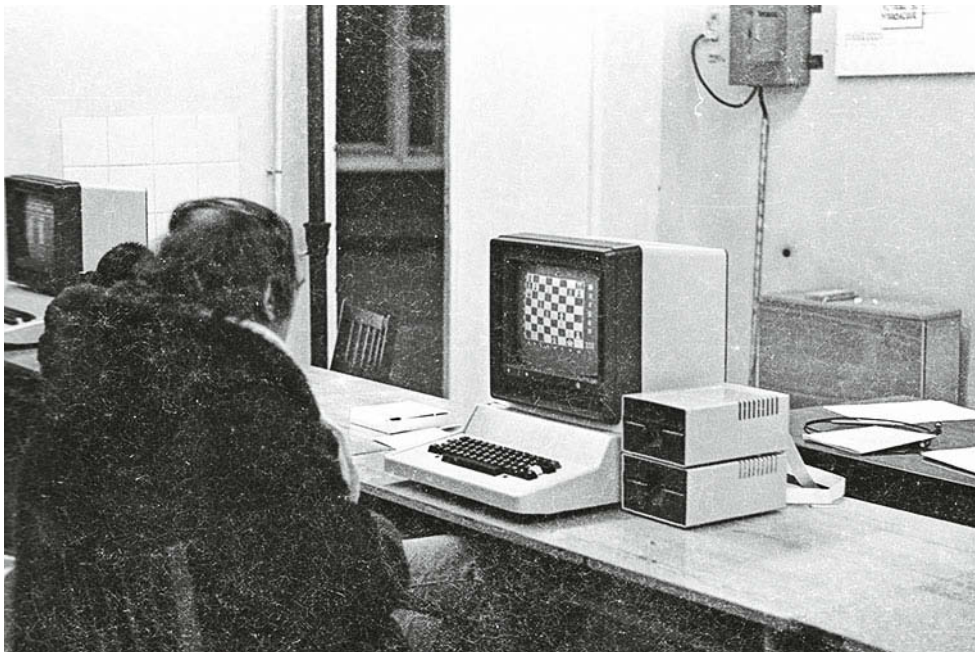

Bulgarische Pravets-82-Computer in einer russischen Schule, 1986. W. I. SPIRIDONOW | PERESLAWSKAJA NEDELJA [CC-BY-SA 3.0]

»Kopier mich, ich möchte reisen!«

Um 1990 kamen die weltweit schädlichsten Computerviren aus Bulgarien. Ihr genialer Programmierer, »Dark Avenger«, ist bis heute unbekannt

Von Frank Stier

Auf der bulgarischen Webseite *android.bg* erinnert sich ein User, der unter dem Nickname *emski_vas* schreibt, an seine Jugend um 1990: »Als ich die ersten *Pravetsi* sah, schienen sie mir eine kosmische Technologie. Ich war höllisch beeindruckt. Wir hatten fünf dieser Computer in der Schule. Eine Lehrerin ließ uns an sie ran, und aus Büchern schrieben wir ein, zwei Stunden Programme für Spiele und andere Wunder ab. Danach daddelten wir ein Stündchen, bis sie uns davonjagten.«

Ein anderer User, *professor_glavtcho,* kommentiert: »An dieser Stelle ist es Zeit, den Kollegen Dark Avenger zu ehren. Ihm ist es zu verdanken ist, dass Bulgarien eine Computermacht geworden ist, ohne dass es überhaupt Internet gab.«

Darauf antwortet *emski_vas:* »Wir alle werden ihn ehren, wenn du uns sagst, wer er ist.«

Auch nach über zwanzig Jahren ist der Autor gefürchteter Computerviren, Dark Avenger, in Bulgarien ein Mythos. Seine Identität ist ein Rätsel, das viele gern gelöst haben würden. »Ja, ich glaube ihn zu kennen. Es wäre aber nicht rechtens, seinen Namen zu nennen, weil ich es nicht beweisen kann«, sagt Wesselin Bontschew, Bulgariens prominentester Antiviren-Forscher. Zu Beginn der 1990er Jahre, als die *New York Times* Bulgarien als weltweit führende Brutstätte für Computerviren adelte, galt Bontschew als Dark Avengers Erzfeind. Er stand zugleich selber im Verdacht, der »temnijat otmestitel« zu sein, jener »finstere Rächer«, wie die bulgarische Übersetzung von »Dark Avenger« lautet. »Das Rätsel ist noch immer nicht gelöst«, schreibt *professor_glavtcho.* »Entweder ist es Wesselin Bontschew von der Zeitschrift *Kompiuter sa vass.* Oder Todor Todorow vom Nationalen Mathematischen Gymnasium.«

Bontschew ist nach vielen Jahren im nordeuropäischen Ausland nach Bulgarien heimgekehrt. Der heute 53-Jährige sitzt im Café Athene an Sofias Prachtboulevard Witoscha, nippt an einem Cappuccino und erinnert sich an die romantische Frühzeit der Computervirologie. Warum wurde ausgerechnet das kleine Balkanland zum Hotspot berüchtigter Computerviren wie Old Yankee, Eddie, Anthrax oder des polymorphen Programmgenerators MtE (Mutation Engine)? »Wir Bulgaren wollen Gesetze nicht gerade brechen,

aber wir möchten sie umgehen«, versucht er sich in Nationalpsychologie. Damals, in den 1980er Jahren, schulten viele junge Rechnerfreaks ihre Programmierfähigkeiten, indem sie den Kopierschutz von Computerspielen aushebelten. »Computerviren zu schaffen, also sich selbst reproduzierende Programme, die wie Lebewesen wandern können, erschien ihnen als eine intellektuelle Herausforderung«, erklärt Bontschew. Zudem habe es zu dieser Zeit keine Unternehmen gegeben, in denen junge Computerspezialisten ihre Fähigkeiten sinnvoll hätten einsetzen und Karriere machen können.

Bontschew selbst beschäftigt sich seit 1988 mit Computerviren, zunächst als eine Art Fachberater für die *Kompiuter sa vass*. 1990 wurde er Gründungsdirektor des Nationalen Laboratoriums für Computervirologie an der Bulgarischen Akademie der Wissenschaften (BAW). 1991 legte er die Studie »The Bulgarian and Sovjet Virus Factories« vor. Sie ist noch heute das Standardwerk über diese Zeit. Nach seiner Promotion am Virus Test Center der Universität Hamburg mit einer Doktorarbeit über Computerviren ging er Mitte der 1990er Jahre zur isländischen Antivirenprogrammschmiede Frisk nach Reykjavik. Dort beteiligte er sich maßgeblich an der Entwicklung des Antivirenprogramms F-Prot antivirus. Heute arbeitet Bontschew wieder am Computerviren-Laboratorium der BAW in Sofia. In den letzten Jahren hat er sich vor allem mit Viren für mobile Anwendungen beschäftigt.

Bei den Recherchen für den 1997 in der Zeitschrift *Wired* veröffentlichten Bericht über seine Reise ins »Herz der Finsternis, der heißen Zone, die Bulgariens berüchtigte Computerviren hervorgebracht hat«, gelang es dem US-Journalisten David S. Bannahum, mit Todor Todorow zu telefonieren, einem der wichtigsten Akteure in der Szene. Auszüge aus dem Gespräch: »›Was halten Sie von Bulgarien?‹

›Ich hasse es.‹

›Was denken Sie von Wesselin Bontschew?‹

›Er ist ein Idiot!‹

Ich hielt den Hörer nahe an mein Ohr. Durch die breiten Fenster meines Hotelzimmers blickte ich auf das Witoscha-Gebirge, seine runden Gipfel glitzerten mit dünnen Spuren Juni-Schnees, darunter ausgebreitet lag die Stadt Sofia.

›Was ist mit Dark Avenger, was halten Sie von ihm?‹

›Ich möchte nicht über ihn reden. Die Zeit ist vorbei. Es ist aus. Ich will nicht darüber reden.‹«

Bannahum besichtigte auch das Klassenzimmer Nr. 28 des Nationalen Mathematischen Gymnasiums in Sofia. Dort saß Todorow einst. »Schwüle Luft weht durch das geöffnete Fenster, bauscht die zerfledderten grünen Vorhänge auf, die dem Raum einen gespenstisch phosphorizierenden Schimmer verleihen. Auf zwei langen Holztischen stehen sieben IBM-PCs mit 386er Prozessoren. Die Tafel ist beschrieben mit Pascal-Code. Der Raum wirkt friedlich.« War dies die Brutstätte lästiger Evilware »made in Bulgaria«? Möglich, schließlich machten hier Bulgariens talentierteste Nachwuchsprogrammierer vor und nach dem Zusammenbruch des kommunistischen Regimes im November 1989 ihre Fingerübungen. Damals standen hier keine IBMs, sondern die legendären *Pravetsi*-Computer.

Einige von ihnen, darunter die emblematischen Modelle *Pravets 82* und *16,* sind heute in der Werkstatt »Laptopclean« im Sofioter Bezirk Losenets zu besichtigen. Im Herbst 2013 hat Laptopclean-Chef Boiko Wutschew die bulgarische Öffentlichkeit mit der »Rückkehr der Legende« elektrisiert: Er will 2014 den von ihm entworfenen Laptop *Pravets 64M* auf den Markt bringen. Dafür hat er sich die seit Anfang der 1990er Jahre verwaisten Rechte an der Marke gesichert. Die Komponenten bezieht Wutschew aus Taiwan. In Bulgarien lässt er sie lediglich zusammenbauen.

»Das machen die Hersteller anderer Markenlaptops nicht anders«, sagt Wutschew.

Das große Interesse an seiner Geschäftsidee hat ihn überrascht. »Eigentlich wollten wir nur probehalber mit unsere Website für den *64M* ins Netz gehen. Doch die Nachricht hat sich wie ein Lauffeuer verbreitet und ein riesiges Medieninteresse erzeugt.« Über ihre Computer sprechen die Bulgaren gleichermaßen mit Stolz und Ironie. Es ist eine Geschichte der Marktführerschaft im sozialistischen Wirtschaftsraum. Aus Bulgarien kamen zeitweise 40 Prozent der im sowjetischen Einflussgebiet ausgelieferten Computer. Es ist aber auch eine Geschichte der Industriespionage, waren die bulgarischen Computer doch technisch raffinierte, vom Design etwas hausbacken wirkende Nachbauten führender westlicher Modelle.

Bereits seit den 1960er Jahren hatte das noch agrarisch geprägte Bulgarien eine elektronische Industrie erhalten. Ende der 1970er Jahre beschloss das Politbüro der Bulgarischen Kommunistischen Partei dann den Aufbau einer nationalen Computerindustrie. Die Produktion von Personalcomputern blieb dem Kombinat für Mikroprozessortechnik in der Kleinstadt Prawez vorbehalten. Der Geburtsort des damaligen KP-Chefs Todor Schiwkow liegt sechzig Kilometer von der Hauptstadt Sofia entfernt.

Der 1979 hergestellte »Individuelle Mikro-Komputer« IMKO konnte noch als Eigenentwicklung der bulgarischen Ingenieure gelten. Doch der 1982 produzierte *Pravets 82* war bereits eine Version des Apple II. 1985 kam dann mit dem *Pravets 16* ein geklonter IBM-PC auf den Markt. »Erst mit mit ihm begann Ende gegen Ende der 1980er Jahre die Verbreitung bulgarischer Computerviren«, erklärt Boiko Wutschew. Seinerzeit seien Computer für Privatpersonen unerschwinglich gewesen, fast nur in in Unternehmen, Schulen und Hochschulen zugänglich. Der Wirtschaftszweig wuchs, 300 000 Menschen arbeiteten in Bulgariens elektronischer Industrie. In Spitzenzeiten sollen sie jährlich 60 000 Computer produziert haben. Dann folgte der Zusammenbruch des Realsozialismus.

»Als mich damals ein Reporter zu Computerviren in Bulgarien interviewte, musste er das Gespräch abbrechen, um zur Zentrale der bulgarischen KP zu eilen, die in Flammen stand«, erzählt Wesselin Bontschew. Der Reporter damals war Chuck Sudetic, Korrespondent der *New York Times.* In seinem Ende 1990 erschienenen Artikel hat er Bontschews »eherne Gesetze der Computervirologie« überliefert: »Das erste Gesetz lautet: Kann ein Virus geschaffen werden, wird er geschaffen. Das zweite: Kann ein Virus nicht geschaffen werden, wird er dennoch geschaffen.« Morton Swimmer vom Hamburger Virus Test Center zitiert der Artikel mit den Worten: »Die Bulgaren produzieren nicht nur die meisten Computerviren, sie produzieren auch die besten.« Und John McAfee von der Computer Virus Industry Association (CVIA), selbst ein bekannter Anbieter von Antivirensoftware, berichtete, die Viren von Dark Avenger hätten gar Computer des amerikanischen Militärs, von Banken und Versicherungen befallen.

Die Initialzündung für Bulgariens Entwicklung zur führenden Exportnation von Schadprogrammen gab ein im April 1988 in *Kompiuter sa vass* erschienener Artikel über das Phänomen des Computer-

Fortsetzung auf Seite 85

Fortsetzung von Seite 81

virus. »Der Artikel kam ursprünglich von der deutschen Zeitschrift *Chip* und wurde von jemandem übersetzt, der zwar gut Deutsch konnte, von Computern aber keine Ahnung hatte«, erinnert sich Wesselin Bontschew. Die Redaktion bat ihn, den übersetzen Artikel zu überarbeiten. So begann er sich für das Thema zu interessieren. Damals waren in Bulgarien einige wenige ausländische Viren verbreitet, der aus Österreich stammende »Vienna« etwa, der italienische »Ping Pong«, und »Cascade« aus Deutschland. Bontschew fiel auf, dass »Vienna« und »Cascade« lediglich .com-Dateien infizierten. Gegenüber einem Freund vermutete Bontschew, die Infektion von .exe-Dateien sei erheblich schwieriger. Diesen Freund packte der Ehrgeiz, und bald hatte Bulgarien mit dem »Old Yankee« den ersten einheimischen Virus. Er brachte Computer dazu, die Melodie des Yankee Doodle zu spielen.

Im Frühjahr 1989 tauchte dann ein Virus auf, der seine Herkunft durch eine Copyright-Zeile verriet: »This program was written in the city of Sofia (c) 1988-89 Dark Avenger«. Er begründete den Ruhm seines Autors. Gelangte der auch als »Eddie« bekannte Virus in den Speicher eines Computers, infizierte er sowohl .com- als auch .exe-Dateien. »Es war dies der bis dahin scheußlichste Virus überhaupt. Er infizierte Dateien nicht nur, wenn sie geöffnet, sondern auch wenn sie nur kopiert wurden. Das machte ihn so ansteckend«, erklärt Wesselin Bontschew. Seinen Namen hatte er von der auf dem Bildschirm erscheinenden Textzeile »Eddie lives … somewhere in time!« – eine Reminiszenz an ein Maskottchen der Rockgruppe Iron Maiden.

»Copy me, I want to travel«, lautete eine Zeile im Code von Dark Avengers Eddie-Variation V2000, eine der weiteren Schöpfungen, die von Originalität und Destruktivität zeugten. In dem Virus manifestierte sich zudem seine ausgeprägte Aversion gegen Wesselin Bontschew. Er behauptete, »written by Vesselin Bontchev« zu sein, und fror den Computer ein, sobald ein Antivirenprogramm verwendet wurde, dessen Copyright Bontschews Namen enthielt. Personalisiert war auch Dark Avengers 1992 geschaffene Mutation Engine (MtE), einer der ersten polymorphen Programmgeneratoren. Er konnte selbst einfachste Viren derart verändern, dass sie für Antivirenprogramme kaum mehr zu erfassen waren. Dark Avenger widmete die MtE der US-amerikanischen Computerspezialistin Sarah Gordon, die ihm gegenüber in einer Mailbox-Nachricht den Wunsch geäußert hatte, einen nach ihr benannten Virus zu bekommen.

Doch nicht alle bulgarischen Virenschreiber hätten ihn gehasst, sagt Wesselin Bontschew. »Manche kamen sogar zu mir, um mir ihre Werke zu zeigen. Sie dachten, ich könne sie am besten beurteilen.« Zwar hätten die meisten Viren-Schöpfer unverantwortlich und kindisch gehandelt, es habe aber auch Programmierer gegeben, die darauf achteten, dass ihre Kreationen keinen Schaden anrichteten. »TP« zum Beispiel, der anonym gebliebene Autor des Virus »Vacsina«, der nur »neue Ideen« habe ausprobieren wollen. Dark Avenger hingegen sei ein »Technopath« gewesen, dessen erklärte Absicht es war, Daten zu zerstören.

Bontschew führt Dark Avengers Feindschaft ihm gegenüber auf dessen prinzipielle Opposition gegen alles und jeden zurück. »Vielleicht hasste er mich auch, weil ich an seinem Ruhm teilhatte. Er tat die Arbeit, ich schrieb über sie und wurde bekannt. Er wollte der beste Virenschreiber sein, meine Antivirenprogramme aber machten seine Werke schadlos.« Nur ein einziges Mal traf Bontschew seinen Widersacher persönlich, sagt er: »So um 1990/91 hielt ich an der Sofioter Universität eine Vorlesung. Im Publikum war eine Gruppe von Freunden, von denen sich einer mir gegenüber besonders feindselig verhielt: ›Du verstehst überhaupt nichts, es ist alles Unsinn, was du redest‹, pöbelte er mich an.« Wo Dark Avenger heute steckt? Bontschew sagt, er wisse es nicht.

Vor der allgemeinen Verbreitung des Internets konnten Computer miteinander direkt nur über Mailboxen kommunizieren, die sie über Telefonverbindungen anwählten. Mailboxen wurden neben der Weitergabe infizierter Disketten zum zweiten wesentlichen Verbreitungsweg für Malware. Todor Todorow, auch genannt Commander Tosh, damals Student der Computerwissenschaften an der Universität Sofia, vereinfachte die Kommunikation zwischen den Programmierern, indem er 1990 das weltweit erste auf Viren fokussierte Bulletin Board System (BBS) schuf. Sein Virus eXchange BBS wurde zum wichtigsten Diskussions- und Austauschforum für Virenschreiber und Antivirenprogrammierer. Wer wollte, konnte in diese Mailbox neue Viren einspeisen oder bekannte Viren zur Untersuchung oder Weiterverarbeitung entnehmen. Es war die virtuelle Virenuniversität von Sofia.

Auch Dark Avenger nutzte das BBS, aber auch andere Kanäle. Er kam mit Sarah Gordon in Kontakt, die später im Magazin *Virus News International* ihre mit Dark Avenger geführte Mailkorrespondenz veröffentlichte. Dort kann man seine Gesetze zur Computersicherheit nachlesen: »1. Kaufe dir nie einen Computer! 2. Wenn du ihn dir doch gekauft hast, schalte ihn nicht ein!« In seinen Botschaften offenbart sich der »finstere Rächer« als reflektierte, zu Mitgefühlt fähige Persönlichkeit. Er habe im September 1988 angefangen, seinen ersten Virus zu schreiben, weil er von Viren gehört habe und über sie mehr erfahren wollte. »Aber niemand in meiner Umgebung konnte mir mehr zu ihnen sagen. Deshalb beschloss ich, einen eigenen Virus zu schreiben. Ich fügte in ihn einen Code ein, der darauf abzielte, Daten zu zerstören. Das tut mir leid.«

Wesselin Bontschew hält das für gespielte Reue. Denn an anderer Stelle habe Dark Avenger auf die Frage, warum seine Viren so zerstörerisch seien, geantwortet: weil ihm die Vernichtung von Daten Vergnügen bereite, weil er es liebe, das Werk anderer zu zerstören. Auch die gelegentlich zu hörende Spekulation, die Beziehung zu Gordon habe Dark Avenger dazu gebracht, mit dem Virenschreiben aufzuhören, bezweifelt Bontschew. »Ich bin mir zwar nicht sicher, warum er 1993 aufgehört hat. Die Version, er habe es Sarah Gordon versprochen, kann ich aber nicht glauben.«

Solange die Identität Dark Avengers nicht zweifelsfrei geklärt ist, wird auch der Verdacht nicht aus der Welt zu schaffen sein, die beiden unversöhnlichen Antipoden Dark Avenger und Wesselin Bontschew seien in Wahrheit ein und dieselbe Person. So notiert user *V12* im *Kaldata-Forum,* einem bulgarischen Onlineportal: »Der bekannteste bulgarische Virologe Wesselin Bontschew schrieb Antivirenprogramme am Laboratorium für Virologie der BAW. Gleichzeitig schrieb er unter dem Pseudonym Dark Avenger Viren, die sein eigenes Antivirenprogramm eliminierten. Und er führte sogar mit sich selbst eine Polemik in der Zeitschrift *Kompiuter sa vass.*« Beweise für diese Behauptung bleibt auch er schuldig. ●