FOTOS: DEPARTMENT OF CYBERPOLICE UKRAINE

Anschlag auf den König

Das Emotet-Netzwerk war eine der gefährlichsten Plattformen für Cyberattacken weltweit und verursachte bei Unternehmen, Behörden und Hochschulen Milliardenschäden. Bis Ermittler die Schadsoftware mit einer gewagten Strategie lahmlegten. Rekonstruktion einer digitalen Verfolgungsjagd.

TEXT THOMAS KUHN

Die Häuserblocks am Rand der ostukrainischen Industriestadt Charkiw haben ihre besten Zeiten hinter sich. Rollläden hängen schief, manche Balkone sind mit Planen abgehängt, an den Fassaden bröckeln die Fliesen. In dieser unspektakulären Kulisse, im Obergeschoss von Haus 55, soll sich die Schaltzentrale eines kriminellen Cyberimperiums befinden: Emotet.

Am frühen Morgen des 26. Januar dieses Jahres öffnen sich die Türen einiger davor parkender Kleinbusse, heraus stürzen Spezialkräfte der ukrainischen Nationalpolizei. Sie überrumpeln einen Mann in seiner mit Computern, Bildschirmen und Netzwerktechnik zu einem improvisierten Kontrollzentrum umgerüsteten Bleibe. Hier wurde das bis heute größte bekannte Cybercrimenetzwerk gesteuert, mit dem Kriminelle sieben Jahre lang weltweit Milliarden erbeuteten. Gestützt auf Gespräche mit Ermittlern und Informanten aus der IT-Szene, lässt sich erstmals detailliert dokumentieren, wie es den Fahndern gelang, die Strukturen dieses Netzes zu durchdringen und es mit einer ebenso riskanten wie einzigartigen Strategie auszuschalten.

Zugriff im Morgengrauen
Im ostukrainischen Charkiw stellten Spezialkräfte der Polizei den Netzwerkmanager von Emotet

Juni 2014
Die unterschätzte Gefahr

Als Joie Salvio, Risikoanalyst beim IT-Sicherheitsdienstleister Trend Micro, am 27. Juni 2014 einen Bericht zu einer neu entdeckten Schadsoftware veröffentlicht, liest sich die Warnung wie viele andere zuvor. Millionenfach flutet schädliche Software das Netz. In dessen dunklen Ecken hat sich eine florierende Schattenwirtschaft etabliert: Manche Hacker haben sich auf den Versand von Spam- und Phishingnachrichten spezialisiert, andere auf den Einbruch in Computersysteme. Einigen geht es um Sabotage, andere durchforsten geknackte Rechner nach verwertbaren Informationen. Cyberkriminelle betreiben sogar Callcenter, um Erpressungsopfern, nachdem sie Lösegeld gezahlt haben, die Rechner zu entschlüsseln.

Salvio nennt die neue Schadsoftware Emotet, „eine weitere Schadsoftware“, die sich mithilfe gefälschter E-Mails verbreite und „darauf ziele, die Zugangsdaten von Bankkonten zu stehlen“. Im Visier scheinen vor allem deutschsprachige Bankkunden zu sein. Doch die Warnung nimmt kaum jemand wahr. So entsteht, anfangs unter dem Radar von Sicherheitsexperten und erst recht außerhalb des Bewusstseins der Menschen, die ihre Bankgeschäfte im Netz regeln, ein Softwareschädling, der in seiner Wirkweise und im dahinter liegenden Geschäftsmodell einzigartig ist.

Ins öffentliche Bewusstsein gelangt Emotet erst Anfang 2018, als Hacker damit das IT-Netz der Stadtverwaltung von Allentown im US-Bundesstaat Pennsylvania lahmlegen und eine Million Dollar Schaden verursachen. Dann schwappt die Welle um den Globus. Allein in Deutschland werden Ermittler Zehntausende befallene Rechner zählen, werden im Netz etwa 35 Millionen Datensätze mit Zugangsinformationen zu Konten kursieren, die Kriminelle mithilfe von Emotet gesammelt haben.

Spätsommer 2018
Ein erster schwerer Fehler

Es ist ein Routinetermin, zu dem Arne Schönbohm und Holger Münch, die Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Bundeskriminalamtes (BKA), allmonatlich verabredet sind. Doch diesmal geht es vor allem um ein Thema: Emotet. Dessen Entwickler haben das Spionageprogramm inzwischen zu einer kriminellen Serviceplattform ausgebaut, die es ihnen erlaubt, weitere Schad- ▶

software auf mit dem Emotet-Virus infizierten Rechnern zu installieren oder von dort weiter zu verbreiten. Diese Dienstleistung verkaufen sie mit Erfolg an andere Kriminelle. Die Zahl der Attacken steigt rasant. Zwar gelinge es, den Schädling aus den Regierungsnetzen herauszuhalten, in der Wirtschaft aber habe er „erhebliche Durchschlagswirkung“, berichtet Schönbohm. Er wird Emotet später den „König der Schadsoftware“ nennen.

Die Behördenchefs beschließen, den Ermittlungen gegen das Netzwerk mehr Gewicht zu geben, sich stärker auszutauschen. Regelmäßig schickt das BSI von nun an seine Reports ans BKA, bis wenig später ein echter Schatz für die Ermittler darin steckt. Zu verdanken haben sie ihn der Nachlässigkeit der global vernetzten Kriminellen. Ort des Leichtsinns: Brasilien.

Spätherbst 2018
Ein grober Bauplan des Netzes

Vier Jahre haben die Verbrecher von den Verästelungen des deutschen Föderalismus profitiert. Die Ermittlungen lokaler Polizeibehörden blieben erfolglos. Nun entscheidet das BKA mit der zuständigen Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) bei der Frankfurter Generalstaatsanwaltschaft, die Ermittlungen bundesweit zusammenzuführen.

In den Datenbeständen, die ihnen die Forensiker des BSI weitergeleitet haben, stoßen die Fahnder vom BKA auf die Log-Dateien eines Servers aus Brasilien. Darin enthalten: detaillierte Kommunikationsdaten, anhand derer die Ermittler über eineinhalb Jahre verfolgen können, mit welchen Rechnern der brasilianische Emotet-Server weltweit kommuniziert hat – auch in Deutschland. „Normalerweise achten Kriminelle darauf, dass diese Log-Dateien gelöscht und mehrfach überschrieben werden“, sagt Carsten Meywirth, Chef der zuständigen Abteilung Cybercrime beim BKA. „Aber Menschen machen Fehler, auch Hacker.“

Schritt für Schritt hangeln sich die Ermittler in den folgenden Wochen von IP-Adresse zu IP-Adresse, die so etwas sind wie die Hausnummern von im Internet verbundenen Computern. Langsam entsteht ein grober Bauplan des Netzes. Bei einer Frage aber tappen die Fahnder im Dunkeln: Arbeitet die Cybercrimeplattform dezentral – oder gibt es einen Knoten im Netz, auf den alle Kommunikationswege zulaufen, eine Spinne, die alles steuert?

Klar hingegen ist, dass sich der Schädling über E-Mails verbreitet (Grafik Seite 70). Einmal aktiviert, installiert sich das Programm unauffällig im Hintergrund. Statt sofort die Rechner zu manipulieren, liest dieser Trojaner das E-Mail-Postfach der Opfer aus, kopiert ältere Nachrichten aus dem Posteingang und schickt passend wirkende Antworten an deren Absender. Im Anhang: ein mit einer neuen Emotet-Kopie verseuchtes Word-Dokument.

Frühjahr 2019
Tarnung auf Knopfdruck

Inzwischen ist den Fahndern klar: Ihre Befehle bekommen die infizierten Rechner über eine Kette aus Kontrollrechnern, die die Ermittler als T1-, T2- und T3-Server bezeichnen. Anders als viele andere Schadprogramme aber ist Emotet modular konzipiert, sodass die Kriminellen ihre Infrastruktur quasi auf Knopfdruck immer wieder verändern und damit tarnen können. „Rechner, die wir eben noch als Teil des Netzes identifiziert hatten, sind tags darauf plötzlich bei Emotet außen vor“, erläutert BKA-Mann Meywirth. Es ist, als versuchten die Fahnder ein Hehlernetz zu zerschlagen. Immer wieder, wenn sie anrücken, um getarnte Lager hochzunehmen, finden sie Hallen leer vor.

2,5

Milliarden Dollar Schaden hat das Hackernetzwerk Emotet in rund sieben Jahren mindestens verursacht, ergaben Berechnungen der ukrainischen Cyberpolizei

Trotzdem gelingt es den Ermittlern schrittweise, über die IP-Adressen immer mehr relevante Server in Deutschland und Europa zu identifizieren. Auf richterliche Anordnung und unbemerkt von den Hackern überwachen sie den Datenverkehr zu den relevanten Computersystemen. Ähnliches tun Ermittler in den USA, Kanada, Frankreich und Großbritannien, die nun ebenfalls eingebunden sind.

Sommer 2019
Unerreichbare Spinne im Netz

Kurz nach Pfingsten verstummt das Emotet-Netzwerk schlagartig. „Quasi von einem auf den anderen Tag herrschte komplette Funkstille im Netz“, beschreibt BKA-Mann Meywirth den Schreckmoment. Hatten die Hacker Wind bekommen von den Ermittlungen? Waren die Fahnder aufgeflogen? „Wir haben fieberhaft nach möglichen Fehlern gesucht oder nach irgendwelchen Tricks, mit denen die Emotet-Betreiber ihren Datenverkehr vor uns hätten verbergen können.“ Zunächst ohne Erfolg.

Bis sich bestimmte Kontrollserver für einen kurzen Moment wieder rühren, freilich mit ganz anderen IP-Adressen als zuvor. Die Fahnder können die Spur zurückverfolgen und landen in einer bekannten Ferienregion. Offenbar machen auch Hacker mal Urlaub und schicken ihr Netzwerk in den Dämmerschlaf. Der endet am 23. August. Da verschicken die Experten des BSI eine Warnung an die IT-Experten: „Seit dem Vormittag ist Emotet wieder aktiv.“

Und wie: Reihenweise legen die Angreifer Behörden und Unternehmen lahm. Im September trifft es das Berliner Kammergericht, kurz darauf die Humboldt-Universität. Die Hochschulen in Freiburg und Hannover folgen. Die Stadtverwaltungen von Frankfurt und Bad Homburg müssen nach Emotet-Infektionen ihre IT abschalten. Hacker, die ihre Schadprogramme über Emotet verbreiten, attackieren Krankenhäuser in den USA, Großbritannien, aber auch Deutschland, etwa in Fürstenfeldbruck und Fürth.

Zugleich liefern die Hacker den Ermittlern immer neue Datenspuren. Terabyte um Terabyte protokollieren die Ermittler. Dabei zeigt sich: An die zentrale Spinne im Netz, die Kriminellen hinter den T3-Servern, in der IT-Szene inzwischen „Mummy Spider“ genannt, kommen die Fahnder vorerst nicht heran. Deren Rechner stehen in Staaten, die für die Strafverfolger nur schwer zugänglich sind. Geschützt durch Justizbehörden, die „alle nationalen und internationalen Anfragen, Rechtshilfeersuchen, Mitfahndungsbitten, alles beharrlich ignorieren“, stellt ein Fahnder frustriert fest. Immerhin, zumindest über Umwege lassen sich die Täter trotzdem verfolgen.

Herbst 2019
Verborgene Kanäle in die Ukraine

In Deutschland stoßen die Fahnder auf einen Server, der eine besondere Rolle im Hackernetzwerk zu haben scheint: Er kommuniziert nicht bloß mit gehackten Rechnern aller Hierarchiestufen und speist unter anderem neue Varianten der Schadsoftware ein. Er verbindet sich zudem mit allen drei Emotet-Teilnetzen, obwohl die sonst strikt getrennt sind. Warum aber empfängt dieser Server selbst keinerlei Steuerbefehle? Es dauert Tage, bis die Fahnder die Lösung fin-

Auf der Spur der Erpressung
Koordiniert von Europol (o.), jagten Fahnder aus acht Ländern die Hacker, die Krankenhäuser, Konzerne und Behörden attackiert hatten

FOTOS: LAIF/HOLLANDSE HOOGTE, LAIF/JENS SCHWARZ

den: Die Kontrolle des rätselhaften Servers läuft über einen verdeckten, kaum genutzten Kanal. Absender für diese Befehle: ein Rechner, der in der Ukraine steht. Und „mit deren Justizbehörden funktioniert die Zusammenarbeit bestens“, sagt Linda Bertram, die als Staatsanwältin die Emotet-Ermittlungen am ZIT in Frankfurt leitet. So wird bald klar: Es ist der Kontrollrechner selbst, der da in einem Plattenbau am Rande von Charkiw steht.

Warum aber kommuniziert der Administrator so sorglos? BKA-Mann Meywirth hat nur eine Erklärung: „Der konnte sich bei all dem Aufwand, den er mit dem verborgenen Datenkanal getrieben hat, nicht vorstellen, dass ihm noch einer auf die Schliche kommt.“ Kommen die Fahnder aber doch. Puzzleteil um Puzzleteil fügen sich die Details zum Bild der Netzwerkstrukturen.

Sommer 2020
Die Angst vor Schlupflöchern

Für die Fahnder ist es essenziell, alle Strukturen dieses Netzwerks gut zu kartieren, um sie am Ende auch stilllegen zu können. „Ansonsten könnten die Hinterleute von Emotet ihr Netzwerk nach einem Zugriff der Sicherheitsbehörden einfach wieder reaktivieren“, sagt Daan de Graaf von der Hightech-Crime-Abteilung der niederländischen Polizei. Auch die ist inzwischen Teil der Fahndungstruppe. Und wird bald eine zentrale Rolle übernehmen.

Denn die Niederlande zählen weltweit zu den Staaten mit der besten Internetanbindung, den größten Rechenzentren und den schnellsten Onlineverbindungen. Das machen sich die Betreiber von Emotet zunutze. Da ihr Netzwerk rasant wächst, buchen sie nun ganz regulär Rechnerkapazitäten dort, wo die Technik schnell, stabil und billig ist.

Herbst 2020
Hacker vor der Haustür

Im Oktober zeigen die Überwachungssysteme der Niederländer plötzlich, dass zwei der drei T3-Server nicht mehr über IP-Adressen aus Staaten kommunizieren, die für die Fahnder unerreichbar sind. Stattdessen haben sie IP-Adressen, die in niederländische Rechenzentren führen. „Plötzlich schlug das Herz des Netzes quasi direkt vor unserer Haustür“, sagt de Graaf. „Ich habe meinen Augen gar nicht getraut.“ Der überraschende Umzug zeigt, dass die Ermittler vor allem eines brauchen: Geduld. „Die Kriminellen müssen alles richtig machen, um anonym zu bleiben, wir hingegen müssen nur auf einen Fehler warten, den sie machen“, sagt Philipp Amann, Strategiechef der Abteilung EC3, die bei der europäischen Polizeibehörde Europol die Jagd auf Emotet koordiniert. Kehrseite des Geduldspiels: Solange die Hacker keine Fehler machen, können sie ihrem Geschäft ungestört nachgehen. Bei Emotet mehr als sechs Jahre.

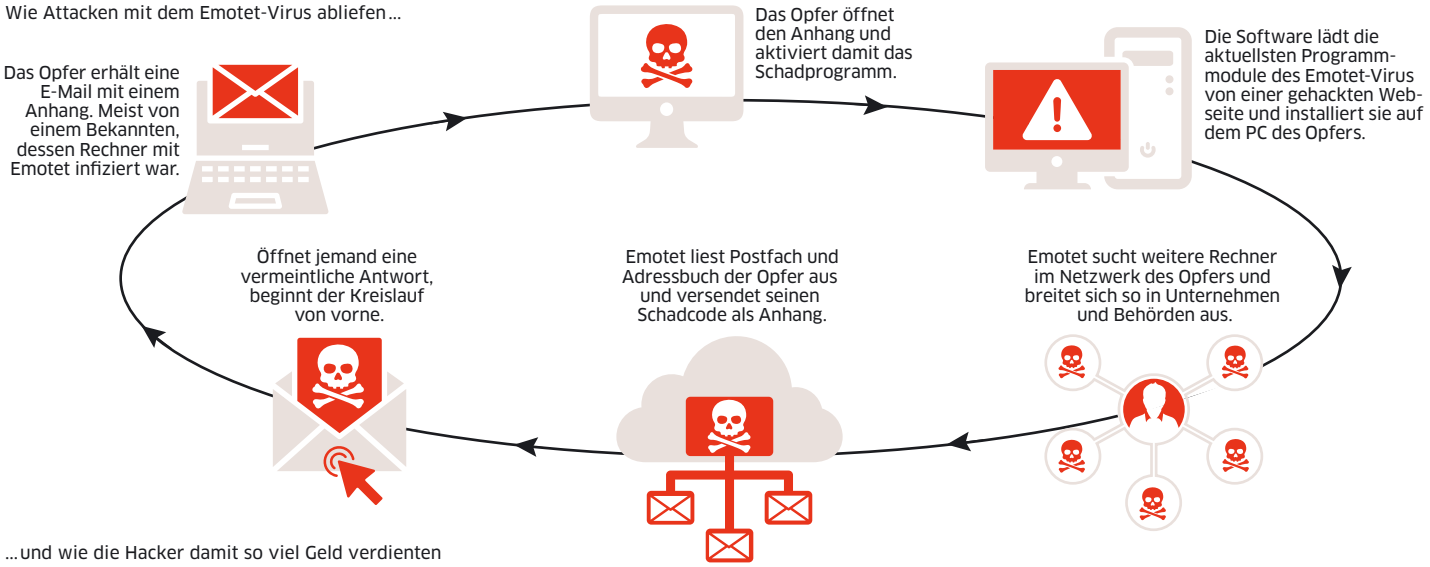
Der Umzug in die Niederlande erweist sich gleich als doppelter Fehler. Dort können die Ermittler auf den Rechnern nicht bloß ihre Abhörtechnik installieren, sondern auch Krypto-Schlüssel kopieren, mit denen die Hacker ihren weltweiten Datenverkehr absichern. Und so gelingt endlich, woran sich die Fahnder seit Jahren die Zähne ausbeißen: Ein Team von IT-Spezialisten, die die Rechner infiltrieren, verschafft ihnen Zugriff auf die Steuerung der T3-Server. Die Hacker selbst sind gehackt. Jetzt können die Ermittler den Zugriff vorbereiten.

Winter 2020
Ein technischer Kunstgriff

Die Strategie, die Deutsche und Niederländer entwickeln, ist ebenso ungewöhnlich wie riskant. Sie wollen nicht nur die wichtigsten Server konfiszieren und die zentralen Verbindungen kappen, sondern die Infrastruktur als Ganzes abschalten. Ihr Plan: über die Computer des Netzwerkadministrators in der Ukraine ein modifiziertes Pro- ▶

KRIMINELLE GELDDRUCKMASCHINE

Wie Attacken mit dem Emotet-Virus abliefen …



… und wie die Hacker damit so viel Geld verdienten

Das Virus im infizierten PC meldet sich bei einem Kontrollserver des Emotet-Netzwerks und lädt weitere Schadsoftware, für deren Verbreitung Hacker die Emotet-Infrastruktur gemietet haben.

Für jede erfolgreiche Installation von Spionage- oder Erpressungssoftware zahlen Cyberkriminelle den Emotet-Betreibern eine Provision.

Hat Emotet Verschlüsselungssoftware auf PCs geladen, müssen die Opfer hohe Lösegelder zahlen, um wieder Zugriff auf ihre Daten zu bekommen.

Emotet zeichnet beim Opfer Zugangsdaten für Onlinebanking und anderes auf und sendet sie an die Emotet-Betreiber, die sie an andere Kriminelle verkaufen.

Quelle: Eigene Recherche

grammmodul einschleusen. Das soll sich mithilfe automatischer Updates von allein im Netzwerk verbreiten. Das Modul würde jeden Rechner, den es so erreicht, aus dem Emotet-Netz abmelden, das Schadprogramm für die Ermittler sichern und den Rechner als gesichert bei einer Datenbank melden, die das BKA in Wiesbaden installiert. Das Vorgehen ist rechtlich umstritten.

Denn eigenen Programmcode auf fremden Rechnern auszuführen, das lässt das deutsche Recht nur unter großen Auflagen zu. Also beschränken die BKA-Ermittler die geplante Injektion auf eine „Beschlagnahmung mit technischen Mitteln“, bei der das Ausschalten des Schadcodes auf den infizierten Rechnern nur ein Nebeneffekt der Beweissicherung ist. Dem zuständigen Gericht in Gießen genügt das.

Zudem ist der Zugriff technisch eine Gratwanderung. Denn die Infiltrierung muss gelingen, ohne dass die Rechner abstürzen, wenn die Tätersoftware auf den Computern in Quarantäne verschoben wird. „Schlimmstenfalls hätten wir Zigtausende Rechner gecrasht“, sagt BKA-Abteilungsleiter Meywirth. „Deswegen waren wir besonders gründlich, um das Risiko am Einsatztag gering zu halten.“

Januar 2021
Zugriff nach Plan B

Es ist gegen vier Uhr früh am 26. Januar, als sich der niederländische Ermittler de Graaf und Experten weiterer Sicherheitsbehörden in einem Besprechungsraum der Europol-Zentrale in Den Haag versammeln. Wenig später trifft sich auch ein BKA-Team um Emotet-Jäger Meywirth im Lageraum der Wiesbadener Behörde. Bildschirme an den Wänden zeigen den Datenverkehr im Emotet-Netz, die Liste angemeldeter Server und wer von den Hackern wo eingewählt ist. Der Zugriff auf die Rechner des Administrators soll erfolgen, sobald der Mann sich wie sonst üblich von seinem Büro in einem anderen Viertel von Charkiw ins Netzwerk einloggt.

An diesem Dienstag aber läuft es nicht nach Plan. Der Verdächtige verlässt seine Wohnung nicht, melden Observationsteams. Stattdessen wählt er sich plötzlich von seiner Wohnung aus ins Emotet-Netz ein. Hektisch ändern die Fahnder ihren Plan, gehen in der Nachbarschaft in Stellung. Und entscheiden sich für den Zugriff – in Charkiw und gleichzeitig in Rechenzentren weltweit. In Wiesbaden verfolgt Staatsanwältin Bertram mit dem Team um BKA-Mann Meywirth gebannt das weitere Geschehen. Schaltet der Mann seine Rechner noch ab? Aktiviert er bisher unentdeckte Backups, um das Netz vor dem Zugriff der Fahnder zu sichern?

Nichts dergleichen passiert. „Tatsächlich erfolgt der Zugriff fast unreal geschmeidig“, staunt Juristin Bertram. Nur Minuten nachdem die Software der Ermittler ins Emotet-Netz eingespielt ist, beginnt sie zu wirken. Mindestens 700 Kontroll- und Steuercomputer nehmen die Fahnder außer Betrieb. Bis zum Ende des Tages werden Zehntausende Rechner beschlagnahmt sein. Und in Charkiw stellt die Polizei derweil Computer und Kisten mit Festplatten sicher, Mobiltelefone und bündelweise Geldscheine, Bank- und Kreditkarten. In den Schränken finden sie mehr als 50 Gold- und Silberbarren, mehrere Kilo schwer.

Mai 2021
Der König ist tot

Die Ruhe nach dem Sturm hält an. Bis heute. Anders als bei anderen Hackernetzen bleibt die Emotet-Infrastruktur still. Die Fahndung aber läuft weiter. „Wir sind ja noch nicht fertig“, sagt Daan de Graaf. Charkiw, so viel ist klar, war nur der erste Schlag. „Der König ist tot“, sagt BKA-Mann Meywirth. „Und nun finden wir seine Leute.“ ■