


India: Human Rights Defenders Targeted by a Coordinated Spyware Operation

 [amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation](https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation)

Nine human rights defenders, most of whom have been fighting for the release of the Bhima Koregaon 11 through litigation, research, or activism, were unlawfully targeted with a spyware attack

This blog post is jointly written by Amnesty International and Citizen Lab. Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy at the University of Toronto.

Summary

Amnesty International and the Citizen Lab have uncovered a coordinated spyware campaign targeting at least nine human rights defenders (HRDs) in India. Eight of the nine HRDs have been calling for the release of other prominent activists, popularly known as the Bhima Koregaon 11, most of whom have been imprisoned in Maharashtra, India since 2018.

Between January and October 2019, the HRDs were targeted with emails containing malicious links. If these links were clicked, a form of commercially-manufactured Windows spyware would have been deployed, compromising the target's Windows computers, in order to monitor their actions and communications. This is a violation of their rights to freedom of expression and privacy.

At least three of the nine HRDs were also targeted with NSO Group's Pegasus spyware in 2019.

Introduction

Amnesty International and the Citizen Lab have uncovered a coordinated spyware campaign targeting at least **nine** human rights defenders (HRDs) in India. These targets include activists, lawyers, academics, and journalists.

Between January and October 2019, each of the targets were sent spearphishing emails containing malicious links that, if opened, would have installed NetWire, a commercially available spyware. A spearphishing attack is a targeted attempt to install a spyware (a malicious software) on the victim's computer or smartphone. Spearphishing is generally performed by sending very carefully crafted and personalized emails to the target, often impersonating colleagues or loved ones.

While NetWire is known to be used in cybercrime and corporate espionage, Amnesty International and the Citizen Lab believe that in this case it was used to target the HRDs because of their human rights work.

Surveillance of people based solely on their human rights work amounts to an arbitrary and unlawful attack on their privacy and violates their right to freedom of expression and other rights that are enshrined in the International Covenant on Civil and Political Rights, to which India is a state party.

Context

The targeted HRDs have been openly speaking out about human rights violations in the country. Recently, eight called for the release of 11 prominent activists arrested two years ago in relation to the protests and violence at Bhima Koregaon in Maharashtra, a state in south-west India. One of the targets is not directly linked to this case, but has been vocal in calling for the release of GN Saibaba, a disabled academic jailed in Maharashtra.

The Bhima Koregaon Case

On 31 December 2017, activists organized a public event in Bhima Koregaon, Maharashtra. The following day, violence erupted between Dalits and Hindu nationalists. Police claim that activists at the event allegedly instigated the violence through inflammatory speeches. The police allegedly found evidence of other criminal activities as well. In 2018, the Maharashtra Police arrested nine activists including Sudha Bharadwaj, Shoma Sen, Surendra Gadling, Mahesh Raut, Arun Ferreira, Sudhir Dhawale, Rona Wilson, Vernon Gonsalves and Varavara Rao. The subsequent charge sheets filed by the police accuse the HRDs of terror-related activities. In February 2020, the National Investigation Agency (NIA) took over the case from the Maharashtra police after the newly-elected Maharashtra Government raised doubts about the police investigation and signalled a probe against the officials. In March 2020, the Supreme Court of India denied anticipatory bail applications of two other activists, Gautam Navlakha and Anand Teltumbde, who were also charged in the same case. They were both arrested on 14 April 2020. The case relies almost entirely on digital evidence obtained from the arrested activists' devices. In a breach of due process, some materials found on their devices were also released to the media in an effort to smear the activists.

The arrest of the eleven HRDs is an egregious example of how Indian authorities are clamping down on dissent and activism. These activists have been charged under various penal provisions and the draconian Unlawful Activities (Prevention) Act (UAPA), an anti-terror law that violates several international human rights standards and circumvents fair trial guarantees. It is also routinely used to intimidate HRDs, journalists, activists and students through arbitrary arrests and prolonged detention. These 11 activists are currently imprisoned and rights groups, including Amnesty International India, have demanded their release.

The attempts at unlawful surveillance outlined in this blog are not the first time that activists and HRDs have been targeted with malware in India. In October 2019, Facebook's WhatsApp revealed that NSO Group, a surveillance tool vendor, had exploited a zero-day vulnerability on their platform to target 1400 individuals earlier in the year. A zero-day vulnerability is a security flaw in software which is unknown to the vendor or developer. In collaboration with Citizen Lab, WhatsApp revealed that more than 100 of those targeted were HRDs, activists, journalists, across numerous countries and notified them of the breach. Subsequent reports revealed that at least 22 of the 100 were activists, lawyers, and scholars, including many HRDs who have been involved in advocating for the release of the 11 activists. NSO Group says that it sells its products only to "government intelligence and law enforcement agencies".

Targeted Campaign against HRDs demanding the release of the Bhima Koregaon 11

The spyware campaign revealed in this blog targeted lawyers and activists **Nihalsing B Rathod, Degree Prasad Chouhan, Yug Mohit Choudhary, and Ragini Ahuja**; academics **Partho Sarothi Ray** and **PK Vijayan**, a journalist who prefers to stay anonymous, and a human rights collective – **Jagdarpur Legal Aid Group (JAGLAG)**, received malicious e-mails on the group's official ID, which is accessed by all of its members, including lawyer **Shalini Gera**. Another JAGLAG member, **Isha Khandelwal** also received malicious emails on her personal account. All the people mentioned consented to be named in this blog.

- **Nihalsing B Rathod** is a human rights lawyer based in Maharashtra. He has worked closely with the imprisoned lawyer Surendra Gadling as a junior lawyer. Crucially, he is one of the leading lawyers representing one of the 11 imprisoned HRDs in their legal proceedings.
- **Isha Khandelwal** is a lawyer associated with **JAGLAG**, a Chattisgarh-based lawyers collective which provides legal aid to the Adivasi/indigenous and other marginalised communities. The group's primary email, which was targeted, is also accessed by lawyer **Shalini Gera**. They are also involved in the legal defense of the HRDs in the same case.
- **Degree Prasad Chouhan** is a Dalit HRD who has worked closely with Sudha Bharadwaj in the past. Degree has been documenting and campaigning against land dispossession and forced evictions of indigenous communities in India, which have been carried out by coal companies and governments.
- **Partho Sarothi Ray** is a Kolkata-based activist and academic, who has been a vocal critic of rights violations in the country. He has also been a member of a collective called Persecuted Prisoners' Solidarity Committee, and has spoken out openly against the imprisonment of these 11 activists.
- **Yug Mohit Chaudhry** and **Ragini Ahuja** are criminal lawyers based in Mumbai. Their main area of work include litigating death penalty and civil liberties cases. They represent two of the 11 imprisoned activists in the legal proceedings.

- A journalist based in Maharashtra, who wishes to remain anonymous was also targeted. The journalist has been closely reporting on the Bhima Koregaon case.
- Finally, **PK Vijayan** is a Delhi-based academic. He is not directly linked to the campaign for the release of the 11 HRDs, but is known to have campaigned for the release of GN Saibaba, a disabled academic who remains imprisoned in Maharashtra. Saibaba has been convicted under the draconian UAPA.

While the spyware campaign detailed in this blog has no known links to NSO Group, three of the nine HRDs targeted - Shalini Gera (from JAGLAG), Nihal Singh Rathod, and Degree Prasad Chouhan- were targeted using NSO Group's surveillance tools. Anand Teltumbde, who is one of the 11 charged and imprisoned in the Bhima Koregaon incident, was also targeted using NSO Group's tools. That some of these individuals were targeted multiple times shows that there is a disturbing pattern of spyware attacks against HRDs involved in the Bhima Koregaon case.

A Campaign of Malicious Emails

During this investigation, we identified 12 spearphishing emails sent between January and October 2019 targeting the nine activists.

A spearphishing attack is an attempt to install spyware (a malicious software) on the victim's computer or smartphone by sending very carefully crafted and personalized emails to the target, often impersonating colleagues or loved ones. In a successful attack, computers or mobile devices may, in essence, become wiretaps, revealing confidential and intimate conversations and interactions but nullifying the possibility of privacy or confidentiality. Besides this direct effect, the secretive and ubiquitous nature of these attacks means that the victims never know for certain if they are being targeted or have unwittingly downloaded some kind of spyware. The consequence is that they begin to fear that every communication poses a threat, which can be highly disruptive to trust and collaboration.

Spearphishing Emails

One of the spearphishing emails was sent from an email ID impersonating the name of an activist that may be known by the targets. Other spearphishing emails came from the email IDs pretending to be journalists or masquerading as officials from local courts.

From Muskaan Sinha <sinhamuskaan04@gmail.com> ☆	↩ Reply	↩ Reply All ▾	➔ Forward	More ▾
Subject JAGLAG to be Blacklisted Over Irregularities	10/11/19, 12:58 PM			
To [REDACTED] <> ☆				

UHM Initiates Process to Blacklist JAGLAG Under New UAPA

Muskaan Sinha
Associate Editor, IBC24

Email sent to JAGLAG by someone pretending to work for IBC24 in October 2019

All these spearphishing emails included a malicious link to a file hosted on Firefox Send, a free and secure file sharing platform developed by Mozilla. We suspect that this technique was used to avoid detection by e-mail spam and malware filters, as a malicious file sent in such a way cannot be analyzed by security solutions used by email providers.

From: **Jennifer Gonzales** <jennifergonzales789@gmail.com>
Date: Sat, 26 Oct, 2019, 15:38
Subject: Reminder Summons For Rioting Case
To: <[REDACTED]>

CrPC 146 Indictment Summary

Jennifer Gonzales
Special Public Prosecutor, Jagdalpur

Email sent to a Human Rights Defender in October 2019 masquerading as a court summons

A detailed list of emails is available in **Appendix 1**.

Commercial Off-the-Shelf Spyware: NetWire

NetWire is a commercially available spyware reportedly used for cyber-criminality and corporate espionage since at least 2014. It has been analyzed in depth by several security companies including the Computer Incident Response Center Luxembourg and Fortinet, who have shown that NetWire exhibits classic spyware features such as stealing credentials, audio recordings, logging keystrokes and more.

Screenshot of the website selling Netwire (Retrieved in December 2019)

The spearphishing emails targeting these nine HRDs attempted to deliver NetWire by attaching what looked like a PDF document but which was actually malicious Windows programs that, when opened, would install NetWire on the HRD's device. The disguise of these supposed PDFs included opening a decoy, real PDF when clicked. This tactic was clearly intended to trick the targeted HRD into believing that no infection had taken place. Additionally, this attack takes advantage of numerous other obfuscation techniques often abused by the surveillance industry to make NetWire more challenging to find and analyze (see: **Appendix 1** for more information).

Conclusion

A coordinated spyware campaign targeted prominent HRDs, most of whom were vocal against the arbitrary and prolonged imprisonment of the Bhima Koregaon 11. The spearphishing emails and spyware suggest that this is not a cyber-crime attack, but a spyware campaign trying to compromise devices of HRDs. If successful it would have enabled the attackers, to monitor the HRDs actions and communications and is therefore a violation of their rights to freedom of expression and privacy. This spyware campaign is very concerning in the context of an already perilous situation for HRDs in India where surveillance is used along with threats, imprisonment and smear campaigns against activists to shrink the space for civil society.

Our investigation was not able to conclusively attribute the attack to a particular group with high confidence. However, it is not the first time that activists and journalists in India have been targeted using malware intended to put them under surveillance. Three of the HRDs in this incident were targeted earlier in 2019 with NSO Group's Pegasus spyware, a commercial product only sold to government entities. This new campaign confirms that there is a pattern of digital attacks against HRDs supporting the imprisoned

Bhima Koregaon activists. This pattern underscores the necessity of India fulfilling its obligation to provide a remedy for these abuses by conducting a full, independent and impartial investigation into these attacks, including by determining whether there are links between this spyware campaign and specific government agencies.

Targeting people solely for exercising their right to peaceful dissent amounts to an arbitrary or unlawful attack on their privacy and violates their right to freedom of expression. States have an obligation to protect human rights by ensuring that HRDs are protected from unlawful surveillance.

Recommendations

To Indian Authorities:

Conduct an independent, impartial, and transparent investigation into the unlawful targeted surveillance of the nine human rights defenders, including determining whether there are links between this spyware campaign and any specific government agencies

Ensure that all surveillance meets the tests of legality, necessity, and proportionality as enshrined in international human rights standards and affirmed in the Supreme Court of India's landmark judgement of *KS Puttaswamy v. Union of India*.

Ensure adequate and effective legal remedies are available for people to challenge violations of their human rights linked to surveillance

Review Section 69 of the Information Technology Act and the 2018 order of the Ministry of Home Affairs that allows government agencies to intercept, monitor and decrypt information without any judicial oversight and other procedural safeguards.

Implement domestic legislation that imposes limits on digital surveillance, ensuring that:

- Surveillance is governed by precise and publicly accessible laws
 - Surveillance is only against specified persons, authorized by a competent, independent and impartial judicial body with limitations on time, manner, place and scope of surveillance
 - Authorized digital surveillance is subject to detailed record keeping, in accordance with documented legal processes for a warrant, and targets are notified as soon as practicable without jeopardizing the purpose of surveillance
- Ensure that all digital surveillance is subject to public oversight mechanisms, including:
 - Public notice and consultation for new surveillance purchases
 - An approval process
 - Regular public reporting

- Ensure that the Personal Data Protection Bill, 2019 is *not* enacted in its current form and is brought in line with international human rights standards.

Appendix 1: Technical Details

We retrieved 9 different malware binaries from the links in the original emails. These samples use several layers of obfuscation before delivering a NetWire sample.

I. Emails and Samples

We identified 12 emails targeting Human Rights Defenders between January and October 2019:

Date	Sender	Subject
Jan 16, 2019	jagdish.meshraam[@]gmail.com	DUSU activist Sujata files harassment complaint
May 13, 2019	drsnehapatil64[@]gmail.com	IPC 120B [REDACTED] (PSSC) Accused of Criminal Conspiracy
Sept 10, 2019	payalshastri79[@]gmail.com	Pune SHO Sexually Abuse Journalists
October 6, 2019	sinhamuskaano4[@]gmail.com	SUMMONS NOTICE JAGDALPUR ARSON CASE
October 6, 2019	sinhamuskaano4[@]gmail.com	SUMMONS NOTICE IN ARSON CASE JAGDALPUR
October 11, 2019	sinhamuskaano4[@]gmail.com	JAGLAG to be Blacklisted Over Irregularities
October 26, 2019	jennifergonzales789[@]gmail.com	Rioting Case Summons Reminder
October 26, 2019	jennifergonzales789[@]gmail.com	Reminder Summons For Rioting Case
October 26, 2019	jennifergonzales789[@]gmail.com	Reminder Summons For Rioting Case

October 26, 2019	jennifergonzales789[@] gmail.com	Reminder Summons For Rioting Case
October 26, 2019	jennifergonzales789[@] gmail.com	Summons Notice For Rioting Case Cr.24/2018
October 28, 2019	jennifergonzales789[@] gmail.com	Summons Notice For Rioting Case Cr.24/2018

We identified ten different malicious samples from 10 different emails shared with us:

File Name	SHA 256 Hash
Com-plaints_from_Ragini_Markande_Harrassment_letter.exe	e3dea449bf74434ee1c9cdc04ca68b8f3c9bac357768e07d-f303433f257d3b9a
Rioting Case Indictment Summary.exe	21d24e08889f75461a7ce6f21fc612a701bca35da1a218cf3cd-d6e23f613bb4d
Pune SHO Sexual Abuse Summary.exe	16b5c74f-b55f52ae0ae4328f65b2bf3bbe3e5ee34268c1d32a247a0a1d-fa3186
Vijayan Rioting Case Indictment Summary.exe	5a4aca57541954195953066a4be96df-b19776ba099d72f8f1d3677581594606e
Detonators_planted_Lawyers_house.exe	11cef331557eb693e718d27b6a7211a98d3982117a03ec1491d-b8098ea3cecc00
55_maoists_killed_by_c60_commands.exe	88b92d985b7d616c93c391731c1e4a6d3c8323fd-cbf31cfc4d340e27253913a7
Reminder Notice SP North Goa Ponda Division.exe	b1b6e133aa320669c772ec7e5fd6fbe4cb3edca13ad5351f14d-f3c1f13939d09
mail2.exe	ea5f37e1feab670171963aa83b235c772202b2d4bb7289d-d45302c3851dbd6f9

mail3.exe	de302a61e5f07boe65753355d44d22181a2742ac3a92aa058 bdcd00cc4dab788
SUMMONS NOTICE JAGDALPUR ARSON CASE.exe	31a3e3abao3b553dof23f1obo6ade30ae053cd667a8c- c966of310705ee471b68

We have also identified three other similar samples uploaded on VirusTotal that we attribute to the same campaign:

File Name SHA 256 Hash

“Supreme Court Or- der Ban Sanatan Sanstha.exe “	b09ca9d48a0455ed5e02a56aabeb397c41fb63320244719749e0741da72e79c4
---	--

[unknown]	095ec879f323a0a3eceb97013125880d49ac701eef568e3b01ofdddb1333941f
-----------	--

[unknown]	ac4d5d938009fd44b2f7587986862ab2278887a17d32f748278445b625b3efd9
-----------	--

II. Obfuscation and payload delivery

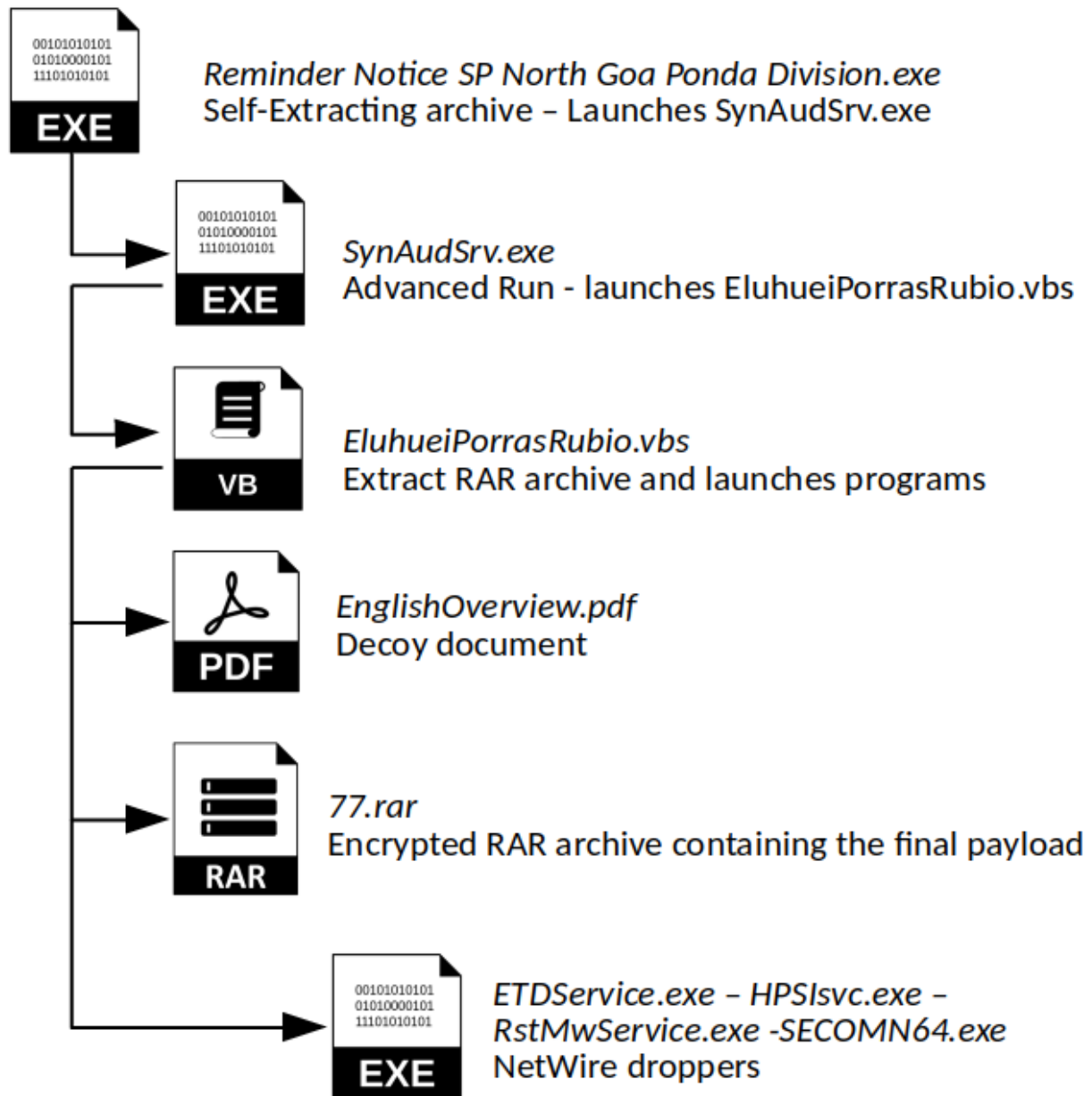
Variant 1

1. SFX archive extracts AndvancedRun/VBS stage.

1. AdvancedRun launches VBS script.

1. VBS script extracts RAR archive containing 2nd level NetWire droppers. Task Scheduler entries created for 3 2nd level NetWire droppers. Launches decoy PDF.

In this variant, payloads are only launched by Task Scheduler.



Delivery of the first payload variant

Variant 2

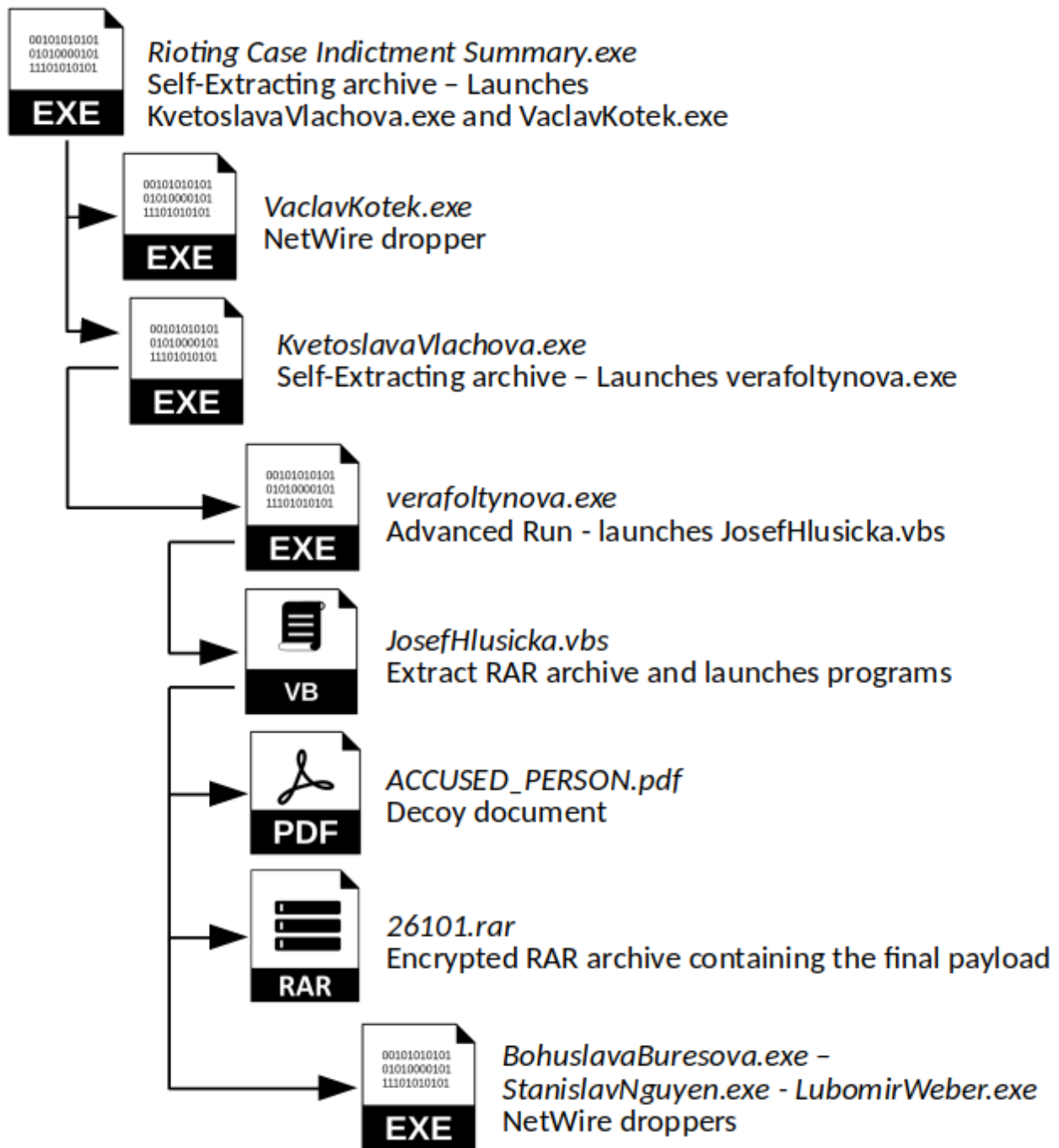
This second variant was modified to add an additional execution of the NetWire payload in parallel to those launched by task scheduler, and in order to add a layer in between with validly signed EXEs, likely to thwart antivirus detection heuristics.

1. SFX archive extracts two payloads. A SFX archive and a NetWire dropper.

1. Launch 1st NetWire dropper. Launch second SFX archive, which extracts AdvancedRun/VBS stage.

1. AdvancedRun launches VBS script.

1. VBS script extracts RAR archive containing additional NetWire droppers. Task Scheduler entries created for 3 new NetWire droppers. Launches decoy PDF.



Delivery of the second payload variant

The Stage 1 SFX archive contains random README files, GPL licenses and even RFCs. Launches both the payloads contained.

The 1st level and 2nd level NetWire droppers all launch the same payload, either by launching and hollowing *dllhost.exe*, or launching and hollowing *rundll32.exe*, or by launching and injecting a copy of themselves.

Bypassing Security Protections With Large Files

It is the first time we have observed large files being used as a trick to bypass security protections. As described earlier, the first dropper is a Self-Extracting RAR archive that extracts several files, including either the dropper or another self-extracting RAR archive running the final dropper. In almost all cases analyzed here, the droppers were very large files, between 50MB and 300MB.

These files mostly contain the byte 00 that is efficiently compressed by the RAR format, making the initial file quite small. As many security solutions include a file size limitation to avoid overloading the detection system with heavy files, it is likely that this trick would prevent some solutions from detecting these files as malicious.

Digital Signatures

We identified five samples with valid digital signatures for three different UK-registered companies. We contacted the owner of one of these companies who told us that he was never involved in signing any software. Further investigation led us to question the involvement of the companies for which they were issued. It appears that this may be part of a pattern of identity theft of small companies in order to issue signatures for malicious software. A recent study has shown that since 2017, this underground market for code-signing certificates has substantially increased.

Final Payload: NetWire

The final payload launched in memory by these samples is a NetWire sample communicating with the dynamic DNS domain `researchplanet.zapto[.]org`.

Netwire is a commercial malware known since 2012, that has been analyzed in depth several times. It has been used mostly in cyber-criminal activities, but has also been used several times in cyber-espionage operations for instance by the Iranian attributed group APT33 in 2017. It is today sold online for \$15 a month by a company called World Wired Labs.

III. Network Analysis

Network traffic appears to be similar in structure to typical NetWire C&C communications:

```

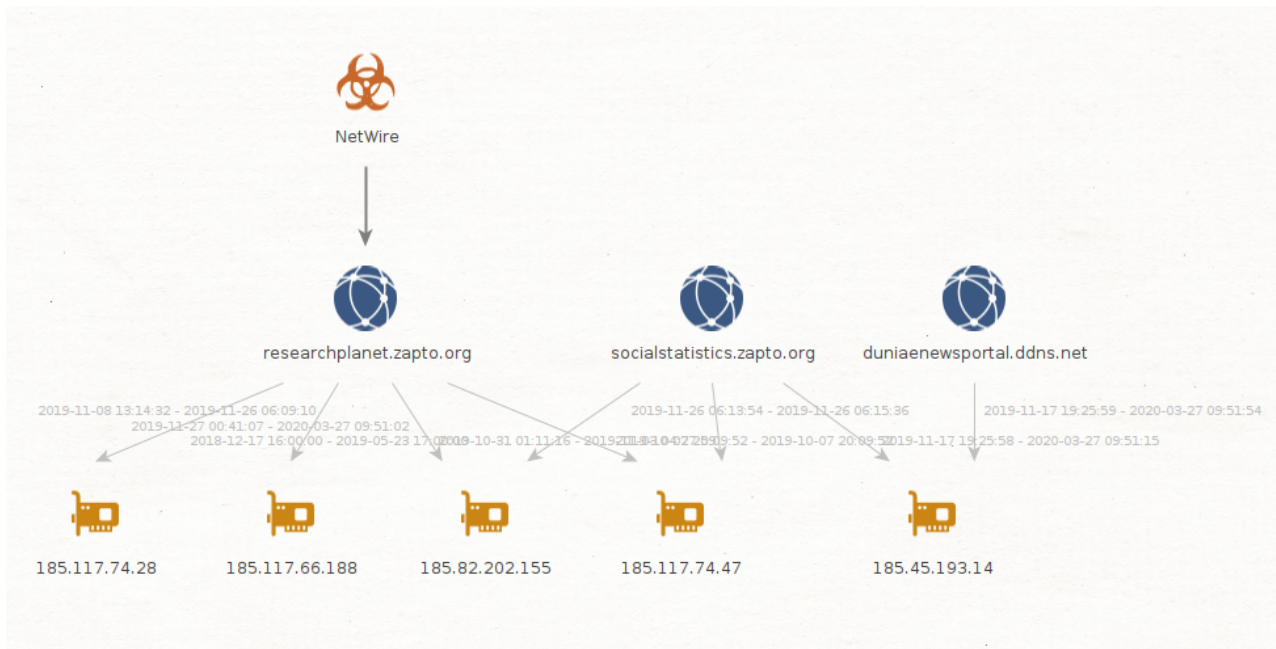
00000000 41 00 00 00 99 f6 e8 80 fc 6c 5a 30 9f c4 58 e6 A..... .1Z0..X.
00000010 80 90 93 b1 d0 50 ac 61 be 51 b8 ea f2 c8 ca b5 .....P.a .Q.....
00000020 73 50 b9 40 da 68 e8 48 8b be 6c cc d4 c1 a0 c0 sP.@.h.H ..1.....
00000030 fe 87 d8 58 b4 73 ab b9 95 24 0f f6 d8 4e 54 58 ...X.s.. .$...NTX
00000040 f5 04 97 1c 53 ....S
00000000 3f 00 00 00 9b 18 55 1a e5 8b a8 3c e1 a9 22 4c ?......U. ...<.."L
00000010 26 01 95 15 e4 03 c9 2c d2 62 d3 c9 e5 2c 01 ee &....., .b....,..
00000020 a2 2f 47 c7 70 eb 0c 35 2c 45 75 f8 d7 98 0e ce ./G.p..5 ,Eu.....
00000030 f9 fb 50 33 54 df 68 77 7b 5d 15 a3 72 05 50 93 ..P3T.hw {}..r.P.
00000040 51 15 42 Q.B
00000045 19 00 00 00 9b c9 ec 00 46 d0 e4 a2 45 3d eb 1c ..... F...E=..
00000055 f1 9e 1a 2d 7a c5 7e be 34 3a a9 9e cc ...-z.~. 4:...
00000043 01 00 00 00 97 .....
00000062 01 00 00 00 97 .....
00000048 01 00 00 00 97 .....
00000067 01 00 00 00 97 .....
0000004D 01 00 00 00 97 .....
0000006C 01 00 00 00 97 .....
00000052 01 00 00 00 97 .....
00000071 01 00 00 00 97 .....
00000057 01 00 00 00 97 .....
00000076 01 00 00 00 97 .....
0000005C 01 00 00 00 97 .....
0000007B 01 00 00 00 97 .....
00000061 01 00 00 00 97 .....
00000080 01 00 00 00 97 .....
00000066 01 00 00 00 97 .....
00000085 01 00 00 00 97 .....
0000006B 01 00 00 00 97 .....
0000008A 01 00 00 00 97 .....
00000070 01 00 00 00 a1 .....

```

All the samples identified communicate with the dynamic DNS domain researchplanet.zapto[.]org on port 1810.

IV. Infrastructure

All the samples identified in this attack used the domain *researchplanet.zapto[.]org* on port 1810 as Command & Control server. This domain is a dynamic DNS domain managed by the company NoIP, and was first seen as used by RiskIQ in mid-December 2018. This domain has used multiple IPs over this year according to several passive DNS databases, we have confirmed the utilisation of the IP addresses 185.117.66[.]188 (Edelaraudtee Infrastrukturi AS) and 185.82.202[.]155 (Host Sailors) as NetWire C2 servers receiving connections from compromised systems.



The dynamic DNS domain `socialstatistics.zapto[.]org` is very likely linked to this campaign, as it was connected with several IPs also used by `researchplanet.zapto[.]org` in the end of 2019. During the investigation, we confirmed that the IP address used with this domain in December 2019, `185.45.193.14` (Host Sailor) was also running a NetWire server on ports 7778 and 50070, confirming the link with this campaign.

Finally, we consider a third dynamic DNS domain, `duniaenewsportal.ddns[.]net` to be linked with this campaign, as it shared the same IP address `185.45.193[.]14` (Host Sailor). This domain could have been created based on the name of Dunya News, an Urdu language television channel from Pakistan.

Appendix 2: Indicators of Compromise

You can find the full list of indicators of compromise here
<https://github.com/AmnestyTech/investigations>

Following are the domain names associated with this campaign:

`researchplanet.zapto[.]org`

`socialstatistics.zapto[.]org`

`duniaenewsportal.ddns[.]net`

The IP address hosting the malicious infrastructure is:

`185.82.202[.]155`

`185.117.66[.]188`

`185.117.74[.]47`

185.117.74[.]28

185.45.193[.]14

Following are the email addresses used in spearphishing emails:

jagdish.meshraam[.]gmail.com

drsnehapatil64[.]gmail.com

sinhamuskaan04[.]gmail.com

jennifergonzales789[.]gmail.com

payalshastri79[.]gmail.com