

Cybercriminals Use Cloud Technology to Accelerate Business Attacks

Trend Micro Research finds terabytes of stolen data sold in cloud logs making cybercrime more widespread and effective

DALLAS, Nov. 16, 2020 /PRNewswire/ -- [Trend Micro Incorporated](#) (TYO: 4704; TSE: 4704), the leader in cloud security, has identified a new class of cybercrime. Criminals are using cloud services and technology to speed up attacks, which decreases the amount of time enterprises have to identify and respond to a breach.

These findings are published in a new report from Trend Micro Research:

<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-cloud-of-logs-the-emerging-underground-business-of-selling-access-to-stolen-data>.

Trend Micro Research found terabytes of internal business data and logins for popular providers like Amazon, Google, Twitter, Facebook, and PayPal offered for sale on the dark web. This data is sold via access to the cloud logs in which it is stored. This results in more stolen accounts being monetized, and the time from initial data theft to stolen information being used against an enterprise has decreased from weeks to days or hours.

"The new market for access to cloud logs ensures stolen information can be used more quickly and effectively by the cybercrime community—that's bad news for enterprise security teams," said Robert McArdle, director of forward-looking threat research for Trend Micro. "This new cybercriminal market shows how criminals are using cloud technologies to compromise you. Which also means a business is not exempt from this attack method if they only use on-prem services. All organizations will need to double down on preventative measures and ensure they have the visibility and controls needed to react fast to any incidents that occur."

Once access is purchased for logs of cloud-based stolen data, the purchaser will use the information for secondary infection. For example, Remote Desktop Protocol (RDP) credentials can be found in these logs and are a popular entry point for criminals targeting enterprises with ransomware.

Storing terabytes of stolen data in cloud environments has similar appeal for criminal businesses as it does for legitimate organizations. Cloud storage offers scalability and speed that provides more computing power and bandwidth to optimize operations.

Access to these logs of cloud data are often sold on a subscription basis for as much as \$1,000 per month. Access to a single log can include millions of records, and higher prices are earned for frequently updated data sets or the promise of relative exclusivity.

With ready access to data in this way, cybercriminals can streamline and accelerate execution of attacks and potentially expand their number of targets. The result is to optimize cybercrime by ensuring threat actors who specialize in specific areas—say cryptocurrency theft, or e-commerce fraud—can get access to the data they need: quickly, easily and relatively cheaply.

The Trend Micro report warns that in the future, such activity could even give rise to a new type of cybercriminal—an expert in data mining who uses machine learning to enhance pre-processing and extraction of information to maximize its usefulness to buyers. The overall trend will be towards standardization of services and pricing, as the industry matures and professionalizes.

About Trend Micro

Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers with connected solutions across cloud workloads, endpoints, email, IIoT, and networks. Our XGen™ security strategy powers our solutions with a cross-generational blend of threat-defense techniques that are optimized for key environments and leverage shared threat intelligence for better, faster protection. With over 6,700 employees in 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. www.trendmicro.com

SOURCE Trend Micro Incorporated

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

<https://newsroom.trendmicro.com/2020-11-16-Cybercriminals-Use-Cloud-Technology-to-Accelerate-Business-Attacks>