ReporterFORUM

www.reporter-forum.de

Der Code des Bösen

Ein deutscher Informatiker sucht ein Thema für seine Doktorarbeit und gerät ins Getriebe der Weltpolitik. Denn er kommt einem der meistgesuchten Cyberkriminellen der Welt auf die Spur: Einem russischen Hacker, der womöglich auch ein Spion ist.

Von Marc Neller, WELT am SONNTAG, Medium, 01.05.2016

An einem düsteren Novembernachmittag, nach Wochen der Suche, gerät Christian Rossow durch einen Zufall ins Getriebe der Weltpolitik. Er sitzt in einem Büro, das gerade groß genug ist für zwei Schreibtische und einen Schrank, und kämpft sich durch einen Wust aus Zahlen, die auf seinem Computerbildschirm leuchten. Rossow hat darin etwas entdeckt.

Die Zahlen kommen aus dem Keller, ein Stockwerk unter ihm, aus einem Raum ohne Fenster. Nur vier Menschen außer Rossow haben einen Schlüssel. Der Raum ist ein Hochsicherheitslabor seiner Hochschule. Wenn Rossow dort etwas zu erledigen hat, beeilt er sich. Der Raum ist kalt und laut, eine alte Klimaanlage hält die Temperatur rund um die Uhr auf 19 Grad. Denn darin stehen 15 Hochleistungscomputer, groß und breit wie Kleiderschränke, sehr hitzeempfindlich. Rossow benutzt sie wie Versuchstiere. Er infiziert sie mit Erregern, mit den neuesten Viren, Trojanern und Würmern, die ihm die Hersteller von Antivirenprogrammen täglich schicken. Auf dem Bildschirm in seinem Büro kann er beobachten, was diese Viren anrichten. Nur eine Handvoll Computer sind mit dem Labor im Keller verbunden, durch ein spezielles Programm.

Gleich die erste Zahl auf Rossows Bildschirm bedeutet, dass im Keller ein Schadprogramm wütet, wie er es selten erlebt. Es kann sich in wenigen Minuten mit Hunderten fremden Computern verbinden. Genau das, was er sucht. Rossow macht ein paar Tests und schaut im Internet, ob sich schon mal jemand mit diesem Programm

beschäftigt hat, ein Technikfreak oder ein Wissenschaftler. Er findet nichts. Das ist es, denkt er, das perfekte Beispiel für seine Doktorarbeit.

Noch ohne es zu ahnen, beginnt Rossow an diesem Nachmittag, einen der meistgesuchten Cyberkriminellen der Welt zu jagen. Etwa fünf Jahre später wird er zu Hause auf einem schwarzen Ledersofa sitzen, mit blassem Gesicht, und die Geschichte seines Lebens erzählen, stolz und inzwischen auch ein bisschen besorgt. Ihm ist gelungen, was selten gelingt. Aber die Sache ist außer Kontrolle geraten.

Die USA haben ein Phantom gestellt, einen Meister des digitalen Diebstahls. Sein Name ist Jewgeni Michailowitsch Bogatschow, russischer Staatsbürger, 32 Jahre alt, ein Mann mit rundem Gesicht, kahl geschorenem Kopf und dunklen Rändern unter den Augen. Strafverfolger aus mehr als zehn Ländern waren hinter ihm her, sie haben Undercoveragenten auf ihn angesetzt, Nerds und die Giganten der Computerindustrie um Hilfe gebeten, Firmen wie Dell und Microsoft. Doch es waren Rossow und ein paar Bekannte, die Bogatschow mit seinen eigenen Waffen geschlagen haben.

Das FBI nennt Bogatschow einen Hacker von Weltformat. Denn er hat Programme geschrieben und vermietet, mit denen er, seine Helfer und seine Kunden auf Raubzüge gingen, hunderttausendfach.

Sein Programmpaket trägt den Namen "Gameover Zeus". Es ist eine Wortschöpfung, halb dem Computerspiel entlehnt, halb der griechischen Mythologie. Nichts geht mehr, wenn der oberste Gott des Olymp kommt, so in etwa könnte man sie übersetzen. Kein bescheidener Name, aber ein treffender. Denn Bogatschow hat ein digitales Werkzeug geschaffen, mit dem er und ein paar Helfer per Mausklick fremde Konten plündern, Computer sperren und Server lahmlegen konnten.

Nach Erkenntnissen des FBI haben Bogatschow und etwa 20 Helfer mit diesem Programm eine Million Computer in aller Welt infiziert. Seine Opfer waren Unternehmen, Banken und Privatleute. Einem Indianerstamm im US-Bundesstaat Washington soll er 277.000 Dollar gestohlen haben, einer Bank in Florida 6,9 Millionen. Man weiß nicht genau, wie viel Geld er insgesamt erbeutet, welchen Schaden er angerichtet hat. Das FBI geht von rund 100 Millionen Dollar aus, allein in

den USA. Wahrscheinlich war es also ein Vielfaches. Denn Bogatschow hat mit seinem Programm auch in Asien, in Europa, in Deutschland geraubt.

Er konnte sich sicher fühlen, jahrelang. Er hatte ein Verbrechen perfektioniert, das die Täter schützt und die andere Seite, Polizisten und Staatsanwälte, vor Aufgaben stellt, die sie ohne Spezialisten wie Rossow nicht lösen können.

Die Ermittler haben es mit Geistern zu tun, die sich hinter Kürzeln oder Kunstnamen verbergen. Ihnen fehlt fast alles, was sie üblicherweise brauchen, um einen Fall aufzuklären. Es gibt keinen Tatort, keine Fingerabdrücke, keine Spuren von Haut oder Haaren, die sich mithilfe von Genanalysen auswerten ließen, es gibt keine Zeugen und keine Täterbeschreibung.

Die Diebe des digitalen Zeitalters müssen in keine Bank, in keine Wohnung mehr einbrechen. Sie können Computerviren einsetzen, die ihre digitale DNS in fremde Rechner schleusen und, ganz von selbst, immer neue Rechner infizieren und große Schwärme von Computern schaffen, sogenannte Botnetze. Die Hacker können diese Botnetze im Verborgenen steuern, auf die Konten von Internetnutzern zugreifen, ihre Passwörter stehlen und ihr Geld. Bogatschows Programm konnte das perfekt. Es konnte sogar spionieren.

Die Ermittler reiben sich deshalb in einem ungleichen Kampf auf, oft jahrelang, meist vergeblich. Manchmal aber läuft es anders. Manchmal wird nach und nach hinter den Pseudonymen ein Mensch mit Gewohnheiten und Schwächen erkennbar, ein Täter, dessen Spur man verfolgen kann, wie in Bogatschows Fall. Die USA haben Bogatschow alias "slavik", "lucky12345" und "Pollingsoon" angeklagt. Das FBI ist stolz auf einen der seltenen großen Erfolge. Er wäre ohne Rossow so nicht möglich gewesen.

An einem klaren, kalten Freitagmorgen sitzt Rossow in seiner Dachgeschosswohnung in Dinslaken, westdeutsche Provinz, rot verklinkerte Einfamilienhäuser. Alles an ihm ist lang und schmal, sein Gesicht, sein Körper, seine Finger. Ein schwarzer Laptop, kaum größer als ein Blatt Papier, liegt griffbereit neben ihm auf dem Sofa. Er muss lachen, wenn er an seinen ersten Rechner denkt, einen IBM, einen großen Kasten.

Er war neun, als er in seinem Kinderzimmer saß, Doppelhaushälfte, und sein erstes Spiel programmierte. Er war elf, als das Internet in Mode kam und er Bekannten eigene Webseiten baute, damit sie Filme oder Bücher verkaufen konnten. Nach der Schule ließ er sich zum Fachinformatiker ausbilden, begann ein Studium, spezialisierte sich auf Schadsoftware.

Es gibt unzählige Viren, Trojaner, Internetschädlinge, jeden Tag kommt etwa eine halbe Million dazu. Es sind miserabel programmierte darunter, plump und nahezu wirkungslos, aber auch gefährliche Cyberwaffen, mit denen sich Banken plündern, Kraftwerke lahmlegen und Staaten sabotieren lassen. Rossow interessiert sich nur für die gut programmierten. Er sieht sich jeden Tag Dutzende davon an, liest ihre Codes, Befehlszeile für Befehlszeile. Er will verstehen, wie sie funktionieren, wie sie auf fremde Rechner geschleust werden und wie man sie entschärfen kann.

Er ist Teil eines stillen Kampfes, der mithilfe von Tastaturen, Bytes, Codes und Glasfaserkabeln ausgetragen wird, Programmierer gegen Programmierer, Gut gegen Böse. Die einen erfinden die Cyberwaffen, die anderen studieren ihre Baupläne und versuchen, diese Waffen unschädlich zu machen.

"Es ist ein Spiel", sagt Rossow.

Er sitzt an einem Schreibtisch oder auf seinem Sofa, vor einem Bildschirm, der ihn mit der Welt da draußen verbindet. Er studiert seine Gegner, ihre Strategie, um möglichst schon vorher zu wissen, was sie als Nächstes vorhaben. Sie könnten Teenager sein oder Männer, die irgendwo in einem abgedunkelten Zimmer sitzen und Kapuzenpullis und Ziegenbärte tragen, er erfährt es nie. Wahrscheinlich haben die meisten angefangen wie er, haben ein bisschen programmiert oder Spiele geknackt, um sie nicht kaufen zu müssen. Rossow hat sich früh entschieden, auf der Seite des Guten zu stehen. Als Forscher, unabhängig, gewissenhaft, sachlich.

Die professionellen Hacker, sagt er, werden immer besser, ihre Attacken immer zielgenauer und trickreicher. Was sie selbst nicht programmieren wollen oder können, kaufen sie in Foren in Internet, dem Schwarzmarkt der digitalen Unterwelt. Sie können dort Rechner für Attacken mieten. Oder den Zugang zu Computern, die ohne das Wissen ihrer Besitzer zu Botnetzen zusammengeschlossen werden. In diesen Foren

bietet eine arbeitsteilige Industrie die Bauteile für digitale Hochleistungswaffen an, manchmal in geschlossenen Klubs, zu denen nur zahlende Mitglieder Zugang haben.

Als Rossow in seinem Büro zum ersten Mal auf "Gameover Zeus" stößt, ist es Mitte November 2011. Kurz zuvor hat jemand dem Mitarbeiter einer Firma im Nordwesten des US-Bundesstaats Pennsylvania eine Mail mit einem Link geschickt, die aussah, als käme sie von einem seiner Chefs. So hat er sich Zugriff auf Daten und Konten des Unternehmens verschafft. Es war, wie sich herausstellen wird, Bogatschows erster großer Raubzug. Die Beute, rund eine Million Dollar, verschob er mithilfe von Strohmännern auf ein Bankkonto in London.

Rossow kann davon nichts wissen. Das Programm, das er im Virenlabor im Keller entdeckt hat, ist noch unbekannt. Sein Code liest sich wie eine kaum zu entziffernde Geheimschrift. Es nistet sich tief im System eines Rechners ein, schickt keinen Spam und scheint auf etwas zu lauern. Außerdem ist es offenbar sehr gut verschlüsselt. Rossow will mehr darüber herausfinden, wie dieses Programm arbeitet. Er will beobachten, wie die Waffe funktioniert.

In den nächsten Wochen sitzt er tagsüber in seinem grauen Hochschulbüro und abends zu Hause im Arbeitszimmer mit seinem kleinen schwarzen Laptop, oft bis tief in die Nacht. Er schläft nur noch wenig, seine Freundin sieht er kaum. Nur tagsüber, wenn die Sonne scheint, geht er joggen, um mal eine halbe Stunde nichts denken zu müssen.

Allmählich beginnt er, die Logik dieses Trojaners zu verstehen. Wie er fremde Computer anspricht, wie er sich vorstellt und sein gigantisches Botnetz bildet. Im Sicherheitslabor seiner Hochschule baut Rossow eine Kopie des Schadprogramms nach, um weitere Tests machen zu können. Irgendwann findet er in einem polnischen Fachblog einen Artikel. Jemand, Forscher wie er, hat offenbar denselben Trojaner entdeckt, ihn analysiert und ist zu dem Schluss gekommen, dass dieser Schädling perfekt gebaut ist, nicht zu knacken. Denn "Gameover Zeus" ist nicht nur sehr schnell, sein Schöpfer hat sich auch eine besondere Tarnung einfallen lassen.

Die Hacker müssen eine Reihe von Entscheidungen treffen, wenn sie ihre Schadsoftware entwickeln. Zum Beispiel die, wie die infizierten Rechner die

entscheidenden Befehle erhalten sollen. Sie können diese Informationen im Code ihrer Cyberwaffen hinterlegen. Sie können aber auch die Rechner, die sie heimlich übernehmen, von einem anderen Computer oder gleich von mehreren kontrollieren lassen. Der Vorteil der ersten Variante ist, dass ihre Kontrolle direkter ist, zuverlässiger. Der Nachteil: Sie hinterlassen mehr Datenspuren, mit denen Cyberermittler oder Männer wie Rossow ihnen nachspüren können.

Bogatschow hat sich für die zweite Variante entschieden. Der Rechner, von dem aus er seinen Trojaner verschickt, benutzt die infizierten Rechner als Boten. So macht er sich praktisch unsichtbar, ein Computer in einem Verbund von Hunderttausenden, von denen fast alle unablässig irgendwelche Befehle versenden und weiterleiten.

Rossow ist beeindruckt. Eine derart kunstvolle Waffe sieht er selten, der Macher bietet seinen Gegnern fast keine Angriffsfläche. Trotzdem, jedes Programm hat Schwachstellen, den perfekten Code gibt es nicht, denkt Rossow. Sonst wären auch Betriebssysteme wie Windows, Mac OS oder Linux unverwundbar.

An einem dieser langen Abende, als er durch das Fenster seines Arbeitszimmers zu Hause in einen nachtschwarzen Himmel blickt, glaubt Rossow, diese Schwachstelle gefunden zu haben. Bogatschow kontrolliert nicht, wer sich seinem Botnetz anschließt. Er hat darauf verzichtet, ein zuverlässiges Schloss einzubauen. Vielleicht hat er das Problem nicht bedacht. Vielleicht aber war er sich seiner Sache auch zu sicher und glaubte, dass seine Tarnung nicht aufzuheben sei.

Rossow gelingt es, sich unerkannt in Bogatschows Botnetz zu mischen. Jetzt ist er es, der lauert und seinen Gegner ausspäht, gut getarnt. Wenn seine Vermutungen stimmen und es ihm gelingt, Bogatschows Trojaner auszuschalten, wird das nicht nur seine Professoren interessieren, sondern auch die Hersteller von Antivirensoftware, die großen Computerfirmen, die Sicherheitsunternehmen der IT-Branche, das Bundeskriminalamt, Europol, womöglich sogar das FBI. Allein wird er das allerdings nicht hinbekommen. Es ist zu viel Arbeit, und er muss schnell sein, wenn er der Erste sein will. Er hat zwei Bekannte, die ihm helfen. Einen Studenten, den er betreut, und einen Kollegen, den er lange kennt.

Sie sitzen in ihren Wohnungen in Dinslaken, Amsterdam und Düsseldorf, analysieren Daten und schalten sich zu Videokonferenzen zusammen, sobald sie etwas Neues herausgefunden haben, oft mehrmals täglich. Nach ein paar Wochen glauben sie zu wissen, wie sie Bogatschows Waffe attackieren können. Und auch, wann der beste Moment dafür ist: ein Freitagabend.

Rossow hat im Virenlabor getestet, welche Rechner in Bogatschows Botnetz besonders viele Informationen miteinander austauschen. Mit denen steuert er wahrscheinlich sein Botnetz. Außerdem haben Rossow und seine beiden Bekannten herausgefunden, dass die Updates für "Gameover Zeus", die neuesten Programmversionen, immer unter der Woche erscheinen, meist frühmorgens. Das heißt, die Cybergangster scheinen am Wochenende nicht zu arbeiten und in einer ähnlichen Zeitzone zu leben, vielleicht in Europa, wahrscheinlicher in der Ukraine oder in Russland. Es gibt dort eine Menge sehr gut ausgebildeter Informatiker. In Deutschland würden Unternehmen oder Forschungseinrichtungen sie mit lukrativen Verträgen locken, in Russland aber gibt es zu wenig Jobs.

An einem Freitagabend, kurz nach 17 Uhr, sitzt Rossow in seinem heimischen Arbeitszimmer. Es ist Mitte Mai 2012. Auf Rossows Computerbildschirm sind zwei Fenster nebeneinander geöffnet, ein weißes und ein schwarzes. In dem weißen sieht er die Gesichter der anderen beiden, angespannt wie seines. Zu Hause vor ihren Computern blicken sie auf das gleiche schwarze Fenster wie er, die Matrix. Wo andere nur eine endlose Aneinanderreihung von Zahlen, Buchstaben und Zeichen sehen, sehen sie eine Welt.

Sie haben fast zwei Monate gebraucht, um den Code für ihren Angriff zu schreiben. Er soll die Verbindungen der Rechner zueinander manipulieren und sie so aus Bogatschows Botnetz herauslösen, einen nach dem anderen. Es muss schnell gehen. Ein Computer wartet sich alle zwanzig bis dreißig Minuten automatisch selbst. Das ist die Zeit, die ihr Programm hat. Dauert es länger, machen die Rechner ihren Versuch automatisch zunichte. Sie nutzen deshalb das Internet und die Computeranlage von Rossows Hochschule. Ihre Internetanschlüsse zu Hause wären viel zu langsam.

Rossow drückt die Enter-Taste und wartet.

Auf seinem Bildschirm beginnen die weißen Zeilen zu tanzen, so schnell, dass sie verschwimmen. Jeder Computer, den sie Bogatschow geklaut haben, schickt eine Bestätigung, eine Zeile Text. Es sind viele, sehr viele, es geht rasend schnell. Um zwei Uhr nachts kontrolliert Rossow noch einmal das Warnsystem, alles ist in Ordnung, danach legt er sich ins Bett, zufrieden, dass alles gelaufen ist wie geplant.

Am nächsten Morgen ist er früh wach. Die Hacker haben immer noch nicht reagiert. Das Wochenende vergeht, die erste Woche, die zweite Woche. Rossow ist überrascht. Sie haben Bogatschow ein teures Problem beschert. Er hat die Kontrolle über die Computer verloren, deren Besitzer er ausgeraubt hat, manche mehrmals. Ihm entgeht Beute. Außerdem hat auch er Bauteile seiner Waffe eingekauft, um fremde Computer infizieren und Kontodaten auslesen zu können. Nun braucht er neue.

Drei Wochen nach dem Angriff legt jemand das Internet von Rossows Hochschule lahm. Es ist Bogtaschows Gegenangriff, Rossow hat ihn erwartet, er bricht seine Attacke ab. Er weiß jetzt, dass Bogatschow und sein Schadprogramm nicht unbesiegbar sind. Sein bisheriger Erfolg hat ihn verwundbar gemacht. Je mehr Computer ein Botnetz umfasst, desto schwieriger ist es zu reparieren, wenn jemand einen Fehler einschleust. Nichts anderes hat er, Rossow, getan.

Innerhalb weniger Tage veröffentlichen Bogatschow und seine Leute ein gutes Dutzend Updates. Es gibt ein paar neue Funktionen. Aber die Schwachstelle ihres Programms haben sie offenbar nicht erkannt. Das heißt, Rossow und seine Kollegen können die Hacker noch einmal angreifen. Allerdings brauchen sie dieses Mal effektivere Waffen, einen ausgefeilteren Code, größere Rechner und mehr Serverkapazität.

Im August 2012 bittet Rossow seine Freundin, zu ihren Eltern zu ziehen. Eine Woche lang verwandeln er und die anderen beiden seine Wohnung in die Zimmer ihrer Jugend. Tagsüber sitzen sie mit ihren Laptops, Unterlagen und Gummibärchen um den Esstisch im Wohnzimmer, nachts rollen sie für ein paar Stunden ihre Isomatten auf dem Boden aus. Schon früh am Morgen, beim Frühstück, diskutieren sie über Peer-to-peer-Netzwerke, Bulletproof Hosting und Sinkholing und schreiben weiter an ihrem neuen Code.

Sie haben sich zwei Männer zu Hilfe geholt, die für IT-Sicherheitsfirmen arbeiten und die sie auf Konferenzen kennengelernt haben. Einer, Tillmann Werner, sitzt mit ihnen am Tisch. Der andere, ein Kalifornier, loggt sich am frühen Abend deutscher Zeit bei Skype ein. Brett Stone-Gross ist sein Name, er steht im Ruf, ein gutes kriminalistisches Gespür zu haben, außergewöhnliche technische Fähigkeiten und glänzende Kontakte zu den amerikanischen Sicherheitsbehörden. Wie sich herausgestellt hat, ist auch er schon seit einiger Zeit hinter Bogatschow her.

Am Ende der Woche fühlen sie sich bereit für den zweiten Angriff. Sie haben vier Firmen gefunden, die ihnen mehrere Server zur Verfügung stellen. Sie haben dieses Mal mehrere IP-Adressen, nicht nur die einer Hochschule, sie sind also als Angreifer viel schwieriger zu erkennen. Vor allem, findet Rossow, ist ihr Code dieses Mal deutlich raffinierter.

Er glaubt zwar, dass es den perfekten Code nicht gibt, aber er will ihm so nahe wie möglich kommen. Der Code ist die Handschrift, mit der sich ein Programmierer offenbart, seine Kunstfertigkeit und auch seine Persönlichkeit. Ein Code verrät zum Beispiel, ob er von einem eitlen Menschen geschrieben ist, sein Macher kann geheime Botschaften darin versteckt haben, Referenzen an ein Buch oder einen Musiker. Für Rossow ist der perfekte Code elegant, frei von Zierrat, er lässt das Schwierige einfach aussehen. Bogatschows Code ist elegant. Dieser Mann, das verrät seine Handschrift, hatte ungewöhnliche Ideen, trotzdem hat er auf alles Überflüssige verzichtet. Doch Rossow glaubt, dass sie ihm etwas entgegenzusetzen haben.

Etwa zu dieser Zeit klagt fast 8000 Kilometer entfernt ein Gericht im Norden der USA einen Mann an, der sich hinter den Alias-Namen "slavik", "lucky12345" und "Pollingsoon" verbirgt. Die Anklage wirft diesem Mann unter anderem Schutzgelderpressung, Bankbetrug und den Verstoß gegen diverse Computergesetze vor.

An einem Freitagabend im September 2012 greifen Rossow und seine Helfer zum zweiten Mal an. Es läuft ähnlich wie zuvor. Es wird Mitternacht, ein Uhr, zwei Uhr. Der Samstag vergeht, die erste Woche, die zweite. Sie lösen neunzig Prozent der Computer aus Bogatschows räuberischem Netz heraus. Am Ende der zweiten Woche

sehen sie, dass die Hacker ihren Trojaner mehrfach überarbeitet haben. Die Schwachstelle haben sie noch immer nicht behoben.

Rossow hat nun eigentlich alles, was er braucht. Er wollte wissen, wie das Programm funktioniert und warum es so erfolgreich ist. Das weiß er. Er hat einen Trojaner besiegt, der als unbesiegbar galt, zweimal, das gilt als Beweis. Er könnte jetzt einfach seine Doktorarbeit schreiben. Die Chancen stehen gut, dass er als erster Wissenschaftler "Gameover Zeus" wirklich beschreibt. Andererseits, denkt Rossow, solch einen Fall hat man als Wissenschaftler wohl nur einmal in seinem Leben. Außerdem gibt es eine Menge Menschen, die durch den Trojaner viel Geld verlieren, jeden Tag.

Monate später, im Mai 2013, steht Rossow im Erdgeschoss eines gewaltigen Betonklotzes mitten in San Francisco in einem Raum ohne Fenster, in dem es ähnlich kühl ist wie in seinem Virenlabor. Er ist auf der IEEE Security and Privacy, der wohl wichtigsten Konferenz der Welt zum Thema Computersicherheit, als Redner eingeladen. Die besten Forscher, Detektive, Ermittler kommen hier einmal im Jahr zusammen. Rossow blinzelt in das gleißende Deckenlicht, alle Sitzreihen sind gefüllt. Es müssen etwa 500 Leute sein, die hören wollen, was er und die anderen über "Gameover Zeus" herausgefunden haben. Es ist das erste Mal, dass ein größeres Publikum davon erfährt.

Für Rossow ist es außerdem der Moment, in dem das Spiel gefährlich wird. Denn er trägt den Kampf heraus aus der virtuellen, hinein in die reale Welt. Bisher war auch er für Bogatschow ein Geist, jemand, der Zugriff auf einen Hochschulserver haben musste und offenbar einiges von Botnetzen verstand. Doch ab jetzt ist er ein deutscher Wissenschaftler, ein Mensch mit einem Namen und einem Gesicht, den man finden kann, wenn man will, und der weiß, dass eine Firewall mehr Schutz bietet als die Wände seines Hauses. Rossow versucht, diesen Gedanken zu verscheuchen. Er beruhigt sich damit, dass inzwischen viele andere versucht haben, Bogatschows Botnetz zu hacken, und dass er, Rossow, ja nur Teil einer Gruppe ist.

Kaum ist er zurück in Deutschland, da mailt ihm Brett Stone-Gross, der Amerikaner aus seiner Gruppe. Ein Mann namens Elliott Peterson, Special Agent des FBI, ein ehemaliger Marine, habe Rossows Vortrag in San Francisco gehört und sich gemeldet. "Er könnte unsere Hilfe brauchen", schreibt Stone-Gross.

Schon bei der ersten Videokonferenz mit diesem Mann hat Rossow das Gefühl, dass der Fall noch um einiges größer ist, als er dachte. Peterson, groß, muskulös und ironisch, ist keiner dieser grimmigen Schweiger, die Rossow aus amerikanischen Agentenfilmen kennt. Seine Fragen und Andeutungen verraten, dass er schon lange hinter Bogatschow her ist und längst mit einer internationalen Armee von Ermittlern und Sicherheitsfirmen zusammenarbeitet "Wir suchen", sagt Peterson, "nach einem Weg, den Hackern dieses Botnetz wegzunehmen, dauerhaft. Kriegt ihr das hin?" Was auch immer sie brauchten, er werde versuchen, es möglich zu machen. Es werde vieles möglich sein, denn dieser Fall sei ungeheuer wichtig für die Vereinigten Staaten von Amerika.

Dieses Mal trifft sich Rossows Gruppe in einem renovierten Altbau in Bonn. Eine Woche Matratzenlager, eine Woche Pizza vom Lieferservice. Inzwischen hat Bogatschow ihnen die Arbeit deutlich erschwert. Er hat seinen Trojaner so umprogrammiert, dass sich der Code praktisch nicht mehr verändern lässt. Außerdem hat er ein gigantisches Hütchenspiel aufgezogen. Sein Trojaner generiert in jeder Woche 1000 neue Domainnamen. Das heißt, sie werden großen Aufwand betreiben müssen, wenn alles klappen soll. Denn sie sind auf die Hilfe all der Firmen angewiesen, die Domains verwalten. Sie müssen mit ihnen verhandeln, um die Adressen sperren zu lassen.

Aber sie wissen nun, was zu tun ist. Sie besprechen sich, testen, schreiben einen neuen Code. Mindestens einmal am Tag ruft Peterson an und fragt, wie es vorangeht. Wenn sie etwas brauchen, besorgt er es, Geld spielt keine Rolle. Doch als sie bereit sind für den Showdown, meldet sich Peterson immer seltener. Manchmal hören sie tagelang nichts von ihm, dann mehrere Wochen oder Monate. Rossow wird nervös. Bogatschows letztes Update war schon sehr gut. Was, wenn er seinen Trojaner noch weiter perfektioniert, wenn er den Fehler findet und ihn ausmerzt? Jeden Tag könnte es passieren.

Vielleicht, denkt Rossow, haben sie schon bald keine Chance mehr, ihn zu stoppen.

Am 31. Mai 2014, zweieinhalb Jahre nachdem Rossow in seinem Hochsicherheitslabor auf den Trojaner "Gameover Zeus" aufmerksam geworden ist und ein Jahr nachdem der FBI-Agent Peterson ihn um Hilfe gebeten hat, klappen Tillmann Werner und Brett Stone-Gross, Rossows Bekannte, in einem leer geräumten Konferenzraum in Pittsburgh ihre Laptops auf. Auf einem Tisch vor ihnen stehen zwei große Monitore, hinter ihnen ein Dutzend FBI-Männer und hochrangige Juristen der Vereinigten Staaten.

Peterson hat wie besessen auf diesen Tag hingearbeitet. In wenigen Augenblicken werden diese zwei Jungs, ein Deutscher und ein Amerikaner, damit beginnen, Bogatschows Botnetz zu vernichten. Dafür hat er sie hierhergebeten, in einen grünen Riegel in der Innenstadt, ins nationale Cyber-Abwehrzentrum der USA. Und während sich ihr Programm immer tiefer in Bogatschows Netzwerk hineinwühlt und seine Waffe zersetzt, werden in Kanada, in Deutschland, Frankreich und England, werden vor allem in Russland und der Ukraine einige Dutzend Ermittler etliche Häuser und Wohnungen durchsuchen und zehn Männer festnehmen, die Bogatschow bei seinem Raubzug durch den Cyberspace geholfen haben. Das ist Petersons Plan.

Es ist kurz nach acht an diesem Freitagmorgen, als Stone-Gross und Werner die Enter-Taste drücken. Etwa sieben Stunden später klingelt Rossows Handy. In Deutschland ist es Abend, kurz vor neun, als Werner sich meldet. Rossow sitzt auf einer Holzbank vor einer Ferienwohnung auf Rügen und liest ein Buch. Er ist mit seiner Freundin in den Urlaub gefahren.

Als es darum ging, zu entscheiden, wer nach Pittsburgh fliegen würde, hatte Rossow überlegt. Er hatte Bogatschows Fährte aufgenommen, seine Spuren verfolgt, seine Eigenheiten kennengelernt, sich ein Bild von ihm gemacht. Jetzt, da alles auf den großen Showdown zulief und er die Sache zu Ende bringen konnte, würde er stattdessen im Urlaub sein. Er hatte viel gearbeitet und seiner Freundin die gemeinsame Zeit schon vor Monaten versprochen, in drei Wochen würden sie heiraten. Außerdem war er schon immer lieber allein, wenn er an etwas Wichtigem arbeitete. Es machte ihn nervös, wenn jemand hinter ihm stand, als würde er alles

überwachen. Wenn es schwierig würde, dürfte nichts ihn ablenken. Außerdem spielte es für ihn keine Rolle, ob er in Gelsenkirchen oder Dinslaken, in Bonn oder Pittsburgh war. Der Kampf gegen Bogatschow fand nicht an einem bestimmten Ort statt, sondern im Cyberspace. Alles, was er brauchte, waren sein Laptop und ein Internetanschluss.

Irgendwas stimmt nicht, sagt Werner.

Ihr Programm macht sich nur sehr langsam in Bogatschows Botnetz breit. Viel zu langsam. So wird Bogatschow keine Mühe haben, Herr über all die fremden Computer zu bleiben. Sie haben alles kontrolliert, vieles versucht. Es muss an ihrem Code liegen. Auch den haben sie kontrolliert, wieder und wieder, aber keinen Fehler gefunden. Alles hängt jetzt von Rossow ab. Findet er keine Lösung, scheitert womöglich eine der aufwendigsten Ermittlungen, die die Welt seit Langem gesehen hat.

Rossow geht in die Wohnung und zieht seinen Laptop aus einem Rucksack, doch das Internet funktioniert plötzlich nicht mehr. Also fährt er mit dem Rad in den nächsten Ort und sucht ein Hotel, in dem es Internet gibt. In der Lobby lässt er sich in ein Sofa fallen, stellt seinen Computer auf den Couchtisch und startet die beiden Programme, die er für die bisherigen beiden Angriffe auch benutzt hat. Dann sitzt er im Dämmerlicht, ein junger Mann in Funktionskleidung, halb Mensch, halb Schemen. Der Bildschirm leuchtet sein Gesicht blau an. Rossow klickt in das schwarze Fenster und sucht die Stelle ihres Codes, an der er den Fehler vermutet, dann beginnt er, ihn neu zu schreiben. Ab diesem Moment nimmt er um sich herum nichts mehr wahr.

Als er fertig ist, drückt er die Enter-Taste und sieht zu, wie sich ihr Programm in Bogatschows Botnetz hineinzufressen beginnt.

Drei Tage später tritt in Washington ein älterer Herr mit schmalem Gesicht, Föhnfrisur und Schnauzer vor die Presse, hinter ihm stehen zwei Flaggen, die Stars and Stripes und der American Eagle. James Cole, stellvertretender Justizminister der USA, hat eine Sensation zu verkünden. Die USA, sagt Cole, hätten mithilfe einer internationalen Fahndungsgruppe einem der gewieftesten Cyberganoven der Welt das Handwerk gelegt. Jewgeni Bogatschow habe das "komplizierteste System von Computerviren geschaffen, das uns jemals begegnet ist". Gemeinsam mit russischen

und ukrainischen Komplizen habe er mehr als eine Million Computer infiziert, darunter die Server von US-Banken. Cole sagt, dass ein US-Gericht Bogatschow wegen Internet- und Bankbetrugs anklagt, wegen Erpressung, Datendiebstahls und Geldwäsche.

Am Nachmittag telefoniert Rossow mit Werner und lässt sich noch einmal in Ruhe erzählen, wie alles gelaufen ist. Als er auflegt, glaubt er, dass die Geschichte für ihn zu Ende ist. Doch die Geschichte hat sich in den vergangenen Monaten verselbstständigt.

Deshalb sitzt Rossow nun, fünf Jahre nachdem alles angefangen hat, zu Hause in seinem Wohnzimmer und weiß nicht recht, was er von alldem halten soll. Er hat allen Grund, stolz zu sein. Er hat etwas Außergewöhnliches vollbracht. Das FBI hat ihm eine Urkunde verliehen, in einer dunkelblauen Kunstledermappe, sie steht aufgeklappt in seinem Büro an der Uni in einem Regal. Er hat, kaum mit dem Studium fertig, eine Forschungsgruppe an einer Uni bekommen, seine Vorlesungen sind gut besucht. Die großen Computerfirmen laden ihn ein, um Vorträge zu halten, nach Nizza, ins Silicon Valley. Aber er zuckt noch immer zusammen, wenn er vor einem großen Publikum steht und hört, wie jemand ihn mit seinem Namen ankündigt. Er hat sich nicht mit irgendeinem Hacker angelegt, sondern mit einem Kriminellen, dem alles zuzutrauen ist. Er fürchtet, dass Bogatschow sich rächen könnte. Außerdem ist da diese Sache mit der Spionage.

Rossow und die anderen haben, gut versteckt in Bogatschows Botznetz, eine Reihe von Suchbefehlen gefunden, die digitale Bankräuber nicht brauchen und die man in ihren Schadprogrammen üblicherweise nicht findet.

Jemand hat dort Informationen über Georgien und die Ukraine, über Syrien und die Türkei zusammengetragen, alle sehr brisant. Seine Suchabfragen verraten, dass er es auf Regierungsdokumente abgesehen hatte, die als geheim gestempelt waren, und auf bestimmte Mitarbeiter von Auslandsgeheimdiensten. Das deutet auf russische Interessen hin. Denn kaum jemanden interessierten diese Länder damals so wie Russlands Präsident Putin. Er hatte einen Krieg gegen Georgien geführt, das Verhältnis war noch sehr angespannt. In Syrien ließ Machthaber Baschar al-Assad das

eigene Volk bombardieren, Putin stand auf seiner Seite, die Türkei auf der Seite Europas und der der USA. Auch in der Ukraine führte Putin einen Krieg.

Die Daten, die Bogatschows Schadprogramm gesammelt hatte, lassen also den Schluss zu, dass sich ein Spion in Bogatschows Botnetz eingenistet hat, womöglich sogar im Auftrag der russischen Regierung. Auch die Qualität seiner Cyberwaffe spricht dafür.

"Na ja, ich wäre da trotzdem vorsichtig", sagt Rossow. Es gibt im Netz viele Möglichkeiten, sich zu tarnen und falsche Fährten zu legen.

Die amerikanischen Ermittler aber, auch FBI-Agent Peterson, sprechen von Spionage und davon, dass Bogatschow hinter der Suche nach den brisanten Informationen steckt. Im Sommer 2014 haben die USA deshalb Russland aufgefordert, Bogatschow auszuliefern. Vergeblich, denn es gibt kein Auslieferungsabkommen. Im Februar 2015 schrieb das FBI Bogatschow zur Fahndung aus, mit einem Kopfgeld von drei Millionen Dollar. Es ist die höchste Belohnung, die US-Behörden je für einen Cyberkriminellen ausgelobt haben.

Vieles deutet darauf hin, dass sich Bogatschow bis heute in Russland aufhält, in Anapa, einem Kurort an der Schwarzmeerküste mit 60.000 Einwohnern. Er hat dort eine Meldeadresse, eine Wohnung in einem Wolkenkratzer, die Polizeistation ist bloß ein paar Hundert Meter entfernt. Er sei immer mal wieder dort gewesen, sagen seine Nachbarn. Sie mögen ihn. Sie erzählen, wie umgänglich er sei und dass er mit einem alten Volvo herumfahre, mit einem Aufkleber auf dem Kotflügel, mit dem er für Computerreparaturen werbe. Es heißt auch, er sei immer mal wieder auf seiner Yacht gesehen worden, vor der Küste. So haben es die Nachbarn einer russischen und einer englischen Zeitung erzählt. Es klingt nicht, als sei Bogatschow sonderlich bemüht, sich zu verstecken. Auch deshalb halten es die Ermittler in den USA und Europa für möglich, dass Putins Regierung ihn deckt.

Es ist eine Spekulation, aber sie ist nun in der Welt und verbreitet sich wie ein Computervirus. Elliott Peterson, Bogatschows Jäger, hat sie vor ein paar Monaten öffentlich gemacht. Er stellte auf einer Cyber-Konferenz in Las Vegas einen umfangreichen Bericht vor, den er über die Jagd auf Bogatschow geschrieben hatte. Es

deute einiges darauf hin, dass "Gameover Zeus" von Anfang an benutzt worden sei, um zu spionieren, schrieb er. Im Nachwort dankt er Rossow.

Rossow verzieht das Gesicht zu einer Grimasse, wenn man ihn darauf anspricht. Es kommt ihm manchmal so vor, als stünde die Welt in Flammen. Als wären die USA und Russland zurück im Kalten Krieg. Er fürchtet, dass in einer Zeit wie dieser schon ein kleiner Anlass genügen könnte, um eine Eskalation auszulösen. Spionage, diplomatische Verwicklungen, Cyberkrieg. Die Sache ist ihm zu groß geworden.

Er ist Informatiker. Er wollte etwas herausfinden und das Richtige tun. Es scheint bloß, als interessierte das niemanden mehr.