



## Ransomware-Banden im Fegefeuer der Eitelkeiten

*Cyberkriminalität ist professionalisiert. Dazu gehören aber nicht nur Arbeitsteilung, Recruiting im Darknet und benutzerfreundliche Malware-Baukästen. Um sich von der Konkurrenz abzusetzen – und die eigenen Leistungen angemessen gewürdigt zu wissen – gehört für die Kriminellen offenbar auch Medienarbeit dazu.*

*Sophos X-Ops hat sich die letzten PR-Coups von Ransomware-Gruppen genauer angesehen.*

Der jüngste Hack des MGM-Casinos in Vegas, bei dem die Ransomware-Gruppe Black Cat Reportern öffentlich vorwarf, den Hack fälschlicherweise Scattered Spider zugeschrieben zu haben, rückte die Interaktion von Ransomware-Banden mit den Medien ins Rampenlicht. Nach einem genaueren Blick auf das Darknet und verschiedene Ransomware-Leak-Sites hat Sophos X-Ops herausgefunden, dass dies kein Einzelfall war: Ransomware-Gruppen wenden sich zunehmend an die Medien, um ihre Bekanntheit zu erhöhen und Druck auf die Opfer auszuüben.

Dabei nutzen sie eine Reihe von Strategien, um den direkten Kontakt zu den Medien aufrechtzuerhalten. Auf Ransomware-Leakseiten fanden die Sophos-Forscher spezielle Telegram-Kanäle und Kontaktformulare für die Presse, FAQs für Medien und Sonderangebote zur „Zusammenarbeit“ mit Journalisten. Sophos X-Ops hat sogar Stellenanzeigen für englischsprachige Autoren in kriminellen Foren gefunden, möglicherweise um Texte für Blogbeiträge zu schreiben, die die Angriffe der Gruppen bekannt machen und Artikel der Mainstream-Presse hervorheben, in denen sie vertreten sind.

Eine Einschätzung von Christopher Budd, Director Threat Research bei Sophos:



„Ransomware-Angreifer hacken nicht mehr nur Netzwerke und Systeme – sie versuchen, das öffentliche Narrativ zu ‚hacken‘. Wir haben dies beim [MGM-Hack](#) und bei den [MOVEit-Angriffen](#) von [CIOP](#) gesehen, als die Gruppe versuchte, angebliche Ungenauigkeiten in der Berichterstattung der Medien über ihre Angriffe ‚richtig zu stellen‘. Für die Cyberkriminellen bietet die Zusammenarbeit mit der Presse mehrere Vorteile. Es stärkt nicht nur ihr Ego, sondern erhöht auch ihren Bekanntheitsgrad – und macht sie zu einem begehrteren ‚Arbeitgeber‘ für Kriminelle. Zudem hat sich das Vorgehen als wirksame Methode erwiesen, um Opfer unter Druck zu setzen.

Wir werden es in Zukunft wahrscheinlich erleben, dass Ransomware-Gruppen noch direkter und häufiger mit der Presse interagieren. Interessanterweise haben wir bei unserer Recherche gesehen, dass einige Gruppen wie CIOP und Royal Pressemitteilungen nutzten, um ihre Aktivitäten in „Sicherheitsdienste“ umzubenennen. Dabei könnte es sich um eine Rekrutierungstaktik oder den Versuch handeln, ihr öffentliches Image zu verbessern. Unabhängig davon zeigt es die konzertierten Bemühungen dieser Bedrohungsgruppen, die öffentliche Wahrnehmung zu beeinflussen. Für Verteidiger ist es wichtig, ihrem Wunsch nach Aufmerksamkeit nicht nachzugeben. Wir müssen uns auf die Taktiken, Techniken und Verfahren (TTPs) der Angriffe konzentrieren, damit wir die Abwehrkräfte der Unternehmen stärken können, und nicht darauf, wer hinter dem Angriff steckt.“

Mehr Informationen und Beispiele zu dem Thema gibt es im englischsprachigen [Blogbeitrag](#) der Sophos X-Ops.

## **Social Media von Sophos für die Presse**

Wir haben speziell für Sie als Journalist\*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf  und 

LinkedIn: <https://www.linkedin.com/groups/9054356/>

Twitter: @sophos\_info

## **Pressekontakt:**

Sophos

Jörg Schindler, PR-Manager Central & Eastern Europe

[joerg.schindler@sophos.com](mailto:joerg.schindler@sophos.com), +49-721-25516-263

TC Communications

Arno Lücht, +49-8081-954619

Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198

Ariane Wendt +49-172-4536839

[sophos@tc-communications.de](mailto:sophos@tc-communications.de)