Trojaner gefangen

Ermittlern gelingt Schlag gegen Emotet-Infrastruktur

Nach mehr als zwei Jahren Ermittlungsarbeit haben Behörden aus acht Ländern nach eigenen Angaben die Infrastruktur der Schadsoftware Emotet „übernommen und ausgeschaltet“. Doch das muss nicht bedeuten, dass der Trojaner erledigt ist.

Von Wilhelm Drehling

Fahndern aus Deutschland, den Niederlanden, der Ukraine, Litauen, Frankreich sowie England, Kanada und den USA gelang es Ende Januar, Emotet einen empfindlichen Schlag zu versetzen. Unter der Leitung von Europol und Eurojust, der EU-Agentur für justizielle Zusammenarbeit in Strafsachen, beschlagnahmten die Ermittler Server der Hintermänner unter anderem in den Niederlanden, Litauen, England und Deutschland.

Emotet fällt

Damit sei die Emotet-Infrastruktur „zerschlagen“ worden, teilte das Bundeskriminalamt (BKA) mit. In Deutschland war an den seit 2018 geführten Ermittlungen neben dem BKA auch die Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) der Generalstaatsanwaltschaft Frankfurt am Main beteiligt. Die Strafverfolgungsbehörden deaktivierten eigenen Angaben zufolge insgesamt mehr als 100 Server, darunter 17 hierzulande. Die Server in Deutschland seien der Anfang der Spur gewesen. Das BKA habe die Daten gesammelt und nach weiteren Analysen auch Server in anderen europäischen Staaten lokalisiert.

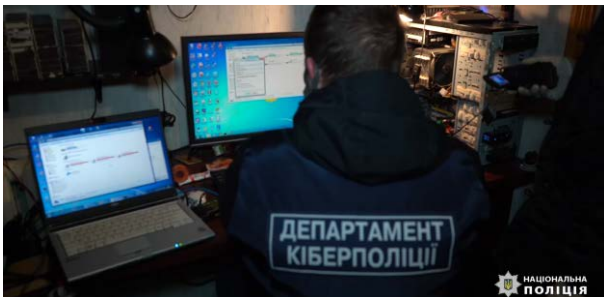
Laut der Aussage des BKA ist die Infrastruktur der Schadsoftware unschädlich gemacht und in der Ukraine sogar übernommen worden. In einem Video, das die ukrainischen Behörden auf YouTube veröffentlicht haben, sieht man einen spektakulären Einsatz: Die Polizei stürmt in voller Montur ein Gebäude und stellt mehrere Computer, Festplatten, Geld und Goldbarren sicher (hier ansehen: ct.de/yrk6).

Wie die Ermittler die Verbindung zu den Drahtziehern im Detail gekappt haben und ob das bereits auf allen mit dem Emotet-Netzwerk verbundenen Opfer-PCs geschehen ist, ist bislang unbekannt. Die Strafverfolgungsbehörden haben nach eigenem Bekunden den Schädling auf infizierten Geräten in Quarantäne verschoben – mit Hilfe der in der Ukraine übernommenen Server. Mit diesem Schritt wollen sie sicherstellen, dass die Emotet-Macher keinen Zugriff mehr auf die infizierten Computer haben.

Um möglichst viele infizierte Systeme ausfindig zu machen, wertet das BKA nun Daten wie IP-Adressen der Opfersysteme aus und stellt die gesammelten Informationen zusätzlich dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Verfügung. Das BSI nimmt Kontakt zu den Internet-Providern auf und will diese bitten, Opfer zu benachrichtigen.

(wid@ct.de) c't

Einsatz der ukrainischen Polizei ansehen: ct.de/yrk6



YouTube: https://www.youtube.com/watch?v=_BLOmClsSpc

Behörden aus der Ukraine dokumentierten akribisch, was sie in der Wohnung eines mutmaßlichen Mitglieds der Emotet-Gang fanden – darunter auch mehrere Windows-Computer.

Das ist Emotet

Der Schädling tauchte 2014 das erste Mal auf und treibt seitdem sein Unwesen. In erster Linie haben es die Hintermänner auf Unternehmen und nicht Privatpersonen abgesehen. Emotet korrumpiert Computer in kürzester Zeit und breitet sich rasant in Netzwerken aus.

Hat sich der Schädling erst mal eingenistet, durchsucht er unter anderem automatisiert E-Mail-Konversationen, analysiert diese und verschickt auf dieser Basis zum Teil sehr gut gefälschte Mails. Diese Spam-Angriffe kommen oft im Namen von Kollegen. In den Nachrichten wollen die Betrüger Opfer mit Betreffzeilen und Texten zu real existierenden Firmenprojekten aufs Glatteis führen. Im Anhang befindet sich häufig eine verseuchte Word-Datei, die beim Öffnen ein Makro aktiviert, das Emotet herunterlädt. Nach der Installation agiert Emotet als Türöffner für weitere Schadsoftware und holt zum Beispiel den Verschlüsselungstrojaner Ryuk oder die Malware Trickbot auf Systeme.

Seit der Entdeckung richtete Emotet in Deutschland Schaden in Millionenhöhe an. Zu den Opfern gehören beispielsweise das Klinikum Fürstenfeldbruck, die Uni Gießen, das Berliner Kammergericht und die Heise-Gruppe. Ryuk erpresste international laut Angaben des FBI eine Summe von mehr als 61 Millionen US-Dollar. Die Dunkelziffer ist vermutlich weitaus höher, da viele Unternehmen eine Infektion ihres Netzwerkes nicht zur Anzeige bringen.

Ist der König wirklich tot?

Eine Analyse von Jürgen Schmidt (Leiter von heise Security)

Nach der Übernahme der IT-Infrastruktur der Emotet-Bande wecken die Ermittler die Hoffnung, dass dies das Ende der Bedrohung durch Erpressungstrojaner bedeuten könnte. Oder, dass man zumindest einen deutlichen Rückgang der Gefahr bilanzieren kann. Schließlich war Emotet ja angeblich der „König der Schadsoftware“ (nicht meine Worte!).

Doch so sehr ich mich freue, dass da tatsächlich ein Wirkungstreffer gegen das organisierte Verbrechen erzielt wurde, so wenig Hoffnung habe ich, dass das bereits ausreichen könnte, um die Situation deutlich zu entspannen. Dafür gibt es eine Reihe von Gründen:

Erster Grund ist, dass Emotet gar nicht selbst erpresst. Das Geschäftsmodell der Emotet-Bande ist das Installieren von Schadsoftware anderer Krimineller. So zahlte etwa die Trickbot-Bande viel Geld dafür, dass Emotet deren Unrat auf tausenden Rechnern nachinstallierte. Erst die Trickbot-Kriminellen verschlüsselten die Daten der Opfer und erpressten Lösegeld. Die Infrastruktur der Trickbot-Bande arbeitet komplett getrennt von Emotet; der Trojaner Trickbot ist somit nach wie vor voll funktionsfähig. Und obwohl der Emotet-Schädling unschädlich gemacht wurde, sind die vielen zehntausend Emotet-Opfer mit Trickbot auf ihrem System auch weiterhin akut in Gefahr.

Auch die Zukunft von Trickbot ist durch den Schlag gegen Emotet kaum gefährdet. Die Trickbot-Gang dahinter hat schon immer auf einen Mix von Einfallsvektoren gesetzt und drang etwa durch kompromittierte RDP-Server in Firmennetze ein. Sie wird sich für den ausgefallenen Dienstleister Emotet jetzt einfach einen Ersatz suchen. Die Cybercrime-Konkurrenz dürfte Schlange stehen, um das lukrative Geschäft zu übernehmen.

Apropos Konkurrenz: Zweiter Grund ist, dass Emotet damals Vorreiter war und zumindest noch vor zwei Jahren als etwas ganz Besonderes galt.

Doch die anderen Banden hinter Computerschädlingen wie Maze, Ragnar Locker und Dharma haben die Zeichen der Zeit längst erkannt und sind auf den Zug aufgesprungen. Tatsächlich haben sie in einigen Aspekten das Duo Emotet/Trickbot bereits überholt. Maze zum Beispiel hat eine eigene Enthüllungsplattform aufgebaut, um die Opfer zusätzlich mit der Veröffentlichung von internen Daten zu erpressen.

Dharma hat eine Art „Erpressung-as-a-Service“-Netzwerk aufgebaut: ein riesiges Netz von kleineren Banden, die die Dharma-Trojaner auf verschiedenste Weisen verbreiten und für jeden erfolgreichen Erpressungsfall Provision kassieren. Überhaupt ist aktuell zu beobachten, dass sich die Cybercrime-Welt immer weiter spezialisiert. So betreiben die einen im Hintergrund die benötigte Infrastruktur und liefern die benötigte Schadsoftware, während sich andere mit dem eigentlichen Einbruch die Hände schmutzig machen.

Ich glaube auch nicht, dass der Schlag gegen Emotet die Konkurrenten so weit eingeschüchtert hat, dass sie ihre Aktivitäten jetzt zurückfahren. Im Gegenteil: Sie dürften den Ausfall des größten Konkurrenten eher als ihre Chance sehen, sich jetzt ein größeres Stück vom Kuchen zu greifen.

Drittens: Emotet selbst ist noch nicht unbedingt schachmatt. Zwar wurden im Zuge der Beschlagnahmungen etwa in der Ukraine auch mutmaßliche Bandenmitglieder verhaftet. Doch noch ist unklar, wie entscheidend die für die Operationen tatsächlich waren. Solange es nicht gelingt, die Köpfe der Bande aus dem Verkehr zu ziehen, besteht die Gefahr, dass sie nach einer Pause mit neuem Team und neuer Infrastruktur zurückkehren. Es wäre nicht die erste Cybercrime-Bande, der ein Comeback gelingt. GrandCab setzte sich angeblich im Mai 2019 zur Ruhe – nur um wenig später mit dem Erpressungs-Trojaner REvil/Sodinokibi für Schlagzeilen zu sorgen.

Der aktuelle Schlag gegen Emotet ist somit zwar ein wichtiges Signal, dass Cybercrime keine risikolose Gelddruckmaschinerie für organisiertes Verbrechen ist. Dass also der Verstoß gegen Gesetze auch eine reale Gefahr mit sich bringt, dafür zur Rechenschaft gezogen zu werden. Sowohl für die IT-Security-Mitarbeiter von gefährdeten Unternehmen als auch für Ermittler dürfte das bestenfalls eine kurze Atempause bedeuten.