Trend Micro Discloses Criminal Insights Following LockBit Disruption, Leaving No Shadow for Threat Actors

Trend and customers reap benefits of strategic intelligence-first approach

DALLAS, April 3, 2024 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today released comprehensive threat intelligence findings in the wake of the law enforcement-led disruption of the LockBit ransomware group. The unprecedented operation, known as Operation Cronos, marks a significant step forward in the global fight against cyber threats, impacting an entity responsible for an estimated quarter of all ransomware attacks worldwide.

To read a copy of the report, Unveiling the Fallout: Operation Cronos' Impact on LockBit Following Landmark Disruption, please visit: https://research.trendmicro.com/LockBitDisruptionAftermath

Robert McArdle, head of forward-looking threat research at Trend:"We are immensely supportive of the excellent disruptive work done by international Law Enforcement against the Lockbit group, and our ability to provide support with analysis of their planned upcoming version. Getting ahead of these threat actors not only allowed us to pass on intelligence to law enforcement, but also bolstered the defense of our global customer base. As we dissect the aftermath of this takedown, our commitment to enhancing security defense through global threat intelligence is yielding tangible results."

Operation Cronos was different in several ways from many of the typical law enforcement takedowns of criminal groups. More than a mere setback for threat actors, it was a decisive strike that crippled their infrastructure, undercut their financial mechanisms, exposed affiliates, and fractured the trust within their own illicit networks.

This cumulative effort has helped to tarnish LockBit's reputation among its networks and the cybercrime community in general, making it inept in its attempts to regroup. Ringleader "Lockbitsupp" has also been banned from two popular underground forums: XSS and Exploit.

The group has been trying to rebuild New Onion leak sites launched a week after the operation, and Lockbitsupp is actively seeking brokers selling access to .gov, .edu, and .org TLDs—in what appears to be a reprisal for Cronos.

However, these efforts appear to be failing. Trend's telemetry reveals limited cases of successful attack since the disruption. Although scores of victims have been posted to the new LockBit leak site, the vast majority were reuploaded from previous campaigns or are victims of other threat groups like ALPHV.

The group has also been developing a new version of ransomware, Lockbit-NG-Dev, which Trend has been monitoring closely and provided advanced protections to customers.

Operation Cronos marks a significant step forward in the global fight against cyber threats.

Key Achievements of Operation Cronos:

- **Reputational Damage to LockBit:** Given its tarnished reputation, LockBit faces significant challenges in rebuilding its operations and affiliate networks.
- **Strategic Disruption of Infrastructure:** The operation's in-depth approach has made LockBit's rebuilding and regrouping process difficult and time-consuming, delaying any potential resurgence.
- **Effective Deterrence:** The insight into affiliate activities and the subsequent warnings have likely dismantled any of LockBit's affiliate programs, further weakening its operational capacity.
- **Enhanced Business Security:** Trend customers stand to benefit from the operation's outcome and a reduced risk of being targeted by a significant player in the ransomware market.

This disruption underscores Trend's relentless pursuit of anticipating threats and shielding organizations worldwide from the evolving dangers of the cyber landscape. The best way to disrupt common adversaries is by sharing intelligence promptly and efficiently.

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

---

Additional assets available online: Video (1)

https://newsroom.trendmicro.com/2024-04-03-Trend-Micro-Discloses-Criminal-Insights-Following-LockBit-Disruption,-Leaving-No-Shadow-for-Threat-Actors