Trend Micro Study Reveals Criminal Abuses of Twitter

Social network used for scams and malice, as well as a threat intelligence source

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced a new study revealing how cybercriminals are abusing Twitter via tech support scams, command-and-control (C&C) operations and data exfiltration.

Trend Micro researchers analyzed a large volume of Twitter data to identify relationships between various entities to spot anomalies and uncover key insights.

“Social media is an inescapable part of modern life, and our new research shines an important light on how it’s being used positively by the security community, and abused by criminals,” said Mark Nunnikhoven, vice president of cloud research for Trend Micro. “This research shows businesses how the misuse of social networks can damage their brand, and it informs consumers how they might be tricked into a scam from what is believed to be a trusted source. We hope by making these abuses known, both businesses and consumers can be vigilant to not become victims of such attacks.”

Criminals were found using fake Twitter accounts to spoof those of legitimate vendors for credible tech support scams. Users call the fake phone number provided, believing they are speaking with the intended company’s help desk, which results in the caller either sharing credit card information or installing malicious content on the their computer.

This is often part of a multi-platform strategy along with YouTube, Facebook, Telegram and other channels to improve SEO for fake tech support websites linked to the Twitter accounts, boosting their search rankings.

While criminals are using the social network for bad, threat researchers can leverage the power of social media for good. Most notably, Twitter is used for monitoring vulnerability disclosures to inform patch prioritization, and scanning for indicators of compromise, threat detection rules, and other contextual information to boost threat intelligence.

Trend Micro recommends users confirm the validity of a Twitter account by checking the company’s website directly, rather than through the account. It is also important for security teams to validate Twitter data when leveraging it for investigations or threat intelligence.

To read the full report, please visit: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter.

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 secures your connected world. For more information, visit www.trendmicro.com.

Contact:

Erin Johnson

817-522-7911

media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.com/2019-07-30-Trend-Micro-Study-Reveals-Criminal-Abuses-of-Twitter