Trend Micro Uncovers Prolific Cyber Mercenary Group "Void Balaur"

Espionage and financially-driven hackers-for-hire have targeted more than 3,500 businesses and individuals since 2015

DALLAS, Nov. 10, 2021 /PRNewswire/ **--** Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today announced new research detailing the activities of a hacker-for-hire group that has targeted at least 3,500 individuals and organizations, including human rights activists, journalists, politicians, and senior telco engineers.

To read a full copy of the report, please visit: *Void Balaur: Tracking a Cybermercenary's Activities*

"Cyber mercenaries is an unfortunate consequence of today's vast cybercrime economy," said Feike Hacquebord, senior threat researcher for Trend Micro. "Given the insatiable demand for their services and harboring of some actors by nation-states, they're unlikely to go away anytime soon. The best form of defense is to raise industry awareness of the threat in reports like this one and encourage best practice cybersecurity to help thwart their efforts."

The report details the activity of a group of threat actors self-described as "Rockethack," which Trend Micro has dubbed "Void Balaur"—named after an evil multi-headed creature from Eastern European folklore.

Since at least 2018, the group has been advertising only on Russian-language forums and has accrued unanimously positive reviews. It's focused on making money from two related activities: breaking into email and social media accounts; and selling highly sensitive personal and financial information, including telco data, passenger flight records, banking data, and passport details.

Void Balaur's charges for such activities range from around $20 for a stolen credit history or traffic camera shots at $69 to over $800 for phone call records with cell tower locations.

Global targets include telecommunications companies in Russia, ATM machines vendors, financial services companies, medical insurers, and IVF clinics—organizations known to store highly sensitive and potentially lucrative information. The group also targets journalists, human rights activists, politicians, scientists, doctors, telco engineers, and cryptocurrency users.

Its efforts have become increasingly bold over the years, with targets including the former head of an intelligence agency, seven active government ministers, and a dozen members of parliaments in European countries.

Some of its targets—including religious leaders, diplomats, and journalists—also overlap with the notorious Pawn Storm group (APT28, Fancy Bear).

Trend Micro has associated thousands of indicators with Void Balaur, which are also available to organizations as part of the comprehensive threat intelligence. It most commonly deploys phishing tactics to achieve its ends, sometimes including info-stealing malware such as Z*Stealer or DroidWatcher.

The group also offers to hack email accounts without user interaction, although it's unclear how this is achieved—i.e., with the help of insiders or via a breached email provider.

Businesses and organizations should take the following steps to help defend against cyber mercenaries like Void Balaur:

- Use robust email services from a reputable provider with high privacy standards
- Use multi-factor authentication for your email and social media accounts via an app or Yubikey rather than one-time SMS passcode
- Use apps with end-to-end encryption in your communications
- Use encryption like PGP for sensitive communications
- Permanently delete messages you no longer need to minimize exposure
- Use drive encryption on all computing devices
- Turn off laptops and computers when not in use
- Utilize a cybersecurity platform approach that can detect and respond across the entire attack chain

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---