Trend Micro Research Uncovers The Business Infrastructure Of Cybercrime

Turns out criminal businesses need hosting services and cybersecurity protections too

DALLAS, July 21, 2020 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released new insights analyzing the market for underground hosting services and detailing how and where cybercriminals rent the infrastructure that hosts their business. This first report of a planned three-part series details the market for buying and selling these services, which are the backbone of every other aspect of the cybercriminal business model, whether that includes sending spam, communicating with a command and control server, or offering a help desk for ransomware.

Over the past five years, increased use and abuse of compromised assets has formed a whole new market. There are varied types of underground hosting and associated services used by cybercriminals to operate their businesses, including bulletproof hosting, virtual private networks (VPNs), anonymizers, and Distributed Denial of Service (DDoS) protection. Such services could variously be used to protect availability, maintain anonymity, disrupt forensics, obfuscate physical location, and enable IP spoofing, among other things.

"For over a decade, Trend Micro Research has dug into how cybercriminals think, as opposed to focusing only on what they do, which is critical when it comes to protecting against them," said Robert McArdle, director of forward-looking threat research at Trend Micro. "Today we release the first of a three-part in-depth series on how these criminals approach their infrastructure needs, and the markets that exist for such commodities. We hope that providing law enforcement and other stakeholders with a go-to resource on this topic will help to further our collective mission of making the digital world a safer place."

Cybercrime is a highly professional industry, with sales and advertisements leveraging legitimate marketing techniques and platforms, all driven by cost to some extent. For example, one advertisement was found for dedicated, compromised servers based in the US starting at just $3, rising to $6 with guaranteed availability for 12 hours. Although many of these services are traded on underground forums, some of which are invite-only, others are clearly advertised and sold via legitimate social media and messaging platforms such as Twitter, VK and Telegram.

In fact, the line between criminality and legitimate business behavior is increasingly difficult to discern. Some hosting providers have a legitimate clientele and advertise openly on the internet but may have resellers that sell exclusively to the criminal underground – either with or without the company's knowledge.

In the case of bulletproof hosters, which are more definitively linked to cybercrime, they are generally regular hosting providers trying to diversify their business to cater to the needs of specific customers. For a premium price, they're prepared to push to the absolute limit of what the law allows and prosecutes in their local jurisdiction.

Understanding where and how these services are sold, and consequently impacting the cost of these sales, is arguably our best strategy to help make a lasting and repeatable dent in the cybercriminal underground market. Parts two and three of the series will further investigate the types of underground services and infrastructure offered, and the operational security and motivations of the actors who sell such services.

To read the complete first report, please visit: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infrastructure-and-underground-hosting-101-where-are-cybercriminal-platforms-offered.

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 enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.

SOURCE Trend Micro Incorporated

For further information: Erin Johnson, 817-522-7911, media_relations@trendmicro.com

---