
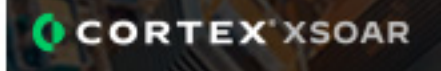
  
**Threat intelligence. Automated.**  
**Security automation for everyone**  
[Learn more](#)

  
  
**Threat intelligence. Automated.**  
**Security automation for everyone**  
[Learn more](#)

Threat Intelligence | 5 MIN READ | ARTICLE

# India's Cybercrime and APT Operations on the Rise

Growing geopolitical tensions with China in particular are fueling an increase in cyberattacks between the two nations, according to IntSights.



Jai Vijayan  
Contributing Writer

September 23, 2020






A combination of economic, political, and social factors is driving an increase in cyber threat activity out of India.


Much of the activity involves scams, online extortion schemes, hacktivist campaigns, and the sale of narcotics and other illicit goods online. But also operating out of the country is a handful of relatively sophisticated advanced persistent threat actors and hacker-for-hire groups that have targeted organizations in multiple countries in recent years, according to a new report from IntSights.


Researchers from the threat intelligence


  
**Predict Encryption.  
End Ransomware.**  
Cybereason Predictive Ransomware Protection  
[LEARN MORE](#)


**Related Content**  
Sponsored by    
**RESOURCES** **TWITTER** **BLOGS** **VIDEO**

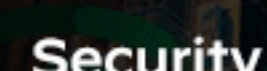
**The Future of Threat Intelligence**  
Download the white paper to learn about the importance of threat intelligence.

**The State of SOAR**  
Get this report and see how your security team can leverage SOAR to improve, automate and securely enable your SOC.

**Cortex XSOAR - The Essential Guide to Phishing Investigation and Response**  
Check out the Essential Guide to Phishing Investigation and Response to learn how to quickly shut down phishing attacks.


**TIM Whitepaper**  
This white paper talks about how we need to transform threat intelligence by integrating it into an extensible SOAR platform enabling analysts to take full control over their threat intelligence combined with the power of...


**Security Orchestration Dummies**  
In Security Orchestration for Dummies®, you will learn about its underlying needs, and implementation best practices.





  
**Threat intelligence. Automated.**  
**Security automation for everyone**  
[Learn more](#)

## Editors' Choice


**Google Paid Record \$8.7 Million to Bug Hunters in 2021**  
Jai Vijayan, Contributing Writer


**What CISOs Should Tell the Board About Log4j**  
Liran Tancman, CEO & Co-Founder, Rezilion


**8 Security Dinosaurs and What Filled Their Footprints**  
Ericka Chickowski, Contributing Writer


**Experts: Several CVEs From Microsoft's February Security Update Require Prompt Attention**  
Jai Vijayan, Contributing Writer


**Webinars**

[Strategies For Securing Your Supply Chain](#)

[Best Practices for Extending Identity & Access Management to the Cloud](#)


[How to Help Your Helpdesk Be More Helpful](#)


[The Tech Exec's Ransomware Incident Response Playbook](#)


[Practical Approaches to Implementing Zero Trust in Your Private Cloud](#)


[More Webinars](#)


**White Papers**

[Supporting Operational Technology's Cybersecurity Mission with XONA](#)

[DAST to the Future](#)


[Operationalizing the Modern AppSec Framework](#)


[Vantage Prevent Datasheet](#)


[The Top 10 PKI Metrics You Need to Track](#)

[More White Papers](#)

**Events**

[Cybersecurity Technology - March 24 Dark Reading Virtual Event](#)

[Black Hat Spring Trainings 2022 - February 28 - March 3 - Learn More](#)

[SupportWorld Live: May 15-20, 2022, MGM Grand, Las Vegas, NV](#)

[More Events](#)

firm recently analyzed how the growing geopolitical and economic tensions with neighboring China and Pakistan might be impacting cyber threat activity in India. As part of the research, IntSights also looked at broader cyber trends within the country and the factors behind them.

The research showed increased cyber threat activity between India and China amid growing border tensions in recent months between the two nuclear-armed countries. Etay Maor, chief security officer at IntSights, says the potential for kinetic conflict between the two sides is fueling efforts to shore up cyber-offensive capabilities within India.

The country's creation of a new tri-service Defense Cyber Agency (DFA) last year that combines cyber forces from India's army, air force, and navy is one example. The agency became operational last November and is thought to have about 1,000 personnel from across the three services. It has been tasked with building capabilities for protecting Indian strategic assets in cyberspace while also developing offensive cyberwarfare capabilities.

According to IntSights, the DCA's mission is to become capable of hacking into networks, mounting surveillance operations against targets of strategic importance, and laying honeytraps. "The agency seeks to build a state-of-the-art lab that can recover deleted data from hard disks and cellphones, break into encrypted communication channels, and perform other complex objectives," IntSights said in its report.

The threat intelligence firm identified three advanced persistent threat (APT) groups working out of India. Maor says that two of them — one called Dropping Elephant and another called Viceroy Tiger — likely carry out state-sponsored campaigns in addition to acting independently. IntSight's research showed that Dropping Elephant is mainly focused on military and intelligence targets based in countries such as China and Pakistan. The group has also been associated with economic espionage activity in the past.

Viceroy Tiger's activities, as described in the IntSights report, appear to be broader in scope. According to IntSight, the group's targets have included government, military, and civilian entities in the region and in countries like the US and Norway. Maor says that both groups have tended to mainly use a combination of known vulnerabilities, exploits, malware tools, and tactics such as phishing and spear-phishing in their campaigns.

Both Dropping Elephant and Viceroy Tiger groups have been around for a long time. [Kaspersky](#), for instance, first reported on Dropping Elephant back in 2016 and [Crowdstrike](#) reported on Viceroy Tiger using a zero-day exploit in 2013. Even so, both groups are relatively unknown compared to state-backed APT actors operating in countries like China, Iran, and North Korea, Maor notes. "We are not able to say one hundred percent if they are sitting under the Indian military or are contractors working for them," he says.

### Hackers-For-Hire

The third Indian APT group identified in IntSight's report is called Dark Basin, a sort of hacker-for-hire outfit that has allegedly targeted government officials, politicians, advocacy groups, and human rights activities in six continents. The group has previously been described as being linked to an Indian company called BellTroX InfoTech Services. It was most recently associated with a string of attacks on environmental NGOs working on a legal case against ExxonMobil this June. According to the University of Toronto's Citizen Lab, which [uncovered the campaign](#) this June after a multi-year investigation, Dark Basin has also been involved in operating phishing campaigns against climate advocacy groups and organizations advocating for net neutrality.

"Dark Basin has a remarkable portfolio of targets, from senior government officials and candidates in multiple countries, to financial services firms such as hedge funds and banks, to pharmaceutical companies," Citizen Lab said in its report. "Troublingly, Dark Basin has extensively targeted American advocacy organizations working on domestic and global issues."

Meanwhile, an abundant availability of cyber talent and relatively limited access to careers in the domestic tech sector in India appears to be luring many to cybercriminal activities, IntSights said. The company's research showed many Indian threat actors using Dark Web forums and underground markets to plan, collaborate on, and execute a wide range of malicious activity.

Multiple scam centers operate within the country that use data purchased from Dark Web forums or obtained through phishing and other social engineering to execute a variety of fraudulent schemes. Among the activity that IntSights identified in its report were tech-support scams, IRS scams, dating scams, extortion using adult content, and the threat of releasing illicit recordings ostensibly obtained through hacking security cameras.

Employees at some tech support scam centers sometimes do not appear to know the fraudulent nature of the organization they are working for and often are led to believe that they are working for big-name companies, Maor says.

Vulnerabilities/Threats   Advanced Threats

Keep up with the latest cybersecurity threats, newly-discovered vulnerabilities, data breach information, and emerging trends. Delivered daily or weekly right to your email inbox.

[Subscribe](#)

### Recommended Reading:

**Aerospace, Telecommunications Companies Victims of Stealthy Iranian Cy...**

**Belarus Linked to Big European Disinformation Campaign**

**Threat Actors Use Microsoft OneDrive for Command-and-Control in Attack Campaign**

**Russian APT Steps Up Malicious Cyber Activity in Ukraine**

## More Insights

### White Papers

- Supporting Operational Technology's Cybersecurity Mission with XONA
- DAST to the Future

[More White Papers](#)

### Webinars

- Strategies For Securing Your Supply Chain
- Best Practices for Extending Identity & Access Management to the Cloud

[More Webinars](#)

### Reports

- How Enterprises Are Assessing Cybersecurity Risk in Today's Environment
- How Data Breaches Affect the Enterprise

[More Reports](#)

### Discover More From Informa Tech

- Interop
- Data Center Knowledge
- InformationWeek
- Black Hat
- Network Computing
- Omdia
- ITPro Today

### Working With Us

- About Us
- Advertise
- Reprints

### Follow Dark Reading On Social

