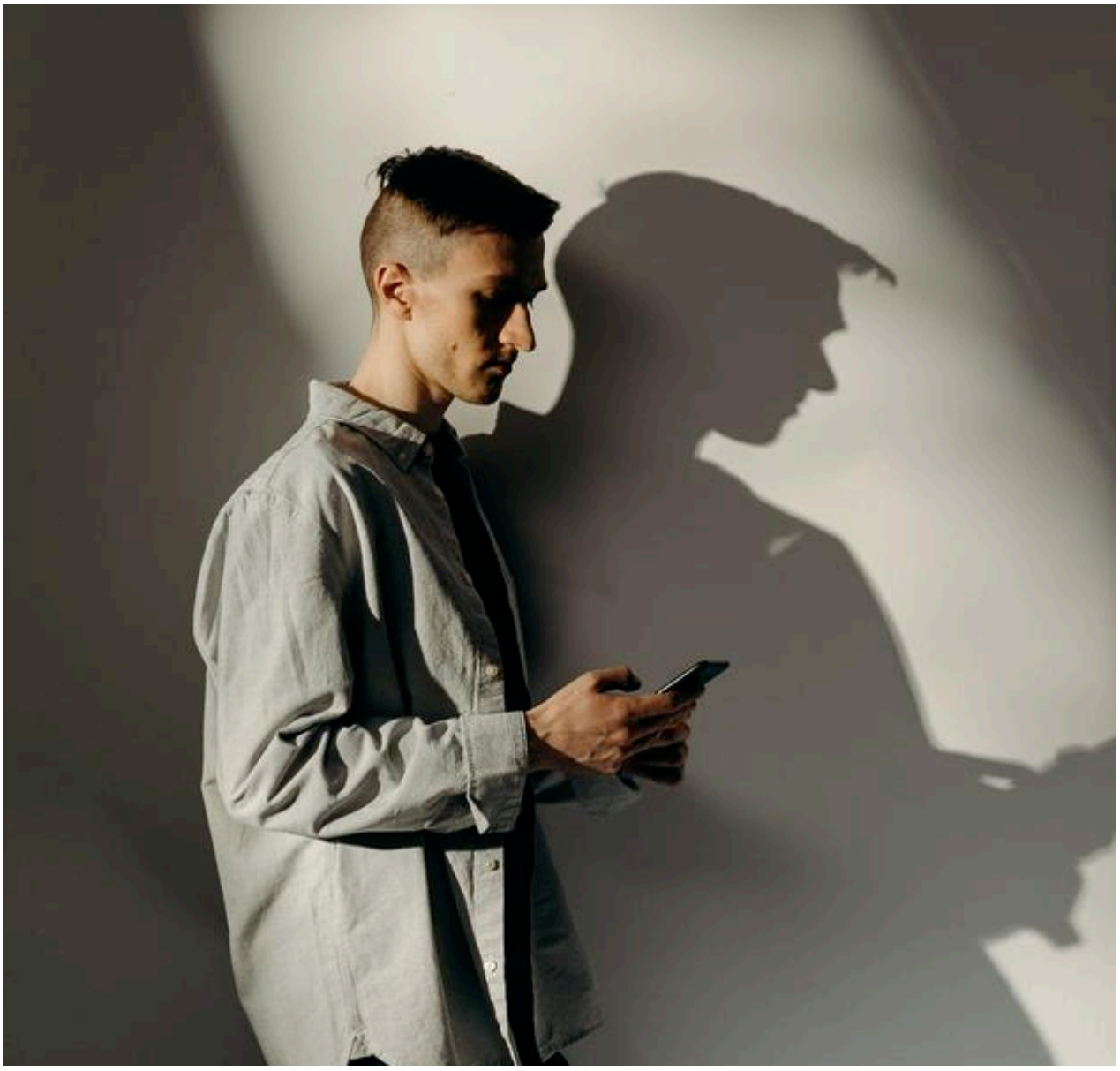
costricto mercenary Outsourced Cyber Spying hackers espionage

Archived: 2026-04-05 13:52:49 UTC



Mercenary hacking groups offering Advanced Package Tools (APT) attacks are becoming more popular and their tactics, techniques and procedures can resemble highly sophisticated state-sponsored campaigns.

Blackberry Research have documented the activity of a hackers-for-hire group, named as CostaRicto which has been monitored using new form of malware to target South Asian financial institutions and global entertainment companies. The profiles and geography of their victims are very varied and so it is unlikely that this is just one hacking band and its likely that there are several different groups for hire.

Although in theory the customers of a mercenary APT might include anyone who can afford it, the more sophisticated actors will naturally choose to work with patrons of the highest profile, be it large organizations,

influential individuals, or even governments.

Cyber criminals must choose very carefully when selecting their commissions to avoid the risk of being exposed. Outsourcing an espionage campaign, or part of it, to a mercenary group might be very compelling, especially to businesses and individuals who seek intelligence on their competition yet may not have the required tooling, infrastructure and experience to conduct an attack themselves. But even notorious adversaries experienced in cyber-espionage can benefit from adding a layer of indirection to their attacks. By using a mercenary as their proxy, the real attacker can better protect their identity and thwart attempts at attribution.

Targeting

Unlike most of the state-sponsored APT actors, the CostaRicto adversary seems to be indiscriminate when it comes to the victims' geography. Their targets are located in numerous countries across the globe with just a slight concentration in the South-Asian region. The list of other countries where victims were observed include China, the US, Bahamas, Australia, Mozambique, France, the Netherlands, Austria, Portugal and the Czech Republic.

Blackberry analysts noticed that one of the IP addresses employed in the attacks of the group has been linked to an earlier phishing campaign initially attributed to the Russia-linked APT28 group. This circumstance suggests that the Costaricto APT carried out attacks on behalf of other threat actors.

The victims' profiles are diverse across several verticals, with a large portion being financial institutions. Like many of the other hacker-for-hire operations, this one appears to have been operational for at least many months, according to BlackBerry. While the earliest time stamps for the custom backdoor date to October of last year, the time stamps on the payload stagers, which date to 2017, could suggest a longer-running operation.

Blackberry: Security Affairs: CSOOnline: CyberScoop: Israel Defense:

You Might Also Read:

Creating Post-Modern Intelligence:

Directory of Suppliers

Resecurity

Resecurity is a cybersecurity company that delivers a unified platform for endpoint protection, risk management, and cyber threat intelligence.

Jooble

Jooble is a job search aggregator operating in 71 countries worldwide. We simplify the job search process by displaying active job ads from major job boards and career sites across the internet.

Authentic8

Authentic8 transforms how organizations secure and control the use of the web with Silo, its patented cloud browser.

Arxan Technologies

Arxan is a leader of application attack-prevention and self-protection products for Internet of Things (IoT), Mobile, Desktop, and other applications.

RiskLens

RiskLens is a software company that specializes in the quantification of cybersecurity risk.

Forensic Pathways

Forensic Pathways focus on the provision of digital forensic technologies, offering clients unique technologies in the management of mobile phone data, image analysis and ballistics analysis.

Gilbert + Tobin

Gilbert + Tobin is an Australian corporate law firm serving clients throughout Australia, and around the world, on a broad range of legal issues including cyber security.

Stellar Cyber

Stellar Cyber makes Open XDR, the only comprehensive security platform providing maximum protection of applications and data wherever they reside.

Kindus

Kindus is an IT security, assurance and cyber security risk management consultancy.

Russell Reynolds Associates

Russell Reynolds Associates is a global leadership advisory and search firm with functional expertise in Digital Leadership, Data & Analytics, and Compliance.

Guernsey

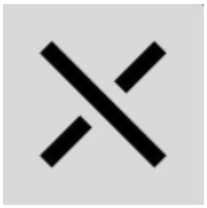
Guernsey provides a wide range of engineering, architecture and consulting services to multiple markets, including cybersecurity consulting and CMMC certification.

Tech Seven Partners

At TechSeven Partners, we provide a full suite of cyber security solutions for your business including network monitoring, onsite and cloud backup solutions, HIPAA or PCI compliance.

ZENDATA

ZENDATA are an innovative provider of intelligent, tailored cybersecurity solutions to global companies and public sector institutions.



MODUS X

MODUS X is a Ukrainian IT product and service company created from the IT department of the DTEK Group of Companies.

Acuvity

Acuvity is the most comprehensive AI security and governance platform for your employees and applications. Secure your GenAI adoption with confidence.

Koop

Koop’s trust management platform helps navigate the complexities of regulatory compliance, security reviews, and liability insurance in a single place.

Maximus

Maximus is a trusted service delivery partner and architect of government technology solutions, we empower communities by ensuring seamless and equitable access to government services.
