Suche nach den „Fab Five“:
USA bieten "bis zu 10 Millionen Dollar" Belohnung für Informationen über die Conti-Bande

Das Wort Conti ist im Zusammenhang mit Cyberkriminalität inzwischen vielen geläufig. Hinter dem Namen Conti steckt eine bekannte Ransomware-Gang – genauer gesagt eine so genannte Ransomware-as-a-Service (RaaS)-Bande. Bei diesem kriminellen Geschäftsmodell wird der der Part der Ransomware-Code-Erstellung, der Erpressung und der Entgegennahme von Erpressungszahlungen von verzweifelten Opfern von einer Kerngruppe übernommen, während die Angriffe selbst von einem lose zusammengesetzten "Team" von Mitgliedern durchgeführt werden. Und diese werden in der Regel nicht wegen ihrer Fähigkeiten zur Malware-Programmierung, sondern wegen ihrer Fähigkeiten in den Bereichen Phishing, Social Engineering und Netzwerkeinbruch rekrutiert.

Diese „Partner“ stecken etwa 70 Prozent der Gelder, die von den Opfern erpresst werden, ein. Das ist ein erheblicher Anreiz dafür, gleich ganze Netzwerke mit einem Schlag anzugreifen und zu infizieren.

Gezielte Rekrutierung von Gangs ist gang und gäbe
Vor etwa zwei Jahren beispielsweise bot die REvil-Ransomware-Bande in einem Hacker-Rekrutierungsforum im Untergrund 1.000.000 Dollar als Vorschuss an, um neue Affiliates für ihre cyberkriminellen Machenschaften zu gewinnen. Die entsprechende REvil „Stellenanzeige“ klang nach einer Kernmannschaft von RaaS. Man suchte „Teams, die bereits über Erfahrungen und Fähigkeiten bei Penetrationstests sowie mit msf / cs / koadic, nas / tape, hyper-v und ähnlichen Software- und Gerätetypen verfügen.“

Die REvil-Bande hatte ein besonderes Interesse an Technologien wie NAS (Networked Attached Storage), oder Hyper-V (Microsofts Virtualisierungsplattform), da mit entsprechender Expertise beispielsweise vorhandene Backups während eines Angriffs mit allem anderen verschlüsselt werden können. Dies macht es den Opfern schwerer denn je, sich selbst zu retten.

Meuterei auf der Conti
Die symbiotischen Beziehungen zwischen den Kernmitgliedern einer RaaS-Gang und den angeschlossenen Mitgliedern, auf die sie sich verlassen, sind indes durchaus fragil. So hatte etwa die Conti-Crew vor etwas mehr als einem Jahr mit einer Art Meuterei in den eigenen Reihen zu kämpfen, wie ein wütender Post offenbarte: „Ja, natürlich rekrutieren sie Trottel und teilen das Geld unter sich auf, und die Jungs werden mit dem gefüttert, was sie ihnen mitteilen werden, wenn das Opfer zahlt,“ hieß es da. Einer der verärgerten Partner hatte zudem eine umfangreiche Archivdatei mit dem Titel Мануали для работяг и софт.rar (Bedienungsanleitungen und Software) veröffentlicht, die sich auf die Conti-Bande bezieht.

Zum Hintergrund des Posts konnte Sophos seinerzeit herausfinden, dass zumindest einige Partner in der Conti-Ransomware-Szene eben nicht 70 % der tatsächlich eingenommenen Lösegeldsumme erhielten, sondern 70 % einer imaginären, aber niedrigeren Summe, die ihnen von den Kernmitgliedern der Conti-Bande mitgeteilt wurde.

USA loben bis zu 10 Millionen Belohnung für Hinweise aus
Die Vereinigten Staaten haben gerade offiziell und öffentlich eine Belohnung von "bis zu 10 Millionen Dollar" unter dem Schlagwort Conti ausgesetzt. Auszüge aus der Begründung: *„Die erstmals 2019 entdeckte Ransomware Conti wurde für mehr als 1.000 Ransomware-*

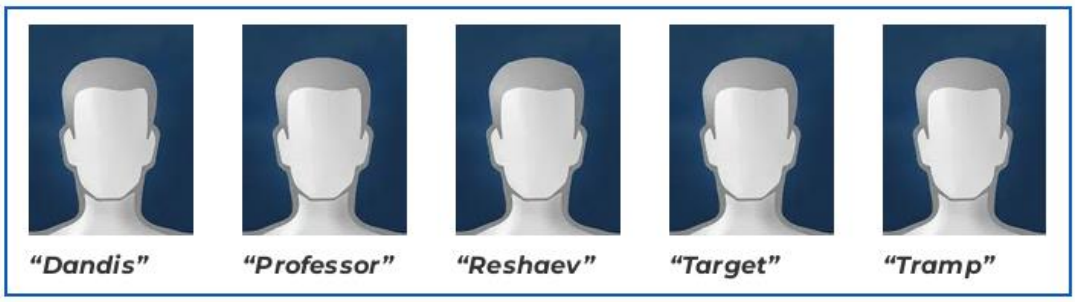
Operationen verwendet, die auf kritische Infrastrukturen in den USA und weltweit abzielten, wie z. B. Strafverfolgungsbehörden, medizinische Notdienste, Notrufzentralen und Gemeinden. Netzwerke des Gesundheitswesens und der Ersthelfer gehören zu den mehr als 400 Organisationen weltweit, die Opfer von Conti wurden, mehr als 290 davon in den Vereinigten Staaten.“

Die Zahlung der Belohnung für Hinweisgebende erfolgt im Rahmen einer globalen US-Initiative zur Verbrechens- und Terrorismusbekämpfung, die unter dem Namen Rewards for Justice (RfJ) bekannt ist und vom diplomatischen Dienst der USA im Auftrag des US-Außenministeriums verwaltet wird. Obwohl es unwahrscheinlich ist, dass ein einzelner Hinweisgeber in der Conti-Saga die gesamten 10 Millionen Dollar für sich beanspruchen werden kann, bleiben auch für weitere Informanten genügend finanzielle Anreize, um sachdienliche Hinweise zu geben.

Wer sind die Fab Five?
Das RfJ-Programm selbst besteht seit fast 40 Jahren und hat in dieser Zeit nach eigenen Angaben etwa 250 Millionen Dollar an mehr als 125 verschiedene Personen weltweit ausgezahlt, was einer durchschnittlichen Auszahlung von etwa 2.000.000 Dollar etwa dreimal pro Jahr entspricht. Auszug aus einer allgemeinen Beschreibung:
„Das RfJ-Programm bietet eine Belohnung von bis zu 10 Millionen Dollar für Informationen, die zur Identifizierung oder zum Auffinden einer Person führen, die auf Anweisung oder unter der Kontrolle einer ausländischen Regierung an böswilligen Cyber-Aktivitäten gegen kritische US-Infrastrukturen unter Verletzung des Computer Fraud and Abuse Act (CFAA) beteiligt ist.“

Diesmal hat das US-Außenministerium jedoch ein ausdrückliches Interesse an fünf Personen bekundet, die im Moment nur unter ihren Untergrundnamen bekannt sind: Dandis, Professor, Reshaev, Target und Tramp.

Fahndungsfotos für die optische Identifizierung scheint es keine zu geben. Die RfJ-Seite zeigt lediglich Dummies.



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, +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