysis for the backdoor payload since it's already covered in some public blog posts but in brief, it contains following functionalities:

1. Taking snapshots 2. Downloading new payloads and executing them 3. Creating persistence 4. Exfiltrating user and system information 5. Exfiltrating file and directory information

The backdoor also uses a helper DLL where the malware author has delegated functionalities like file download from network, writing file to disk, creating new processes.

Credential harvesting attack One of the key targets of APT-36 is the Indian government and it targets the government users with various Kavach related themes including credential harvesting attacks. These credentials can further be re-used by the threat actor to gain access to government related infrastructure.

A domain with the name nic-updates[.]in was registered on 25th August 2022 and it impersonated the official login page of NIC (National Informatics Center).

This domain redirected to the malicious login page only when accessed from an Indian IP address, else it redirected to the legitimate official domain of NIC – nic.in

It is important to note that the phishing URL was well-crafted as it

Cymulate

hosted at the URL: hxxps://kavach.mail.nic-updates[.]in/mfid/secureLogin_showSecureLogin.action/web/

The image file – kavach.jpg in the above open directory stood out based on the file creation date. Analysts pivoted on this image file's hash, and observed that the same image was also referenced from kavach-app[.]com (a domain which Analysts previously attributed to APT-36 group).

Cymulate

Crawls Out of Crimeware...

Rhysida ransomware-as-a-service aS) group has gone from a dubious newcomer to a fully-fledged ransomware...

Running Campaign Pursues Portuguese...

The attackers can steal credentials and exfiltrate users' data and personal information, which can be...