Trend Micro Research Reveals Top Tactics to Disrupt Underground Hosting Businesses

Threat correlation and visibility creates effective means to render cybercrime profitless

DALLAS, Oct. 6, 2020 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), the leader in cloud security, today released key ways to identify and disrupt criminal market operations to conclude a three-part report series on the underground hosting market. In the report, researchers outline the infrastructure business approaches of attackers to help security teams and law enforcement agencies best recognize, defend against, and disrupt them.

Understanding criminal operations, motivations and business models is key to dismantling the bulletproof hosting industry on which the majority of global cybercrime is built.

"Increasingly, mature organizations have SOC and XDR capabilities, which means security teams today have moved into the realm of also being investigators," said Robert McArdle, director of forward-looking threat research at Trend Micro. "At that level of security sophistication, you need to understand how the criminals operate to strategically defend against attackers. We hope this report provides insight into cybercriminal operations that can prove actionable for organizations and ultimately make hosters lose profits."

Bulletproof hosters (BPH) are the root of cybercriminal infrastructure and therefore use a sophisticated business model to outlast takedown efforts. These include flexibility, professionalism and offering a range of services to cater to an array of customer needs.

The report details several effective methods to help investigators identify underground hosters, including:

- Identify which IP ranges are in public block deny lists, or those associated with a large number of public abuse requests, as those may be indicative of BPH.
- Analyze autonomous system behavior and peering information patterns to flag activity that is likely associated to BPH.
- Once one BPH host has been detected, use machine fingerprinting to detect others that may be linked to the same provider.

The report also lists methods for law enforcement agencies and businesses to disrupt underground hosting businesses, without necessarily needing to identify or takedown their servers. These include:

- Submit properly documented abuse requests to the suspected underground hosting provider and upstream peers.
- Add BPH network ranges to well-established deny lists.
- Increase the operational costs of the BPH, to impair business stability.
- Undermine the reputation of the BPH on the cybercrime underground: perhaps via covert accounts that call into question the security of the criminal hosting provider or discuss possible collaboration with authorities.

To read the full report, please visit:https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/inside-the-bulletproof-hosting-business-cybercrime-methods-opsec.

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

---