In Untersuchungen der letzten 48 Stunden zur ScreenConnect Sicherheitslücke findet Sophos auch Malware-Technologie von Lockbit

Vor wenigen Tagen ist internationalen Strafverfolgungsbehörden ein entscheidender Schlag gegen Lockbit gelungen. Laut einem ausführlichen Kommentar von Chester Wisniewski, Director, Global Field CTO bei Sophos, ist allerdings ein Teil ihrer Infrastruktur immer noch online, was vermutlich darauf hinweist, dass einige aus der Lockbit Cyberkriminellengruppe noch nicht gefasst worden sind. Die Chance, dass diese sich anderen Gruppen anschließen oder eine neue Gruppe bilden wäre keine Überraschung.

Jetzt veröffentlicht Sophos X-Ops einen Bericht über die seit kurzem bekannte Sicherheitslücke bei der Remote Management und Monitoring Lösung ScreenConnect. Die detaillierte Analyse „ConnectWise ScreenConnect Attacks Deliver Malware“ stellt auch einen Zusammenhang mit Lockbit fest. Christopher Butt, Sophos X-Ops Principal Researcher bei Sophos, dazu:
„Wir haben in den letzten 48 Stunden mehrere Angriffe analysiert, die sich die ScreenConnect-Sicherheitslücke zu Nutzen gemacht haben. Am bemerkenswertesten war eine Malware, die mit dem im Jahr 2022 geleakten Ransomware-Builder-Tool Lockbit 3 erstellt wurde. Sie stammt möglicherweise nicht von den eigentlichen Lockbit-Entwicklern. Aber wir konnten auch Remote Access Trojaner (RATS), Info- und Passwort-Stealer sowie andere Ransomware entdecken. All dies zeigt, dass viele verschiedene Angreifer ScreenConnect im Visier haben“, sagte Christopher Budd, Direktor Sophos X-Ops Threat Research. „Jeder, der ScreenConnect nutzt, sollte Maßnahmen ergreifen, um anfällige Server und Clients sofort zu isolieren, sie zu patchen und auf Anzeichen einer Kompromittierung zu prüfen. Sophos bietet umfassende Anleitungen und Threat-Hunting-Materialien von Sophos X-Ops als Hilfestellung. Wir setzen unsere Untersuchungen fort und werden bei Bedarf Aktualisierungen vornehmen.“

Die Malware-Aktivitäten der letzten 48 Stunden und der Einsatz von Lockbit-Technologie könnte die Vermutung von Chester Wisniewski bestätigen, dass Teile der Lockbit Gruppe nach wie vor aktiv sind oder die Lockbit Malware-Technologie bei anderen Gruppen auch weiterhin Anwendung findet.

Was Anwender von ScreenConnect jetzt unbedingt unternehmen sollten, ist im Bericht von Sophos detailliert beschrieben.

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/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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