**Presseinformation**

**Untersuchung von Trend Micro zeigt kriminellen Missbrauch von Twitter**

# Wallisellen, 30. Juli 2019 – Trend Micro stellt heute eine neue Studie vor, die zeigt, wie Cyberkriminelle Twitter missbrauchen. Ihre Aktivitäten reichen von Tech-Support-Betrug über Command-and-Control-Kommunikation (C&C) bis hin zur Exfiltration von Daten. Gleichzeitig ergab die Untersuchung aber auch, dass das soziale Netzwerk von Cybersicherheitsexperten auch für positive Zwecke genutzt werden kann.

Forscher von Trend Micro analysierten eine große Menge an Twitter-Daten, um Beziehungen zwischen verschiedenen Akteuren und Anomalien zu erkennen. Daraus konnten sie wertvolle Erkenntnisse gewinnen.

„Soziale Medien sind ein fester Bestandteil unseres alltäglichen Lebens. Unsere neueste Forschung zeigt, wie sie einerseits von der Security-Community positiv genutzt, andererseits aber auch von Kriminellen missbraucht werden“, sagt Richard Werner, Business Consultant bei Trend Micro. „Unser Bericht zeigt Unternehmen, wie der Missbrauch von Social Media ihre Marke beschädigen kann und klärt Verbraucher auf, wie sich Betrüger als vertrauenswürdige Quelle ausgeben. Wir hoffen, dass wir Unternehmen und Verbraucher damit vor zukünftigem Schaden bewahren können.“

# Fake-Support-Accounts

Die Forscher fanden heraus, dass sich Kriminelle mittels gefälschter Accounts als Support-Abteilungen von Technik-Herstellern ausgeben. Nutzer werden dazu aufgefordert, Telefonnummern anzurufen, um mit dem vermeintlichen Helpdesk des Unternehmens zu sprechen. Dort werden die Anrufer dazu gebracht, ihre Kreditkartendaten preiszugeben oder bösartigen Content auf ihrem Computer zu installieren.

Die Kriminellen greifen dabei häufig auf eine Multi-Channel-Strategie zurück, bei der sie neben Twitter auch YouTube, Facebook, Telegram und andere Kanäle nutzen, um mittels SEO (Search Engine Optimization, Suchmaschinenoptimierung) das Suchmaschinen-Ranking ihrer gefälschten Support-Websites zu erhöhen.

Während Cyberkriminelle Twitter mit bösen Absichten nutzen, können Bedrohungsforscher das soziale Netzwerk auch zu positiven Zwecken verwenden. Vor allem können sie sich durch Twitter-Monitoring frühzeitig über die Veröffentlichung von Schwachstellen informieren, um Patches priorisiert einzuspielen. Zudem kann durch das Scannen auf Indicators of Compromise (IoC), Regeln zur Bedrohungserkennung und andere Kontext-Informationen die Qualität von Bedrohungsinformationen verbessert werden.

# Empfehlungen

Trend Micro empfiehlt, dass Nutzer die Echtheit von angeblichen Unternehmens- Accounts überprüfen, indem sie von der Firmen-Website auf den Twitter-Kanal gehen, anstatt direkt auf Twitter danach zu suchen. Auch Sicherheitsverantwortliche sollten auf Twitter gefundene Informationen stets validieren, bevor sie diese nutzen.

# Weitere Informationen

Den vollständigen Forschungsbericht finden Sie unter: [https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-](https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter) [threats/hunting-threats-on-twitter](https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter)

**Über Trend Micro**

Als einer der weltweit führenden Anbieter von IT-Sicherheit verfolgt Trend Micro mit Leiden- schaft das Ziel, eine sichere Welt für den digitalen Datenaustausch zu schaffen – heute und in Zukunft. Unsere innovativen Lösungen für Privatanwender, Unternehmen und Behörden bieten dank der XGen™ Sicherheitsstrategie vernetzten Schutz für Rechenzentren, Cloud-Workloads, Netzwerke und Endpunkte.

Die mehrschichtigen Lösungen von Trend Micro sind für führende Umgebungen wie Amazon Web Services, Microsoft® und VMware® optimiert. Mit ihnen können Organisationen den Schutz ihrer wertvollen Daten vor aktuellen Bedrohungen automatisieren. Unsere Connected Threat Defense ermöglicht das nahtlose Teilen von Bedrohungsinformationen und bietet zentrale Transparenz und Kontrolle, um Organisationen bestmöglich zu schützen.

Zu den Kunden von Trend Micro zählen neun der zehn wichtigsten Unternehmen der Fortune® Global 500 aus den Branchen Automotive, Kreditinstitute, Gesundheitswesen, Telekommunikation und Erdöl.

Mit über 6.500 Mitarbeitern in 50 Ländern und der weltweit fortschrittlichsten Erforschung und Auswertung globaler Cyberbedrohungen bietet Trend Micro Schutz für eine vernetzte Welt.

Die deutsche Niederlassung von Trend Micro befindet sich in Hallbergmoos bei München. In der Schweiz kümmert sich die Niederlassung in Wallisellen bei Zürich um die Belange des deutsch- sprachigen Landesteils, der französischsprachige Teil wird von Lausanne aus betreut; Sitz der ös- terreichischen Vertretung ist Wien.

**Weitere Informationen zum Unternehmen und seinen Lösungen sind unter** [**www.trendmi-**](http://www.trendmicro.com/)[**cro.com**](http://www.trendmicro.com/) **verfügbar, zu aktuellen Bedrohungen unter** [**blog.trendmicro.de**](http://blog.trendmicro.de/) **sowie** [**blog.trendmi-**](http://blog.trendmicro.ch/)[**cro.ch**](http://blog.trendmicro.ch/)**. Anwender können sich auch auf Twitter unter** [**@TrendMicroDE**](http://www.twitter.com/TrendMicroDE) **informieren.**

**Pressekontakt:**

Brand Affairs AG Nina Meroni Dufourstrasse 183 CH-8008 Zürich

Telefon: +41 44 254 80 00

E-Mail: nina.meroni@brandaffairs.ch

Internet: [www.brandaffairs.ch](http://www.brandaffairs.ch/)

**Herausgegeben im Auftrag von:**

Trend Micro Deutschland Ursula-Barbara Schmidt Zeppelinstrasse 1

D-85399 Hallbergmoos

Telefon: +49 (0) 811 88 99 0 – 700

Fax: +49 (0) 811 88 99 0 – 799

E-Mail: ursula\_schmidt@trendmicro.com Internet: [www.trendmicro.com](http://www.trendmicro.com/)

Trend Micro Österreich/Schweiz Daniel Schmutz

Husacherstrasse 3 CH-8304 Wallisellen

Telefon: +41 (0) 44 82860 – 80

Fax: +41 (0) 44 82860 – 81

E-Mail: daniel\_schmutz@trendmicro.com Internet: [www.trendmicro.](http://www.trendmicro./)com