Achtung: Streng geheim!

Ein Mitarbeiter der Saar-Universität machte zusammen mit dem FBI Jagd auf russische Internetkriminelle

Russische Hacker, der amerikanische Inlandsgeheimdienst FBI und Millionen gestohlene US-Dollar – was nach dem Stoff eines typischen Agentenfilms klingt, wurde für einen Mitarbeiter der Saar-Uni zur Realität.

Von SZ-Redaktionsmitglied Florian Mayer

Saarbrücken. Auf dem Campus der Universität des Saarlandes kennen ihn viele. Er ist Forscher und Dozent im Fach Informatik. Doch was nur wenige wissen: Er hat für das Federal Bureau of Investigation (FBI) – den US-amerikanischen Inlandsgeheimdienst – gearbeitet. Zusammen mit dem FBI hat der Saarbrücker IT-Wissenschaftler russische und ukrainische Cyberkriminelle auffliegen lassen, die rund 100 Millionen US-Dollar von amerikanischen Banken gestohlen haben. Aus Gründen der Sicherheit zieht es der IT-Forscher vor, dass sein Name nicht öffentlich bekannt gemacht wird. In diesem Text wird er schlicht „John Doe" genannt.

Der Saarbrücker Informatiker forscht seit mehreren Jahren an sogenannten Botnetzen. Das sind viele verschiedene Computer privater Nutzer (Bots), die durch eine Schadsoftware unbemerkt miteinander kommunizieren können, erklärt der Informatiker. In der Regel sind alle infizierten Computer mit einem gemeinsamen Server verbunden, den ein Hacker steuert und über den er Befehle an die anderen Computer weitergeben kann. Solche Botnetzwerke werden zentralisierte Botnetze genannt. Um sie auszuschalten, muss nur der Server des Hackers gefunden und abgeschaltet werden – für Experten keine schwere Aufgabe. Woran der Saarbrücker FBI-Helfer intensiv forscht, sind sogenannte dezentrale Botnetze. Die besitzen keinen zentralen Server, der sich einfach abschalten lässt. Um diese Netzwerke zu zerschlagen, muss jeder einzelne infizierte PC isoliert und vom Rest des Botnetzes abgetrennt werden.

Die Technik, mit der das gelingt, hat „John Doe" im Jahr 2013 in den USA vorgestellt. „Um ein dezentrales Botnetzwerk anzugreifen, müssen wir erst die dafür verwendete Software verstehen", erklärt der Forscher der Saar-Uni. Da die Hacker aber nicht einfach verraten, wie ihre Programme aufgebaut sind, müssen die Informatiker die Schadsoftware Programmzeile für Programmzeile rekonstruieren – eine Arbeit die Monate in Anspruch nimmt. Ist diese Aufgabe geschafft, muss jeder einzelne infizierte Computer aufgespürt werden. „Dafür brauchen wir einen PC aus dem Netzwerk. Der verrät uns, mit welchen anderen Computern er in Verbindung steht", erläutert der IT-Experte. Auf diese Weise können sich die Wissenschaftler von PC zu PC durch das gesamte Netzwerk durcharbeiten.

„Als der wissenschaftliche Artikel dazu veröffentlich war, wurden wir vom FBI angesprochen", sagt „John Doe". Die US-Agenten beobachteten seit 2011 ein dezentrales Botnetzwerk russischer und ukrainischer Hacker, Gameover-Zeus genannt. Das Netzwerk bestand aus weit über 100 000 Rechnern weltweit. Auf allen konnten durch die Schadsoftware Bankgeschäfte von Nutzern manipuliert und das Geld unzähliger Konten auf die der Cyberkriminellen umgeleitet werden. „John Doe" und Kollegen von der Freien Universität Amsterdam sowie Mitarbeiter der Sicherheitsfirmen Crowdstrike und Dell Secureworks erhielten vom FBI den Auftrag dieses Netzwerk zu zerschlagen. Zwei der Forscher flogen im Mai diesen Jahres in die USA, um von dort aus mit dem FBI den Angriff auf Gameover-Zeus zu koordinieren. „Wir analysierten das Schadprogramm und identifizierten die Rechner im Botnetzwerk", so Doe. Während die IT-Forscher das Schadprogramm untersuchten, änderten die Hacker allerdings immer wieder ihre Software. „Fast täglich kamen neue Updates von den Hackern", sagt Doe. Deshalb passten er und seine Kollegen ihre Angriffs-Strategien ständig an: „Wir mussten rund 20 verschiedene Programmversionen analysieren, bis wir bereit für den Angriff waren."

100 000
Computer weltweit wurden von Hackern für eine Cyber-Attacke missbraucht.
Quelle: Saar-Uni

Als dieser bevorstand, erhielten die IT-Forscher Unterstützung durch FBI-Agenten, die außerhalb des Internets Jagd auf die Hacker machten. Gleichzeitig mit dem Angriff hatten auch Entwickler von Antivirenprogrammen damit begonnen, Schutzsoftware zu entwickeln, die Gameover-Zeus von infizierten Computern entfernt und nicht betroffene Rechner davor schützt. „Außerdem bekamen die Anbieter von Internetzugängen eine Liste ihrer betroffenen Kunden, um sie über die Infektion ihres Computers zu informieren", erklärt der Informatiker der Saar-Uni.

Nach zwei Wochen konnte das riesige Netzwerk vollständig aufgedeckt und zerschlagen werden, sagt „John Doe". Die Kriminellen hinter dem Botnetz wurden ebenfalls ausgemacht. Auch der Kopf der Hackerbande wurde von den amerikanischen Behörden identifiziert. Der russische Hacker Evgeniy Bogachev ist von der US-amerikanischen Staatsanwaltschaft in Pittsburgh für die digitalen Raubzüge angeklagt worden. Laut der Staatsanwaltschaft befindet er sich allerdings in Russland oder der Ukraine auf freiem Fuß.

Der Mitarbeiter der Universität des Saarlandes hält seine Urkunde vom Federal Bureau of Investigation (FBI), die er für seine Arbeit für den US-Geheimdienst erhalten hat, vor sein Gesicht. FOTO: FLOM

AUF EINEN BLICK

Einen effektiven Schutz gegen digitalen Bankraub bieten heute optische Chip-TAN-Generatoren. Dabei wird bei einer Online-Überweisung die EC-Karte in ein Lesegerät gesteckt, das einen blinkenden Strichcode auf dem Bildschirm abliest und daraus eine sogenannte Transaktionsnummer erstellt. Diese muss auf der Internetseite der Bank eingegeben werden, um die Überweisung vornehmen zu können.
Die Experten der Saar-Uni erklären, dieses System sei sicher. Allerdings sollten Nutzer grundsätzlich die eingegebene Kontonummer, Bankleitzahl und den Betrag genau überprüfen, bevor sie die Überweisung bestätigen. Auch das mobile-TAN-Verfahren, bei dem eine Transaktionsnummer per SMS an den Nutzer gesendet wird, bewerten die IT-Forscher als unbedenklich. Allerdings nur, wenn das Handy, auf dem die SMS empfangen wird, über keinerlei Internetverbindungen verfügt – kritisch sind also Smartphones, da diese ständig mit dem Internet verbunden sind. Neben sicheren Transaktionsverfahren, empfehlen Experten außerdem, immer ein Antivirenprogramm zu verwenden und keine Datei-Anhänge oder Links aus unbekannten E-Mails zu öffnen. *flom*

Märchenhaftes Uni-Kino

Das Asta-Kino der Universität des Saarlandes zeigt heute die Tragikomödie Moonrise Kingdom von Regisseur Wes Anderson. Der Film erzählt die skurrile und märchenhafte Geschichte zweier Kinder, die sich verlieben und beschließen, gemeinsam auszureißen. Der Streifen (unter anderem mit Tilda Swinton, Bruce Willis und Edward Norton, v.l.n.r.) wird im englischen Original mit deutschen Untertiteln ab 19 Uhr im Audimax (Gebäude B4 1) gezeigt. FOTO: DPA/FLOM

Studenten drohen bei zu viel Verdienst im Job Bafög-Kürzungen

Berlin. Bafög-Empfänger mit einem Nebenjob müssen genau rechnen. Wer zu viel zum Bafög dazuverdient, muss unter Umständen damit rechnen, dass die staatliche Förderung gekürzt wird. Darauf weist das Deutsche Studentenwerk in einer neuen Broschüre hin. Pro Jahr dürfen Studenten nicht mehr als 4888,20 Euro brutto verdienen, wenn sie eine Kürzung verhindern wollen, erklärt das Deutsche Studentenwerk. Umgerechnet auf zwölf Monate sind das Einnahmen von 407,34 Euro pro Monat. Wer also einen Minijob annimmt, in dem er 450 Euro brutto pro Monat verdient, muss nach den Angaben des Studentenwerks bereits mit einer Kürzung rechnen. Wer unsicher ist, kann sich von den Sozialberatungsstellen der Studentenwerke helfen lassen. *dpa*

Einblicke ins Studium an Saar-Universität und HTW

Saarbrücken. Wie funktioniert das Studium an der Universität des Saarlandes und der Hochschule für Technik und Wirtschaft (HTW)? Um diese Frage Schülern der gymnasialen Oberstufe zu beantworten, haben beide Hochschulen das sogenannte Schnupperstudium eingerichtet. Interessierte können jederzeit kostenlos ausgewählte Lehrveranstaltungen beider Hochschulen besuchen und so an Seminaren, Übungen oder Vorlesungen teilnehmen. Eine Übersicht über alle derzeit angebotenen Veranstaltungen gibt es im Internet unter der Adresse **uni-saarland.de/schnupperstudium**.

Für Schüler, die noch unentschlossen bei der Studienfachwahl sind, hat die Saar-Universität außerdem einen Interessenstest eingerichtet (**uni-saarland.de/schueler**). Dieser soll anhand von Fragen ermitteln, welches Fach den eigenen Neigungen am besten entspricht. *flom*

www.
uni-saarland.de/schnupperstudium
uni-saarland.de/schueler

Im Schnupperstudium können Oberstufenschüler erste Uni-Erfahrungen sammeln. FOTO: UNI

NACHRICHTEN

Saar-Uni richtet Fonds für Fahrtkosten ein

Saarbrücken. Die Saar-Uni hat für Studenten und Doktoranden einen Mobilitätsfonds eingerichtet. Aus diesem sollen Fahrten an die Universitäten der Großregion (Kaiserslautern, Lüttich, Luxemburg, Lothringen, Saarbrücken und Trier) finanziert werden. Die Anträge zum Mobilitätsfonds gibt es im Internet. *red*

www.
uni-gr.eu/leben-verkehr/unigr-mobilitaetsfonds

Woran forschen Kulturwissenschaftler?

Saarbrücken. Was ist Kultur? Antworten auf diese Frage soll der gleichnamige Kurs am Zentrum für lebenslanges Lernen der Saar-Universität liefern. Die Teilnehmer werden erarbeiten, was alles unter die Kategorie Kultur fallen kann und womit sich die Kulturwissenschaften beschäftigen. Mehr Informationen zum Kurs gibt es im Internet. *red*

www.
uni-saarland.de/zell

Vorlesungsreihe zu Regisseur Jim Jarmusch

Saarbrücken. Am Donnerstag, 30. Oktober, hält Dominik Schmitt vom Bachelor Optionalbereich der Saar-Universität im Rahmen der Ringvorlesung „Das postmoderne Kino des Jim Jarmusch" einen Vortrag über den Film „Only Lovers Left Alive". Die Vorlesung beginnt um 16 Uhr auf dem Campus der Saar-Uni in Gebäude C5 3, Raum U10. *red*

Orchester und Chor suchen Verstärkung

Saarbrücken. Chor und Orchester der Universität des Saarlandes suchen nach neuen Mitgliedern. Der Chor probt montags von 19 bis 21 Uhr im Musiksaal der Saar-Uni (Gebäude C5 1), das Orchester mittwochs von 19 bis 21.30 Uhr ebenfalls im Musiksaal. Weitere Informationen zu den musikalischen Ensembles gibt es im Internet. *red*

www.
unimusik-saarland.de

Info-Tag für Jura- und BWL-Studenten

Saarbrücken. Am 19. November findet auf dem Campus der Saar-Universität in Gebäude B4 1 der 5. Fakultätskarrieretag der Rechts- und Wirtschaftswissenschaften statt. Studenten dieser Fachrichtungen können sich dort mit Vertretern von Unternehmen über ihre Karrierechancen und den Berufseinstieg austauschen. *red*

Auszeichnung für Saarbrücker IT-Forscher

Saarbrücken. Die Saarbrücker Informatiker Sven Obser, Philipp von Styp-Rekowsky und Professor Michael Backes wurden beim Deutschen IT-Sicherheitspreis der Horst Götz Stiftung für ihre Anti-Spionage-App SRT Appguard ausgezeichnet. Die Forscher der Saar-Uni belegten mit dem Sicherheitsprogramm den mit 40 000 Euro dotierten dritten Platz. Über die Smartphone-Anwendung können Nutzer festlegen, welche Daten eine App sammeln darf. *afu*

PRODUKTION DIESER SEITE:
FLORIAN MAYER
PETER BYLDA