Thriving Access as a Service Cybercrime Market Fuels Ransomware Attacks

Trend Micro Research highlights the importance of securing enterprise credentials

DALLAS, Dec. 1, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, released new research detailing the murky cybercrime supply chain behind much of the recent surge in ransomware attacks. Demand has increased so much over the past two years that many cybercriminal markets now have their own "Access-as-a-Service" sections.

To read a full copy of the report, *Access-as-a-Service,* please visit: https://research.trendmicro.com/AccessAsAService

"Media and corporate cybersecurity attention have been focused only on the ransomware payload when we need to focus first on mitigating the activity of initial access brokers," said David Sancho, senior threat researcher for Trend Micro. "Incident responders often need to investigate two or more overlapping attack chains to identify the root cause of a ransomware attack, which often complicates the overall IR process. Teams could get ahead of this issue by monitoring for activity by Access Brokers who steal and sell enterprise network access – essentially cutting off the supply for ransomware actors."

The research is based on an analysis of over 900 access broker listings from January throughAugust 2021 across multiple English and Russian language-based cybercrime forums.

Education was the most frequently featured sector, accounting for 36% of advertisements—more than triple the second and third most targeted industries, manufacturing, and professional services, which both account for 11%.

The report reveals three main types of access brokers:

- **Opportunistic sellers** who are focused on making a quick profit and don't spend all their time on access.
- **Dedicated brokers** are sophisticated and skilled hackers who offer access to a range of different companies. Their services are often used by smaller ransomware affiliates and groups.
- **Online shops** that offer RDP and VPN credentials. These dedicated shops only guarantee access to a single machine rather than an entire network or organization. However, they represent a simple, automated way for cybercriminals with lower skill sets to purchase access. They can even search by location, ISP, operating system, port number, admin rights, or company name.

Most access broker offerings involve a simple set of credentials that may have been sourced from: Previous breaches and password hash breaking; compromised bot computers; vulnerability exploitation on VPN gateways, web servers, etc.; or one-off opportunistic attacks.

Prices vary depending on the type of access (single machine or entire network/corporation), annual revenue of the company, and how much extra work the buyer needs to do. Although RDP access can be obtained for as little as $10, the average price for admin credentials into a business is around $8,500. However, prices can reach up to $100,000.

Trend Micro recommends the following strategies for defenders:

- Monitor for public breaches
- Trigger a password reset for all users if you suspect corporate credentials might be breached
- Set up Multi-Factor Authentication (MFA)
- Monitor user behavior
- Watch the DMZ and assume internet-facing services like VPN, webmail and web servers are under constant attack
- Implement network segmentation and micro-segmentation
- Deploy best practice password policies
- Implement some form of Zero Trust architecture

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: Media Contact: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---

https://newsroom.trendmicro.com/2021-12-01-Thriving-Access-as-a-Service-Cybercrime-Market-Fuels-Ransomware-Attacks