Charged by an Elephant
An APT Fabricating Evidence to Throw You In Jail

SentinelLABS

Tom Hegel
Senior Threat Researcher
tomhegel

Juan Andres Guerrero-Saade
Senior Director of SentinelLabs
juanandres_gs

MOTHERBOARD
TECH BY VICE

Turkish Journalist Jailed for Terrorism Was Framed, Forensics Report Shows

New analysis of Barış Pehlivan's computer finds a very rare, targeted malware called Ahtapot. It only gets stranger from there.

AF By Andrada Fiscutean

Odatv:

A Case Study in Digital Forensics and Sophisticated Evidence Tampering

Arsenal is currently developing a detailed case study related to our analysis of computers essential to the Odatv case in Turkey. Odatv is a secular news organization founded in 2007 with a reputation for being critical of Turkey's government and the Gülen Movement. Prosecutors in this case have alleged that Odatv journalists (and others) were members of the Ergenekon terrorist organization, based on documents recovered from two particular computers. We have found that those computers, used by Odatv journalists Barış Pehlivan and Müyesser Yıldız, were attacked in a relentless (and fascinating) fashion - ultimately resulting in placement of the incriminating documents just prior to seizure by the Turkish National Police. We will be sharing our findings as we are able on this page and perhaps even open sourcing some aspects of our analysis. We will announce updates on Twitter @ArsenalArmed.

April 12 2017 13:38:00

Court acquits all 13 suspects in Turkey's controversial OdaTV case

ISTANBUL

An Istanbul court on April 12 ordered the acquittal of 13 suspects, including journalists and writers, charged with membership of the Ergenekon organization in the OdaTV case.

SentinelLABS

EGOMANIAC: AN UNSCRUPULOUS TURKISH-NEXUS THREAT ACTOR

Hacking Team Customer in Turkey Was Arrested for Spying on Police Colleagues [or: The Spy Story That Spun a Tangled Web]

An investigation that weaves a winding tale between police in Ankara who were charged with spying on their own colleagues... and the purchase of Hacking Team's surveillance software.

Kim Zetter
Sep 8, 2021

WORLD

Indian activist charged with terrorism was targeted by hackers linked to prominent cyber espionage attacks, new report finds

By Niha Masih and Gerry Shih

February 10, 2022 at 12:01 a.m. EST

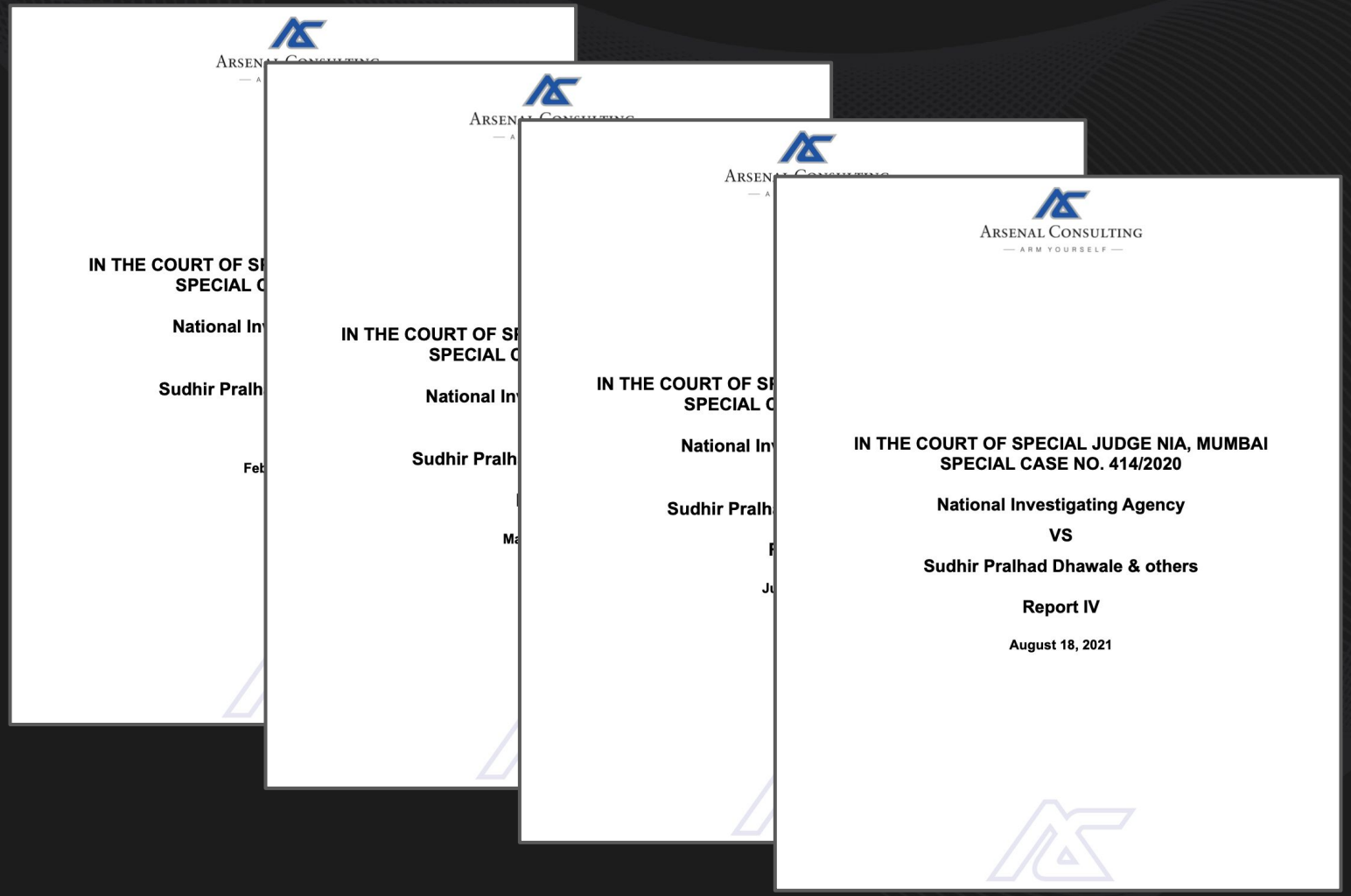
MOST READ WORL

The Arsenal Reports: The rise of targeted surveillance in India

Evidence found on a second Indian activist's computer was planted, report says

By Niha Masih and Joanna Slater

July 6, 2021 at 6:30 a.m. EDT


ARSENAL CONSULTING
ARM YOURSELF
IN THE COURT OF SPECIAL JUDGE NIA, MUMBAI
SPECIAL CASE NO. 414/2020
National Investigating Agency
VS
Sudhir Pralhad Dhawale & others
Report IV
August 18, 2021

From: [redacted]@gmail.com>
Sent: 4/13/2013 10:35:24 PM +0530
To: [redacted]
Subject: Re: MumbaiHigh Court Judgement about ScSt&Backward Caste 5 th April 2013
Attachments: BackwardCaste_judgement_mumbaiHighCourt5april2013.exe

---------- Forwarded message ----------

On 13 Apr 2556 BE, at 11:27, [redacted]@gmail.com> wrote:
please find pdf attachment file about mumbai high court judgement in favour of sc st students of maharashtra.

[redacted]
[redacted]@gmail.com
[redacted]


Executable Attachment
Fake Document Executables
Public Exploit Docs
Maldoc + Mobile Trojan
Password Protected Archives
Links to File Download
Large .rar Archives
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022

NetWire RAT → Remote Attacker Sessions → Planted Evidence

Full Path on Secondary Volume	Created (IST)	Source	Attacker Session (IST)
\Rbackup\Ltr_2312_to_CC.pdf	12/25/2017 22:31:01	NetWire/RAR	12/25/2017 22:28:48 - 12/25/2017 22:32:31
\Rbackup\Ltr_2612_to_CC.pdf	12/27/2017 21:30:37	NetWire/RAR	12/27/2017 21:23:45 - 12/27/2017 21:31:43
\Rbackup\Ltr_from_Com.M_022018.pdf	01/06/2018 02:05:39	NetWire/RAR	01/06/2018 02:03:49 - 01/06/2018 02:06:43
\Rbackup\CC_letter - 08Jun.pdf	01/21/2018 14:16:05	NetWire/RAR	01/21/2018 14:13:18 - 01/21/2018 14:34:51
\Rbackup\Ltr_2_SG-27.1.2018.pdf	01/28/2018 19:14:01	NetWire/RAR	01/28/2018 19:09:30 - 01/28/2018 19:18:12
\Rbackup\Ltr_2_Anand_E.pdf	04/06/2018 00:00:57	NetWire/Direct	04/05/2018 23:59:38 - 04/06/2018 00:01:07

Planted Modi Assassination Plot

Ltr_1804_to_CC.pdf

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.

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

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

the Defense and Release of G N

pol. prisoners. Com. Ashok B, Amit

ngs of CRPP EC. It will facilitate

Odisha, CHH. On the other side

ssible ways. He has been studying

everal 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

e by now you have

4's with 400000 rounds.

party. Several leaders

gly. We are working to

minorities across the

igenous adivasis. In spite

P govt in more than 15

on all fronts. Greater

n 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

Planted ‘Domestic Chaos’ Plans Document

Ltr_2_Anand_E.pdf

issues. We have also sent funds for your upcoming (9-10 April) Human Rights convention at Paris. International campaigns can give more traction to domestic chaos. Frequent protests and chaos will gradually lead to break down of law and order, and this will have significant political ramifications in the coming months. Please coordinate with our friends in America and France, Com. Anupama Rao and

11 Days Before Search and Seizure

Jailed Jesuit human rights activist dies in India

By Inés San Martín
Jul 5, 2021 | Rome Bureau Chief

Share

Jesuit Father Stan Swamy in an undated photo. (Credit: Jesuit Conference of South Asia.)

ROME – An 84-year-old Jesuit priest who had been imprisoned in India since October 2020 died Monday morning in a hospital in Mumbai where he had been since May. He had been placed on a ventilator support on Sunday.

Indian State-Nexus Activity

ModifiedElephant

Long Term Phishing (2012+)

Email Account Compromise (2018)

SideWinder

Rare Phishing Attempts (2013-2014)

Pegasus Infected iPhone (2017-2018)

NSO Group

OPERATION HANGOVER

Unveiling an Indian Cyberattack Infrastructure

May 2013

Snorre Fagerland, Morten Kråkvik, and Jonathan Camp
Norman Shark AS

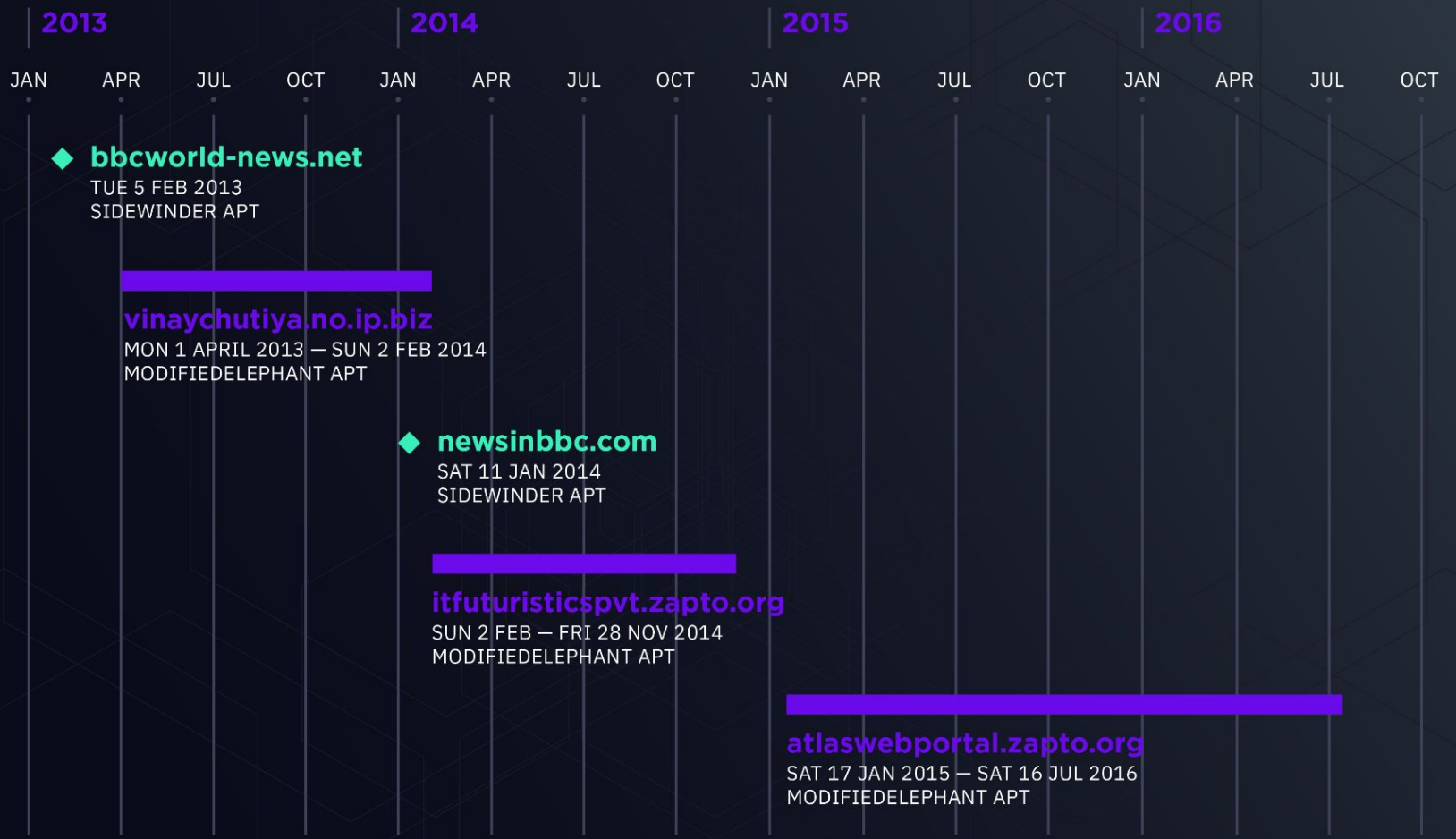
Ned Moran
Shadowserver Foundation

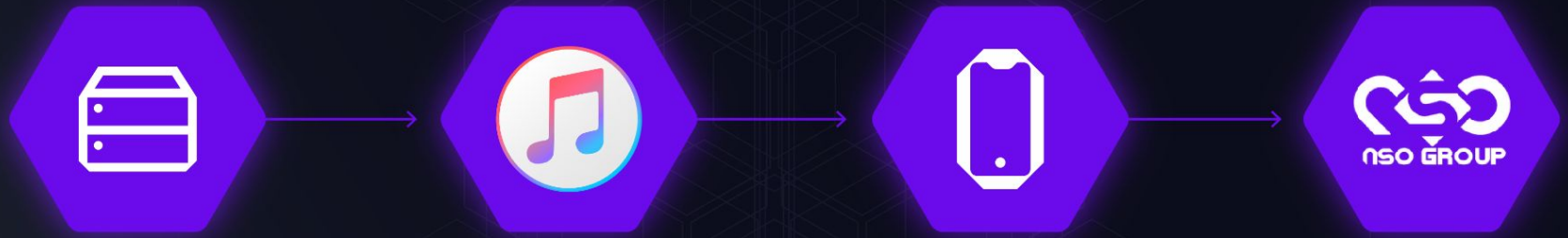
Part of a PDF decoy from one of the malicious installers (md5 06e80767048f3edefc2dea301924346c).

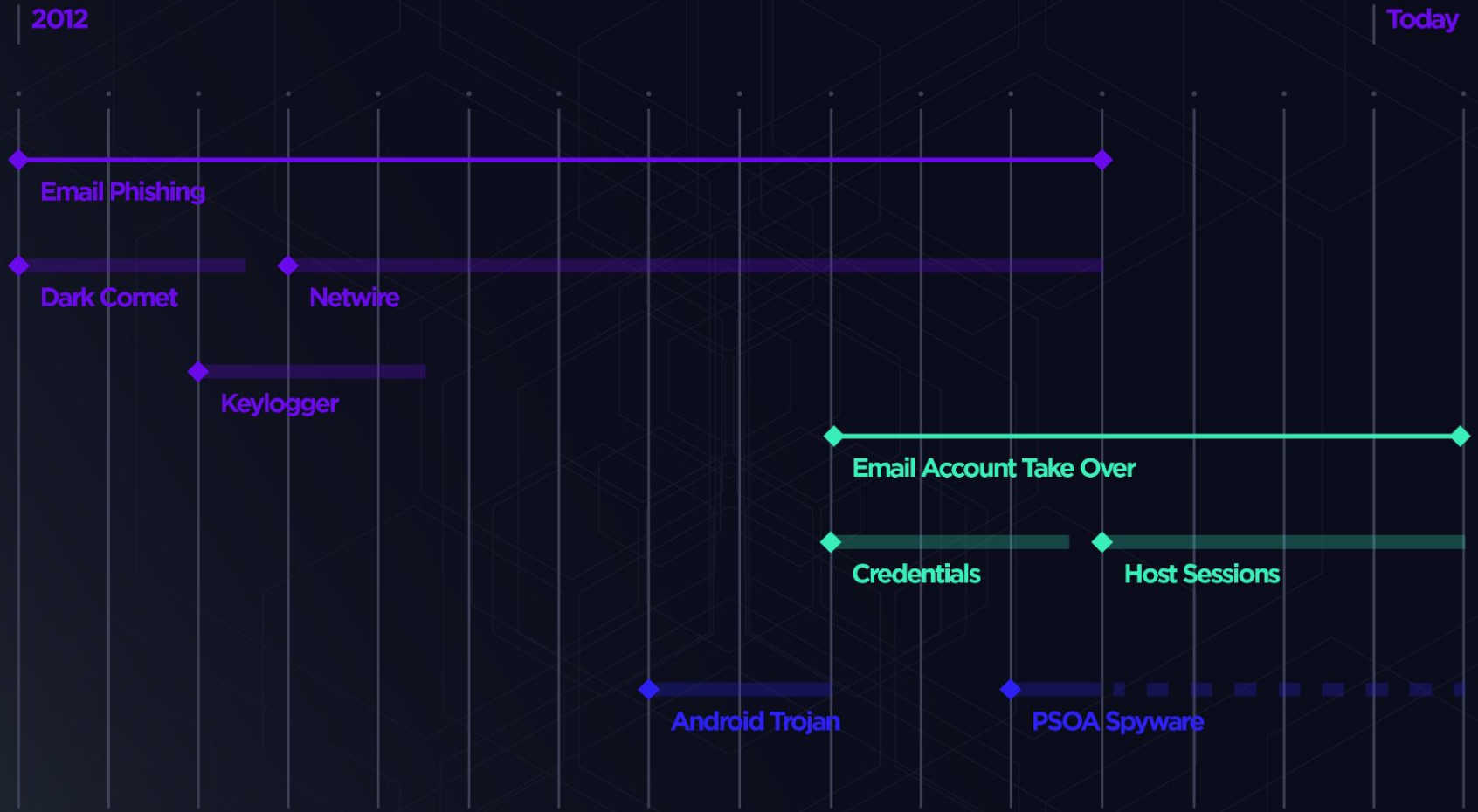
A Global Perspective of the SideWinder APT

January 13, 2021 | Tom Hegel

AT&T Alien Labs has conducted an investigation on the adversary group publicly known as SideWinder in order to historically document its highly active campaigns and identify a more complete picture of targets, motivations, and objectives. Through our investigation, we have uncovered a collection of activity targeting government and business throughout South Asia and East Asia spanning many years. Our findings are primarily focused on activity since 2017, however the group has been reportedly operating since at least 2012.


2013
2014
2015
2016
JAN
APR
JUL
OCT
JAN
APR
JUL
OCT
JAN
APR
JUL
OCT
JAN
APR
JUL
OCT
bbcworld-news.net
TUE 5 FEB 2013
SIDEWINDER APT
vinaychutiya.no.ip.biz
MON 1 APRIL 2013 — SUN 2 FEB 2014
MODIFIEDELEPHANT APT
newsinbbc.com
SAT 11 JAN 2014
SIDEWINDER APT
itfuturisticspvt.zapto.org
SUN 2 FEB — FRI 28 NOV 2014
MODIFIEDELEPHANT APT
atlaswebportal.zapto.org
SAT 17 JAN 2015 — SAT 16 JUL 2016
MODIFIEDELEPHANT APT


NSO GROUP

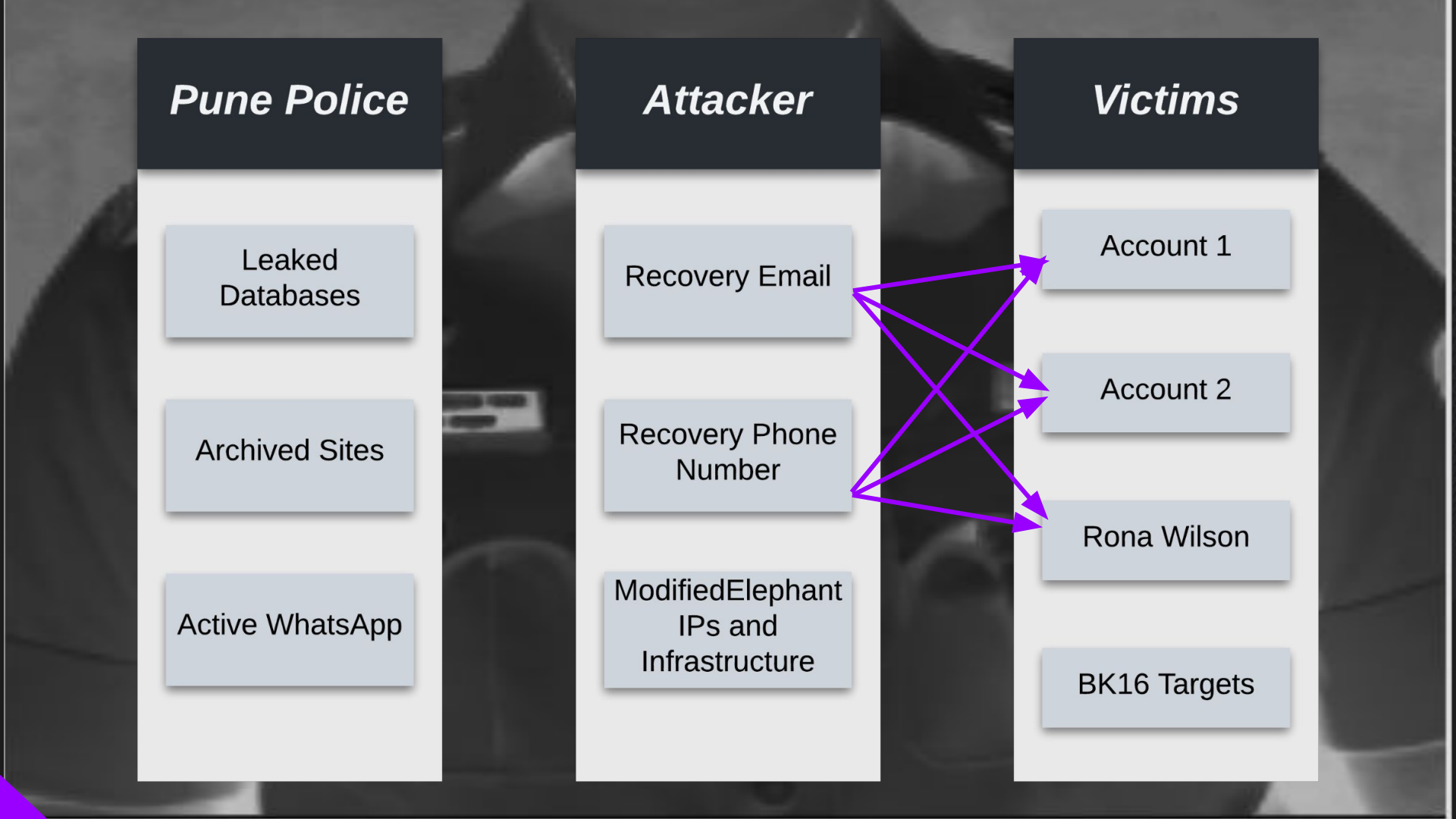

2012
Today
Email Phishing
Dark Comet
Netwire
Keylogger
Email Account Take Over
Credentials
Host Sessions
Android Trojan
PSOA Spyware

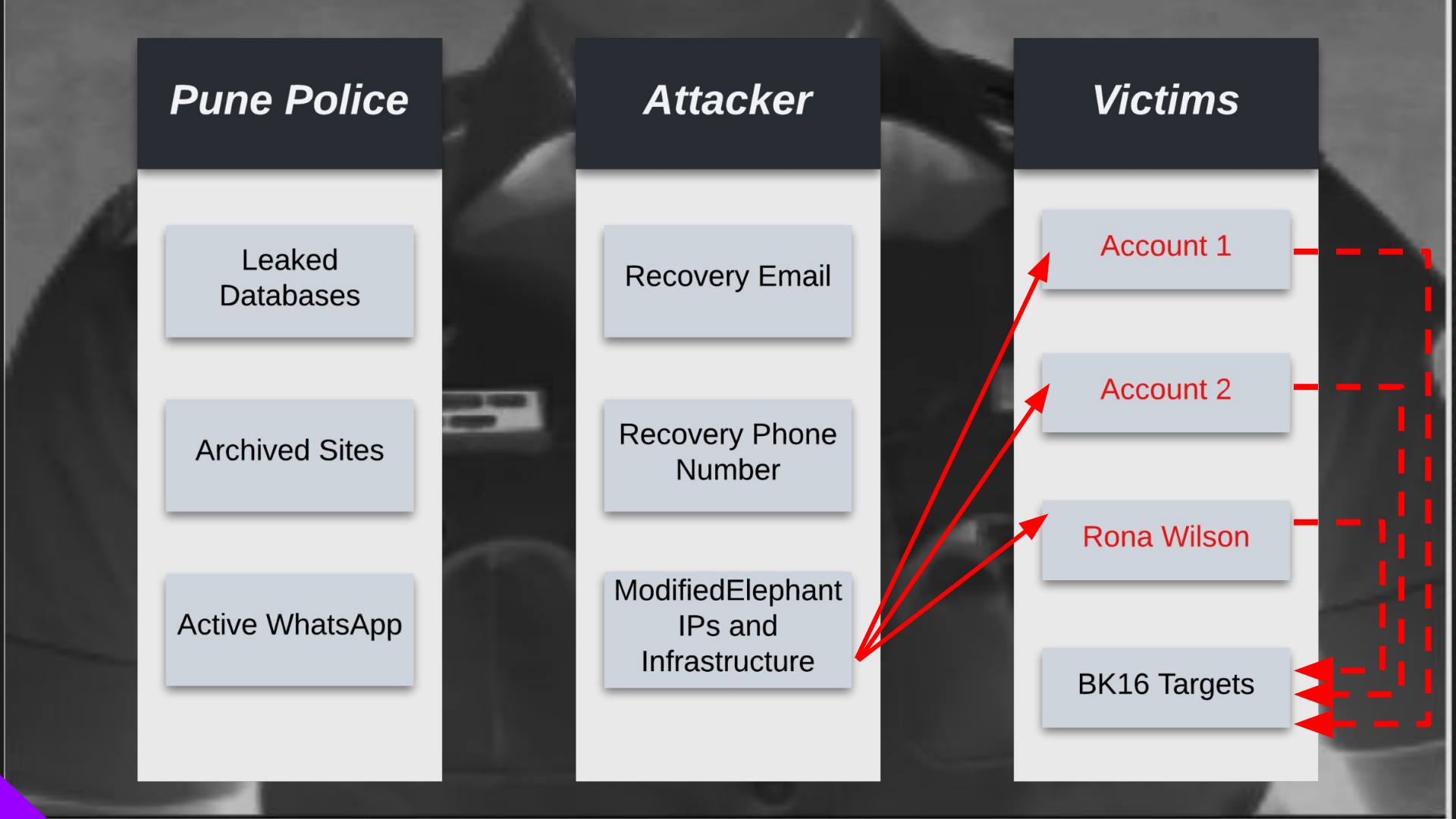
ANDY GREENBERG SECURITY JUN 16, 2022 7:00 AM

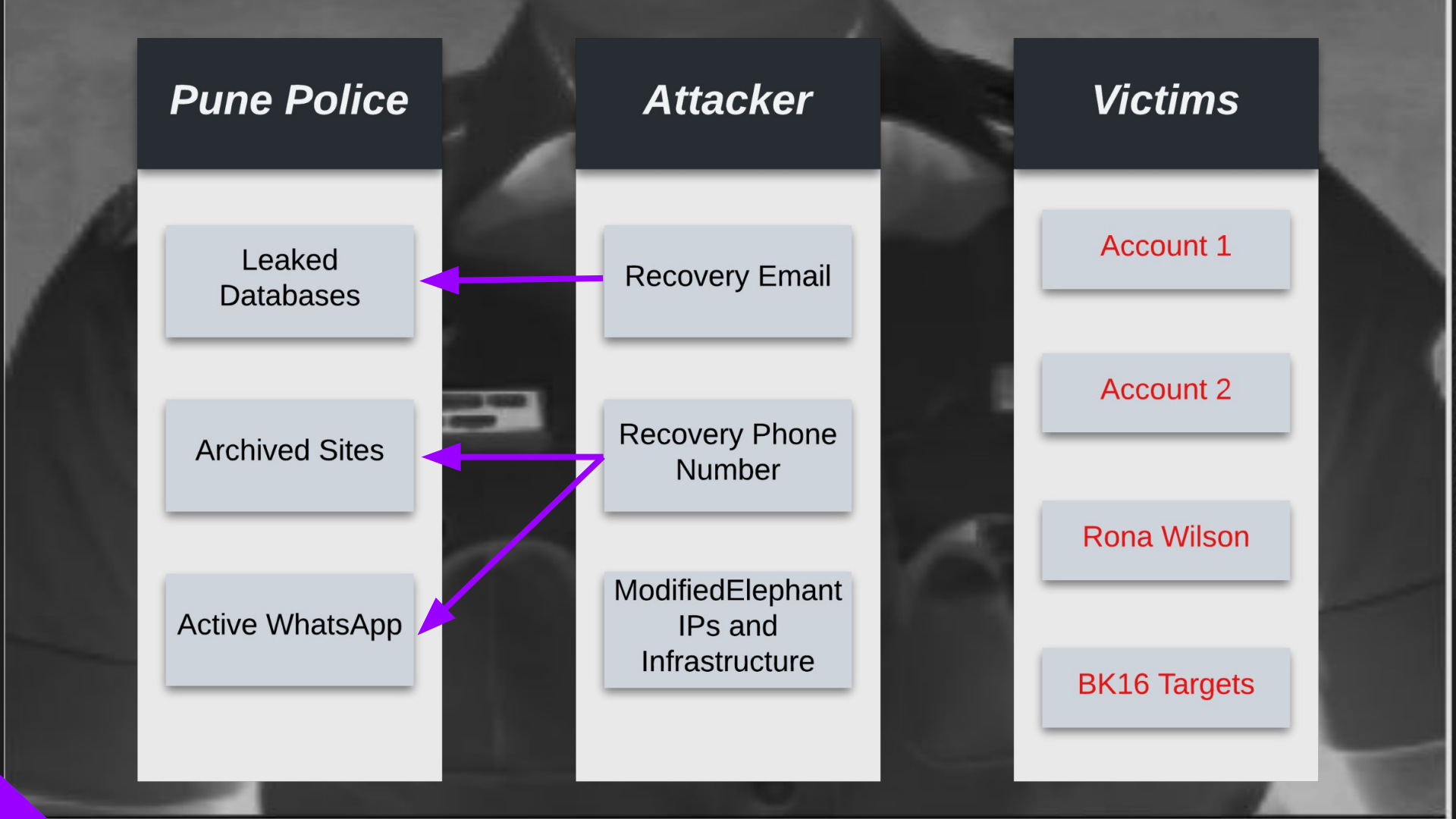
Police Linked to Hacking Campaign to Frame Indian Activists

New details connect police in India to a plot to plant evidence on victims' computers that led to their arrest.

“We generally don’t tell people who targeted them, but I’m kind of tired of watching shit burn,” the security analyst at the email provider told WIRED of their decision to reveal the identifying evidence from the hacked accounts. “These guys are not going after terrorists. They’re going after human rights defenders and journalists. And it’s not right.”


Pune Police
Leaked Databases
Archived Sites
Active WhatsApp
Attacker
Recovery Email
Recovery Phone Number
ModifiedElephant IPs and Infrastructure
Victims
Account 1
Account 2
Rona Wilson
BK16 Targets


Pune Police
Leaked Databases
Archived Sites
Active WhatsApp
Attacker
Recovery Email
Recovery Phone Number
ModifiedElephant IPs and Infrastructure
Victims
Account 1
Account 2
Rona Wilson
BK16 Targets


Pune Police
Attacker
Victims
Leaked Databases
Archived Sites
Active WhatsApp
Recovery Email
Recovery Phone Number
ModifiedElephant IPs and Infrastructure
Account 1
Account 2
Rona Wilson
BK16 Targets

Missing Forensic Artifacts

How a secretive, unknown smartphone app became the center of Turkey's post-coup crackdown

12

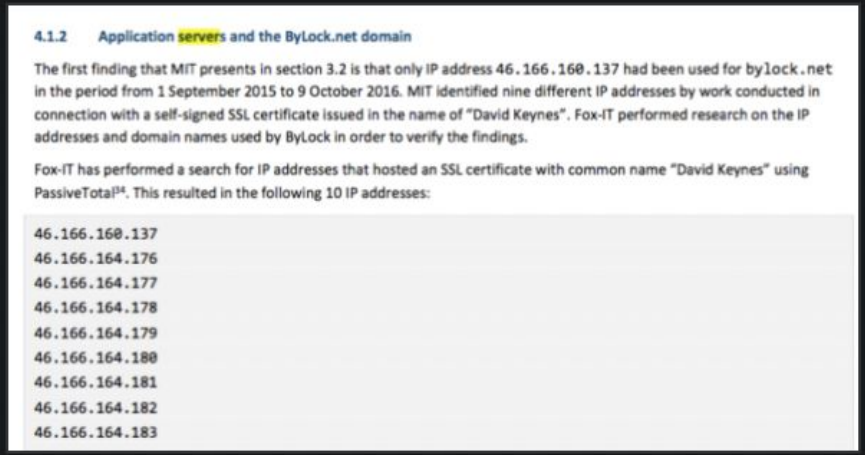
By Paul Benjamin Osterlund | Feb 28, 2018, 10:23am EST | 12 comments

When Digital Evidence Goes Wrong…

C. BYLOCK, AS REGARD TO EVIDENCE INTEGRITY AND AUTHENTICITY

1. IP Convergence (updated)

The main method through which ByLock users are identified is monitoring the respective IP traffic of suspects. If a suspect is found to have accessed to any of the ByLock servers, he is defined a ByLock user and charged and subsequently indicted for being a member of an armed terrorist organisation.



4.1.2 Application servers and the ByLock.net domain

The first finding that MIT presents in section 3.2 is that only IP address 46.166.160.137 had been used for bylock.net in the period from 1 September 2015 to 9 October 2016. MIT identified nine different IP addresses by work conducted in connection with a self-signed SSL certificate issued in the name of "David Keynes". Fox-IT performed research on the IP addresses and domain names used by ByLock in order to verify the findings.

Fox-IT has performed a search for IP addresses that hosted an SSL certificate with common name "David Keynes" using PassiveTotal[34]. This resulted in the following 10 IP addresses:

46.166.160.137
46.166.164.176
46.166.164.177
46.166.164.178
46.166.164.179
46.166.164.180
46.166.164.181
46.166.164.182
46.166.164.183

Spyware for Intelligence vs Law Enforcement?

Importance of Social Institutions

BROKEN NEWS

Why did India's media ignore Wired story on police planting evidence against Bhima Koregaon activists?

Much of the legacy media is doing itself a disservice by neglecting big-impact stories and small-town staff.

By Kalpana Sharma 14 Jul, 2022

Importance of Social Institutions

Bhima-Koregaon case: Justice Bhat becomes 5th judge to recuse from hearing Navlakha's plea

PTI / Updated: Oct 3, 2019, 12:59 IST

SHARE AA

ARTICLES


Bhima-Koregaon case: Justice Bhat becomes 5th judge to recuse...


This ISB programme will help you understand AI

Thank You

SentinelLABS

Tom Hegel
Senior Threat Researcher
tomhegel

Juan Andres Guerrero-Saade
Senior Director of SentinelLabs
juanandres_gs