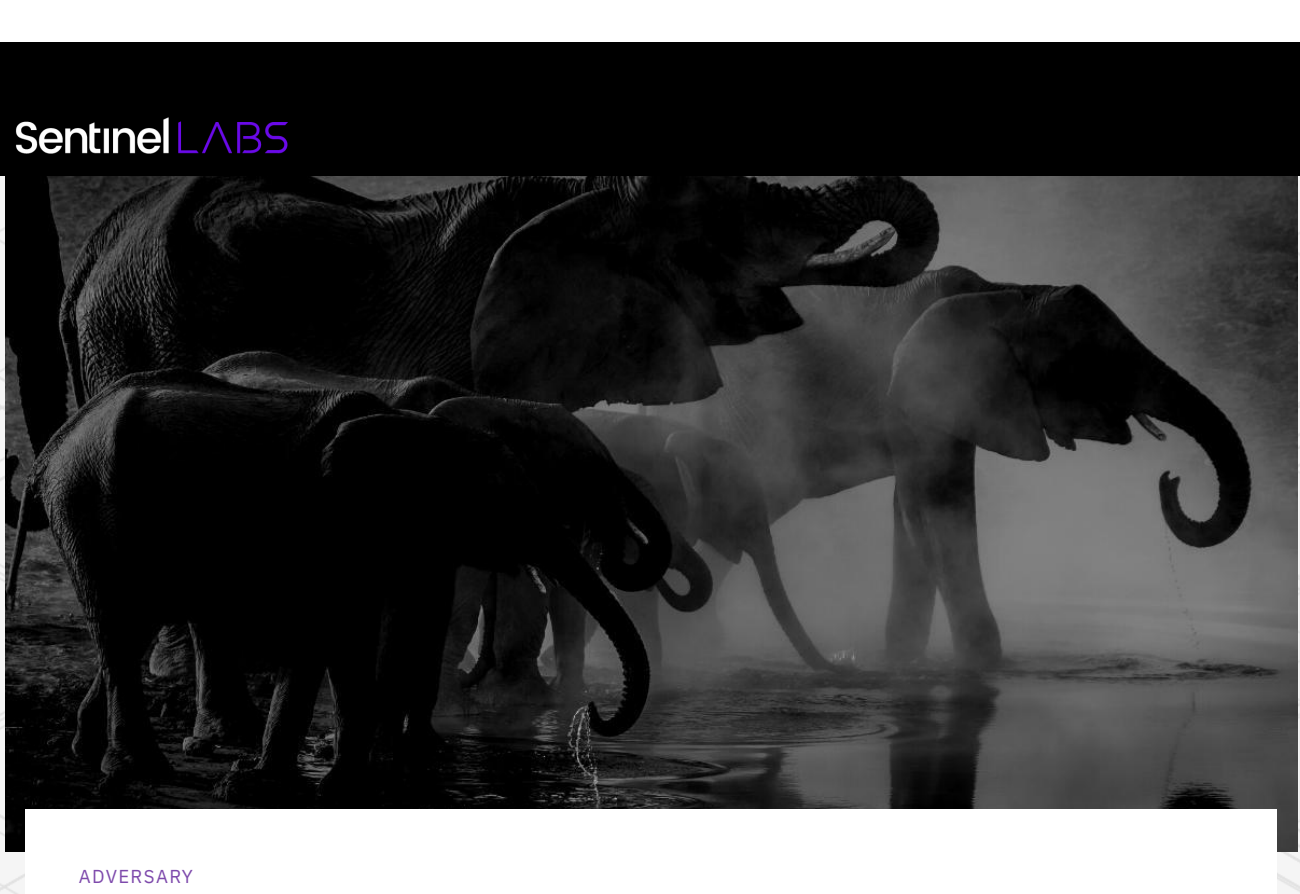


ADVERSARY

ModifiedElephant APT and a Decade of Fabricating Evidence

TOM HEGEL / FEBRUARY 9, 2022

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.

Read the Full Report

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.

ModifiedElephant 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

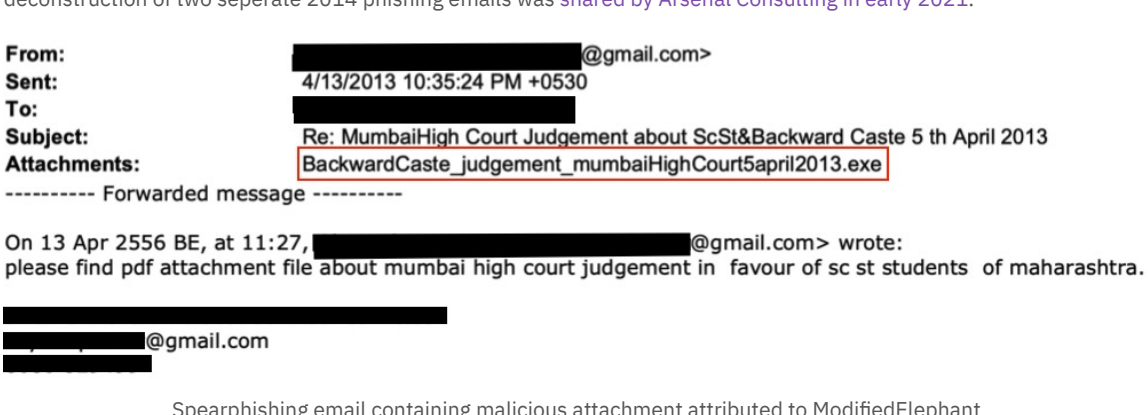
Throughout the last decade, ModifiedElephant operators sought to infect their targets via spearphishing emails with malicious file attachments, with their techniques evolving over time.

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.



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 ----------

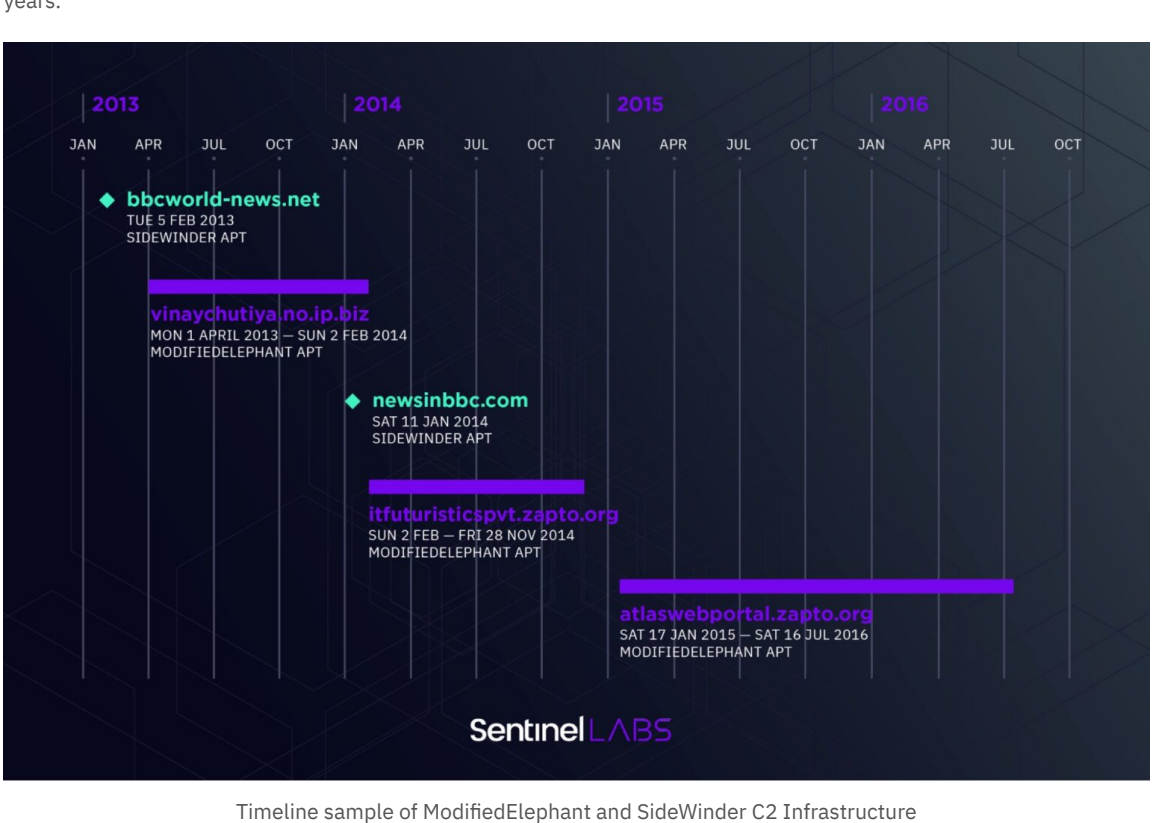
On 13 Apr 2556 BE, at 11:27, [redacted]@gmail.com> wrote:
please find pdf attachment file about mumbai high court judgement in favour of sc st students of maharashtra.

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

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.



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. Further details of the ModifiedElephant variant can be found in our full report.

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. The full report contains further details about the Android Trojan.

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.

Further details, Indicators of Compromise and Technical References are available in the full report.

Read the Full Report

APT ESPIONAGE

TOM HEGEL

Tom Hegel is a Senior Threat Researcher with SentinelOne. He comes from a background of detection and analysis of malicious actors, malware, and global events with an application to the cyber domain. His past research has focused on threats impacting individuals and organizations across the world, primarily targeted attackers.