REPORTER:INNEN forum

Einreichung Recherche-Serie

Erklärung vorab: Mit unserer Recherche-Serie decken wir ein bisher unbekanntes internationales Scam-Netzwerk auf, das betrügerische SMS weltweit verschickt. Die Betrüger erbeuten mehr als 880.000 Kreditkartendaten in kurzer Zeit. Erstmals ermöglichen wir Einblicke in die Infrastruktur dieser Scam-Industrie: Wir zeigen, wie es auf der anderen Seite aussieht, wenn arglose Betrugsopfer ihre Kreditkartendaten in täuschend echt wirkende Fake-Webseiten eintragen. Der Mann, der die Betrugssoftware „Magic Cat" programmiert, mit der die Fake-Webseiten erstellt werden, versteckt sich im Internet hinter Katzenbildern. Wir enthüllen seine wahre Identität: Yucheng C., ein Mann Mitte 20 aus Henan in China. Unsere Recherche führt uns auch in die USA und nach Thailand, wo wir uns auf die Spur der Betrüger begeben. Bis es zur Konfrontation in Bangkok kommt…

Für unsere Recherche kombinieren wir Undercover-Arbeit, OSINT, Datenanalyse, Vor-Ort-Recherche und kooperierten mit Reporter:innen vom Norwegischen Rundfunk NRK sowie der französischen Zeitung Le Monde. Herzstück der Veröffentlichung ist eine dreiteilige Doku-Serie in der ARD-Mediathek. Bei dem eingereichten Text handelt es sich um einen Text auf tagesschau.de, den wir parallel zu unseren anderen Multimedia-Veröffentlichungen (siehe angefügte Links) veröffentlichen.

Links zur Multimedia-Veröffentlichung:

- *Doku-Serie „Kings of Scam. Millionen mit Fake-SMS", ARD Mediathek, 3 Teile, 90 Minuten: https://1.ard.de/kings-of-scam*
- *Trailer Doku-Serie, Kings of Scam, 1 Minute: https://www.ardmediathek.de/video/Y3JpZDovL2JyLmRlL2Jyb2FkY2FzdC8zYzA4OWY4NC0wNGUwLTQ5MDMtODQxYS04ZjMyYmNiZGYwMmZfb25saW5lYnJvYWRjYXN0*
- *Tagesschau-Podcast 11km: Betrug mit Paket-SMS: Das System hinter den Scam-Nachrichten, 33 Minuten: https://www.ardsounds.de/episode/urn:ard:episode:9369e4f81da2b089/*
- *BR 24 Radio: Die Millionen-Abzocker – Phishing-SMS aus China und warum niemand sie stoppt, Der Funkstreifzug, 12 Minuten: https://www.ardsounds.de/episode/urn:ard:episode:ca05f968c13cac70/*
- *Nachrichtentext tagesschau.de: Wie ein Betrugs-Netzwerk in China Schutz findet: https://www.tagesschau.de/investigativ/br-recherche/smishing-china-100.html*
- *Nachrichtentext BR.de: Betrug per SMS – Wie Cyber-Kriminelle in China Schutz finden https://www.br.de/nachrichten/deutschland-welt/betrug-per-sms-wie-cyber-kriminelle-in-china-schutz-finden,VFMPsEe*

- *Nachrichtentext BR.de: Kampf gegen Phishing-SMS – Telekom sieht rechtliche Hürden https://www.br.de/nachrichten/deutschland-welt/kampf-gegen-phishing-sms-telekom-sieht-rechtliche-huerden,VFMUHLx*
- *Pressemitteilung des BR: https://www.br.de/presse/inhalt/pressemitteilungen/kings-of-scam-investigative-doku-serie-bayerischer-rundfunk-team-recherche-100.html*
- *Instagram Reel BR24: https://www.instagram.com/reels/DWrnnouCZGp/*
- *Instagram Reel ARD Mediathek: https://www.instagram.com/reel/DWleU8bmDWR/?hl=de*
- *Instagram team.recherche: https://www.instagram.com/reel/DWlWrEPjImB/?stkn=enRnNHYzY29ta2x3*
- *Instagram team.recherche: https://www.instagram.com/p/DXHcwhNlvGW/?stkn=NGc5eWw5Ymc5aWp0*
- *Tiktok BR24: https://www.tiktok.com/@br24/video/7623431748822617366*
- *Tiktok ARD Mediathek: https://www.tiktok.com/@br24/video/7623431748822617366*
- *Tiktok ARD Mediathek: https://www.tiktok.com/@ardmediathek/video/7628166162282482977*
- *Youtube BR24: https://www.youtube.com/shorts/uT6yOVJBKhQ*
- *Wir finden den DHL Scammer in Thailand, Youtube, offen un' ehrlich: https://www.youtube.com/watch?v=o47x0fpUmLw*
- *Dokuserie Kings of Scam auf Englisch, ARD Mediathek, 3 Teile, 90 Minuten: https://www.ardmediathek.de/video/kings-of-scam-millionen-mit-fake-sms/episode-1-you-ve-got-mail/br/Y3JpZDovL2JyLmRlL2Jyb2FkY2FzdC9kN2UxY2FjYi02MzdjLTQ1OGUtYjNiNS1kYzE5MjI1ZmY5MDVfb25saW5lYnJvYWRjYXN0*

Wie ein Betrugs-Netzwerk in China Schutz findet

Hunderttausende Opfer gefälschter Paket-SMS gibt es weltweit. Der Schaden geht womöglich in die Milliarden. Recherchen des BR und internationaler Medien belegen: Die Betrüger agieren aus China - und die Volksrepublik lässt sie offenbar gewähren.

Von Arne Meyer-Fünffinger, Sammy Khamis, Alexander Nabert, Lena Walbrunn, Julia Schweinberger, BR

"Das DHL-Paket kann nicht zugestellt werden". Als Lucy und Fabrice diese Nachricht erhalten, wirkt sie für sie glaubwürdig. Das Berliner Paar, das nur mit Vornamen genannt werden will, erwartet tatsächlich eine Lieferung - Tierfutter. Die Nachricht enthält einen Link zu einer angeblichen DHL-Seite. 27 Cent Servicegebühr seien noch fällig. Sie geben ihre Kreditkartendaten ein. Wenig später buchen Betrüger dem Paar mehr als 1.600 Euro ab.

Lucy und Fabrice sind zwei von Hunderttausenden Opfern einer globalen Betrugsmasche. Hinter der gefälschten DHL-Seite steht eine chinesische Software namens "Magic Cat" und ein Netzwerk, das sich "Darcula" nennt. Wie ungehindert es von der Volksrepublik aus agieren kann, zeigen neue Recherchen des BR gemeinsam mit dem norwegischen Rundfunk NRK und Le Monde aus Frankreich.

Scammer testen Fake-Webseiten von China aus

Die drei Medien analysierten eine Datenbank, die mit "Magic Cat" verbunden ist. In dieser Datenbank sind Aufrufe der Betrugsseiten gespeichert sowie persönliche Daten von Betrugsopfern wie Lucy und Fabrice. In Summe sind es mehrere Millionen Einträge aus dem Zeitraum von Ende 2023 bis Mitte 2024.

Reporterinnen und Reporter fanden in der Datenbank ein Muster: Bevor die Scammer die Phishing-SMS an Smartphone-Nutzer verschicken, überprüfen sie offenbar die Funktionsfähigkeit ihrer Fake-Webseite - mithilfe von Einträgen wie "Test" oder "123456".

Die Software "Magic Cat" speichert bei jedem Seitenzugriff die IP-Adresse. So lässt sich auf den Aufenthaltsort der Betrüger schließen: Demnach agieren mehr als 300 von ihnen von China oder dessen Sonderverwaltungsregion Hongkong aus.

Expertin: Spur nach China "nicht überraschend"

Antonia Hmaidi, China-Expertin vom Mercator Institute for China Studies (Merics) in Berlin, sagt im Interview mit dem BR, für sie sei "nicht überraschend, dass die Spur nach China führt". Vieles spreche dafür, "dass das in China beheimatete Menschen sind, die mit ziemlich großer Wahrscheinlichkeit chinesische Staatsbürger sind".

Weiter fällt auf, dass sich in der Datenbank kaum Opfer in China finden. Dazu passt, dass die Betrugssoftware Vorlagen für Fake-Webseiten von Unternehmen und Organisationen aus mehr als 130 Ländern anbietet, jedoch nicht für China.

Dem Reporterteam gelingt es im Lauf der Recherche, verdeckt mit einem besonders aktiven Scammer aus dem Netzwerk - er nennt sich "X667788X" - in Kontakt zu treten und ihn zum Vorgehen der chinesischen Behörden zu befragen. Er antwortet: "Solange man die nationalen Interessen nicht antastet, interessiert das die chinesische Polizei nicht." Wie ernst diese Aussage zu nehmen ist, lässt sich nicht abschließend klären.

Komplizierte Ermittlung der Täter

Opfer des Betrugs in Deutschland, die das team.recherche des BR mithilfe der Datenbank ausfindig machen konnte, berichten davon, dass die Polizei die Ermittlungen jeweils eingestellt hat. Die Begründung in der Regel: Täter nicht ermittelbar.

Eine Sprecherin des Bundeskriminalamts teilt auf Anfrage mit, die Behörde kenne "Magic Cat" und das "Darcula"-Netzwerk. Die Frage, ob es aktuell Ermittlungen in diesem Zusammenhang führt, lässt das BKA unbeantwortet und verweist auf "kriminaltaktische Gründe".

Im Mai 2025 hatten BR, NRK und Le Monde erstmals über die DHL-Masche und die "Magic Cat"-Software berichtet. Daraufhin tauchte der 25-jährige Chinese Yucheng C., mutmaßlich Entwickler der Software, ab. Die Betrugssoftware war danach nicht mehr zu kaufen.

Laut dem IT-Sicherheitsberater Ford Merrill (CSIS/SecAlliance) folgten darauf mehrere Programme mit nahezu identischer Funktionalität, darunter das Programm "Magic Mouse". "Es ist wie bei einer vielköpfigen Hydra, schlägt man einen Kopf ab, wachsen zwei neue nach", sagt Merrill. Den globalen Schaden durch diese Art des Betrugs beziffert er auf mehrere Milliarden Dollar.

"Ökosystem" mit Tausenden Akteuren

Insgesamt stellt Merrill fest: "Die Aktivitäten im chinesischsprachigen Betrugsökosystem sind vielfältig. Wir gehen davon aus, dass Zehntausende, wenn nicht Hunderttausende Akteure in diesem System aktiv sind - von Käufern und Verkäufern bis hin zu verschiedenen Anbietern unterschiedlichster Technologien." Phishing durch Textnachrichten habe nicht abgenommen, sondern habe sich "seit Anfang 2023 fortgesetzt und möglicherweise sogar noch verstärkt."

Laut Antonia Hmaidi hätte das Regime in Peking die technischen Möglichkeiten, entsprechende Scams einzudämmen. "Sie könnten es extrem viel schwieriger machen, zum Beispiel die Software zu verteilen. Es würde wahrscheinlich noch immer kleine Fälle geben, aber nicht mehr in dieser fast industriellen Größe."

Der BR konfrontierte die chinesische Botschaft in Berlin mit den Rechercheerkenntnissen und schickte mehrfach eine detaillierte eine detaillierte

Anfrage. Eine Antwort gibt es nicht. Auch telefonische Anfragen blieben bislang ohne Ergebnis.

Kiesewetter: China ist "Rivale"

Nach Einschätzung des CDU-Außenpolitikers Roderich Kiesewetter toleriert China diese Betrugsmasche und leistet "Beihilfe zum organisierten Verbrechen". Solange das so sei, könne man nicht von einer "Partnerschaft mit China" sprechen. "China ist auch kein Wettbewerber, sondern ein Rivale oder besser gesagt ein Gegner", erklärt der CDU-Politiker.

Kiesewetter fordert von der Bundesregierung, das Thema Betrug durch chinesische Cyberkriminelle müsse auf die Tagesordnung der bilateralen Gespräche zwischen der Volksrepublik und Deutschland.

Ähnlich äußert sich die Linken-Digitalpolitikerin Donata Vogtschmidt im BR-Interview: "Ich sehe ganz klar die Bundesregierung in der Verantwortung, diplomatische Beziehungen genau zu diesem Thema mit China aufzunehmen."