RISKIQ®

Think Outside the Firewall™

The Citizen Lab: Defending Civil Society with RiskIQ PassiveTotal™

Challenges

- Small team meant reducing investigation time was critical
- Disconnected threat data led to longer investigations
- Threat infrastructure changes rapidly

Solution Benefits

- Single platform for multiple threat intelligence data sets
- Team collaboration through public and private projects
- Dynamic pivoting to speed up investigations

"Tools like PassiveTotal help us punch above our weight. Its ease of use, rich data set, and ongoing evolution of its features make it an excellent tool for our research, and a benchmark that we compare other options against."

– Masashi Crete-Nishihata
Research Manager
The Citizen Lab

About Citizen Lab

Civil society groups such as journalists, humanitarians, and activists face the same level of threat from targeted digital espionage as major companies and governments but have fewer resources to defend themselves. The Citizen Lab, an interdisciplinary research group based at the Munk School of Global Affairs, University of Toronto, is their guardian.

The Citizen Lab researches the intersection of information security, human rights, and global affairs. A core part of their mission is investigating the prevalence and impact of digital espionage operations against civil society groups and providing communities with information that they can use to raise awareness and improve their defenses.

The Challenge

Often, threat actors that target civil society groups also go after well-resourced governments and businesses and are equipped accordingly. But their civil society victims are usually limited in their capacity to identify and mitigate threats, even when the consequences can mean imprisonment or
physical harm.

When the Citizen Lab begins their investigations, these targets are often at serious risk, and in many cases, besieged by threat actors working for the governments and regimes under which they live. Without these researchers, people like renowned UAE human rights defender, Ahmed Mansoor, whose iPhone was attacked via remote jailbreak using a string of zero-days, or the Latin American journalists targeted by an extensive phishing campaign linked to malware and fake news sites, would have little to no recourse.

The RiskIQ Solution

RiskIQ PassiveTotal™ helps the Citizen Lab enrich its investigations of targeted espionage operations by mapping their infrastructure and monitoring how it changes over time. One of the first steps Citizen Lab researchers take when examining a new sample of malware or phishing is quickly looking for related infrastructure inside PassiveTotal's web interface and Maltego Transforms, which can provide unmatched insight into the behavior of the threat actors they're tracking.

Infrastructure tracking enriched by PassiveTotal also shows researchers how threat actor tactics change over time. For example, finding repurposed parts of known malware command and control infrastructure in phishing attacks indicates a shift in tactics from targeted malware campaigns to conventional phishing. This intelligence would then help the Citizen Lab recommend defensive measures such as using two-factor authentication and avoiding sending and receiving file attachments by email.

"Analysts at the Citizen Lab have been using PassiveTotal in investigations since the very first beta of the platform in 2014. Tools like PassiveTotal help us punch above our weight. Its ease of use and ongoing evolution of its features make it an excellent tool for our research, and a benchmark that we compare other options against."

– Masashi Crete-Nishihata, Research Manager The Citizen Lab

The Results

With PassiveTotal, the Citizen Lab linked the intrusion attempt on Ahmed Mansoor to infrastructure operated by NSO Group, a vendor of commercial spyware for governments. The investigation led to Apple releasing an out of band patch for IOS, as well as international media coverage of how some commercial surveillance products sold exclusively to governments are being used against civil society.

In the case of phishing emails targeting Latin American journalists, the researchers used PassiveTotal to connect the phishing infrastructure to both malware command and control servers, and to a pattern of fake news websites. This information helped them identify a threat actor and actively monitor its behavior.

"We encourage all companies working with threat intelligence to think about ways they can help protect those fighting for human rights. Whether it's donating licenses, empowering staff to volunteer, or just keeping an open mind about pro-bono initiatives, you'll be helping keep democracy alive."

– John Scott-Railton
Senior Researcher
The Citizen Lab

RISKIQ®

RiskIQ provides comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. RiskIQ's platform delivers unified insight and control over external web, social, and mobile exposures. Thousands of security analysts use RiskIQ to expedite investigations, monitor their attack surface, assess risk, and remediate threats.

Learn how RiskIQ could help protect your digital presence by scheduling a demo today.

22 Battery Street, 10th Floor
San Francisco, CA. 94011

sales@riskiq.net RiskIQ.com
1 888.415.4447 @RiskIQ