Trend Micro Research Finds Trust Lacking Within the Cybercriminal Underground

Report details changing tactics and global demand for new malicious services like Deepfake ransomware and AI bots

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released new data on cybercriminal operations and patterns for buying and selling goods and services in the underground. Trust has eroded among criminal interactions, causing a switch to e-commerce platforms and communication using Discord, which both increase user anonymization.

"This report highlights the threat intelligence we collect and analyze from global cybercriminal networks that enables us to alert, prepare and protect our corporate customers and partners," said Ed Cabrera, chief cybersecurity officer for Trend Micro. "This research helps us inform businesses early about emerging threats, such as Deepfake ransomware, AI bots, Access-as-a-Service and highly targeted SIM-swapping. A layered, risk-based response is vital for mitigating the risk posed by these and other increasingly popular threats."

The report reveals that determined efforts by law enforcement appear to be having an impact on the cybercrime underground. Several forums have been taken down by global police entities, and remaining forums experience persistent DDoS attacks and log-in problems impacting their usefulness.

Loss of trust led to the creation of a new site, called DarkNet Trust, which was created to verify vendors' and increase user anonymity. Other underground markets have launched new security measures, such as direct buyer-to-vendor payments, multi-signatures for cryptocurrency transactions, encrypted messaging, and a ban on JavaScript.

The report also reveals the changing market trends for cybercrime products and services since 2015. Commoditization has driven prices down for many items. For example, crypting services fell from US$1,000 to just $20 per month, while the price of generic botnets dropped from $200 to $5 per day. Pricing for other items, including ransomware, Remote Access Trojans (RATs), online account credentials and spam services, remained stable, which indicates continued demand.

However, Trend Micro Research has seen high demand for other services, such as IoT botnets, with new undetected malware variants selling for as much as $5,000. Also popular are fake news and cyber-propaganda services, with voter databases selling for hundreds of dollars, and gaming accounts for games like Fortnite can fetch around $1,000 on average.

Other notable findings include the emergence of markets for:

- **Deepfake services** for sextortion or to bypass photo verification requirements on some sites.
- **AI-based gambling bots** designed to predict dice roll patterns and crack complex Roblox CAPTCHA.
- **Access-as-a-Service** to hacked devices and corporate networks. Prices for Fortune 500 companies can reach up to US$10,000 and some services include access with read and write privileges.
- **Wearable device accounts** where access could enable cybercriminals to run warranty scams by requesting replacement devices.

Trends in underground marketplaces will likely shift further in the months following the global COVID-19 pandemic, as attack opportunities continue to evolve. To protect against the ever-changing threat landscape, Trend Micro recommends a multi-layered defense approach to protect against the latest threats and mitigate corporate security risk.

To find out more and read the full report, please visit: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/trading-in-the-dark.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com.

Contact:

Erin Johnson
817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
OTC Pink:
TMICY

---

https://newsroom.trendmicro.com/2020-05-26-Trend-Micro-Research-Finds-Trust-Lacking-Within-the-Cybercriminal-Underground