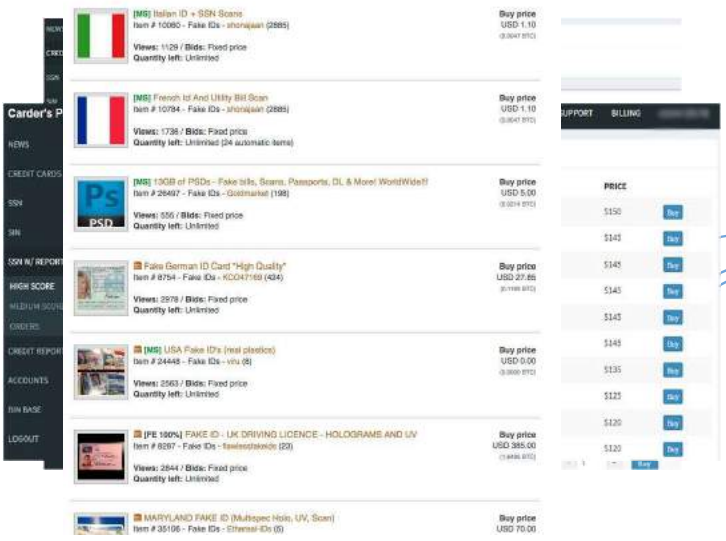

RISK
IDENT
Betrugserkennung durch
Geräteidentifizierung
Verpassen deutsche Banken den Standard?

Das kostet eine Identität



Bankkonto: 25,- bis 65,-

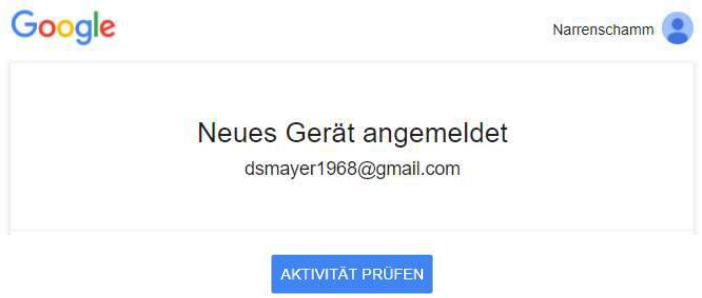
Identitätsdaten inkl. Auskunfteibericht 120,- bis 150,-

Ausweis: nach Land, Art und Qualität 1,- bis 600,-

Quellen: Carders Paradise, Motherboard

Auch Konten deutscher Banken sind zu finden.

Device Identifizierung ist Standard



Schwieriger ist der Rechner.
Natürlich kann auch dieser gefaked werden, doch das ist nicht einfach.

Üblich ist die Verwendung einer VM und ein Anonymisierungsnetzwerk.

Die Einbindung der User in die Betrugsprävention ist bei Technologieunternehmen bereits Alltag.
In der Regel findet die einfache Identifzierung mit Hilfe von Cookies oder einfachem Auslesen der vom Gerät selbst übermitttelten Daten statt.

Beim Einsatz dieser einfach zu umgehenden Technologien geht es i.W. um die Vermittlung eines Sicherheitsgefühls und die Einbindung der User über eine zeitliche Komponente:
es ist nicht so wichtig, ob das Gerät richtig identifiziert wurde. Die fehlerhafte Nicht-Wiedererkennung eines Geräts ist häufig und wird vom User akzeptiert.
Das plausible und hilfreiche Grundprinzip ist in automatisierten Entscheidungsprozessen daher nicht akzeptabel.

Device Fingerprint: so funktioniert‘s

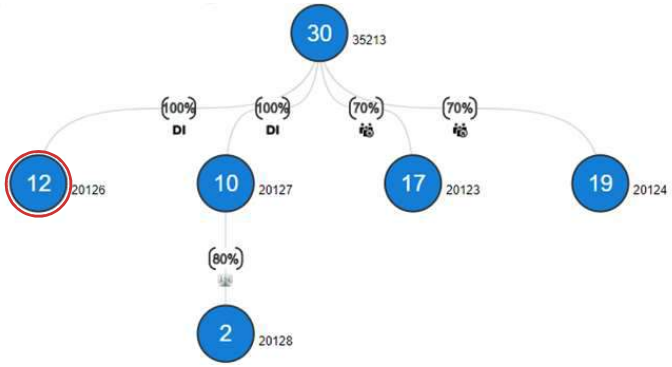
- Operating System: Windows XP
- Language: German
- Browser: Firefox 31.0
- Resolution: 1280x909
- Geolocation: Russia
- Plugin: Java 6.0.220.4
- …

Device Fingerprinting funktioniert etwas komplexer.

Vom Browser wird ein ausführbares Skript aufgerufen, welches verschiedene Browserkonfigurationen ausliest, plugins usw. prüft.
Bei der Nutzung von nativen Apps können teilweise auch Jailbreaks und Schadsoftware erkannt werden.

Die ausgelesenen Daten werden mit einem pseudonymen Merkmal übermittelt, mit dem der Kunde bei der Rückübermittlung der Daten wieder zugeordnet werden kann.
Die Daten werden auf dem Server angereichert (Geolokation), weitergehend pseudonymisiert und ein Fingerprint erzeugt, welcher auch eine unscharfe Suche erlaubt.

Prüfung von Verbindungen



Einfach sind exakte Matches.
Geräteeinstellungen und Browserkonfigurationen verändern sich jedoch im Zeitverlauf. Wesentlich und analytisch komplexer wird es bei Smart-Matches. Dies sind unscharfe Treffer, die angeben, mit welcher Wahrscheinlichkeit ein Gerät wiedererkannt wird. Qualitativ hochwertige Lösungen erkennen sich verändernde Geräte mit einer hohen Trennschärfe.

Aus diesen Übereinstimmungen werden Netzwerke aufgebaut (Graphen). Wird ein Gerät im Netz kompromittiert, kann dieser Hinweis ausgegeben werden.

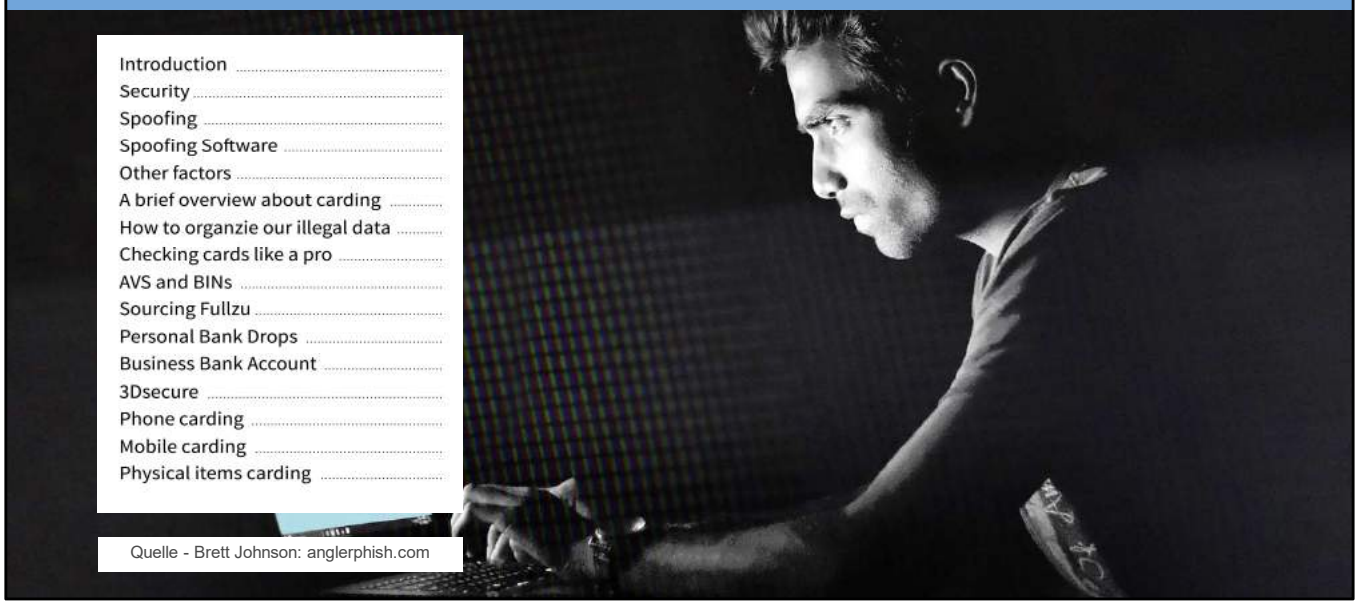
Plausibilitätsregeln

Fingerprint X	Unterschiedliches Device	Fingerprint Y
0116693307	Gleicher Identifikator	**0116693307**
Deutschland	Risk Country	Russland
False	Identifizierte VM	True
Windows 7, FF aktuell	Unterschiedliches Betriebssystem	Windows XP, FF veraltet

In der Betrugsprävention werden direkte Hinweise auf verbundenen Geräten genutzt, außerdem werden Plausibilitätsregeln und Profilregeln geprüft.
Regelmäßig wird dazu ein pseudonymisierter Kundenidentifkator mitgelifert, z.B. die (verhashte) Kundennummer.

Das Ergebnis kann in einzelnen Regelhinweisen und als Score zurückgegeben werden.

The Definitive Fraud Dictionary – eine Anleitung für Betrüger



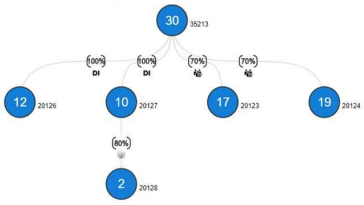
Account Takeover und Identitätsübernahme sind Standard im organisierten angelsächsischem Betrug.
Die Quoten in Deutschland steigen.

Vor Weihnachten wurde ein Trainingsdokument für Betrüger geleakt.
Hier wird vom Aufsetzen des Rechners bis zur Übernahme kompletter Identitäten alles erklärt.
Für 100,- USD erhalten Sie eine Anleitung, wie sie Betrüger werden. Für etwas mehr gibt es dazu auch Online-Kurse.
Dieses amerikanische Szenario wird mit der Digitalisierung der Konten- und vor allem der Kreditprozesse noch deutlich kritischer.

Einer der wenigen Angriffspunkte für die Betrugsprävention ist der Rechner des Betrügers.
„Es ist schwerer einen Rechner zu verfälschen, als eine Identität.“

Anwendungsszenarien

Aufdecken von Antragsbetrug



Multi-Faktor-Authentifizierung

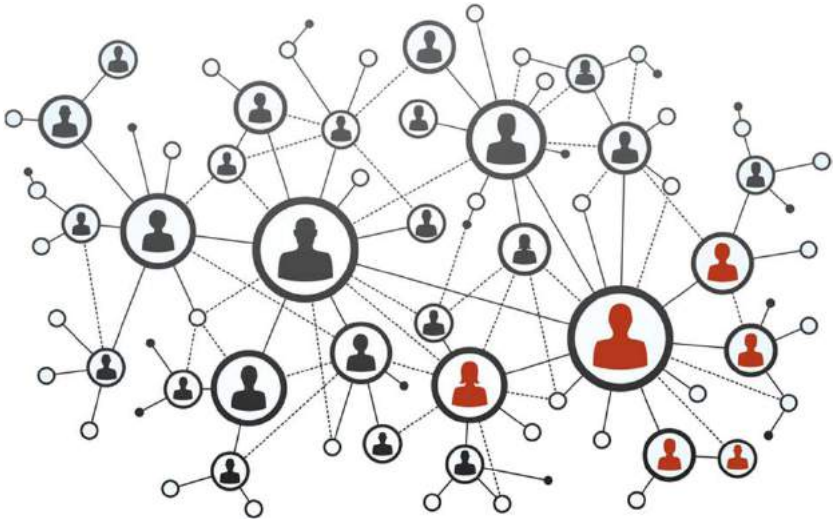
z.B. zur Abwehr von Account Takeover

In der Verhinderung von Antragsbetrug ist das Gerät als schwer austauschbare Ressource eines Betrügers ein wesentlicher Datenpunkt.
Im digitalen Kreditprozess wird ein wesentlicher Baustein in der Verteidigung gegen Antragsbetrug werden, denn die Zugangsdaten zum Konto sollten prinzipiell als kompromittiert gelten.

Bei Transaktionen kann das Gerät als Teil von Multi-Faktor-Authentifizierungen verwendet werden.
Auch eine Härtung von Videoidentifzierungen ist im Gespräch.

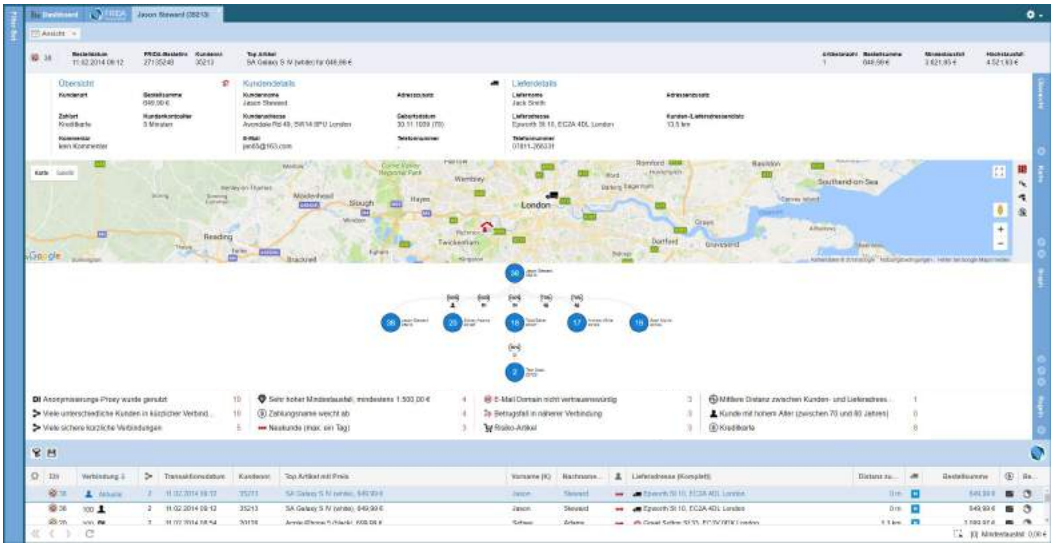
Dabei können die Device-IDs sowohl zur Bestätigung der Identität bekannter Kunden, als auch zur Identifzierung von Betrugsversuchen genutzt werden.

Pooling



Im Handel und in der Telekommunikation werden Gerätedaten bereits lange gepoolt. Typisch sind hier Pools auf dem Gegenseitigkeitsprinzip, d.h. die Teilnehmer liefern Hinweise auf betrügerische Geräte in die Pools ein.
Pools gibt es für einzelne Institute, Konzerne, Branchen oder auch übergreifend über alle Teilnehmer.

Kombination mit weiteren Daten



Inhouse lassen sich die Gerätedaten und die getroffenen Regeln über den Identifikator mit anderen Daten des Kunden verknüpfen.

Der physische Fußabdruck des Geräts erlaubt deutlich trennschärfere Regeln zur Betrugsprävention und zur positiven Bestätigung unkritischer Anträge und Transaktionen.

Das BILD zeigt das Fraud-Case-Management FRIDA von Risk Ident.

RISK IDENT

- Hauptsitz Hamburg
- Teil der otto group
- 75 Mitarbeiter
- Hosting ausschließlich in Deutschland

Risk Ident ist Teil der Otto-Gruppe.
Wir bieten mit Device Ident die einzige relevante europäische Lösung zum Device Fingerprinting.

Risk Ident betreibt den größten Gerätepool innerhalb von DACH.

Mit unserem Fraud-Case-Managementsystem FRIDA bieten wir eine der wenigen Lösungen zur Identifzierung und Bearbeitung von Verdachtsfällen.

Zusammenfassung

- Device Identifizierung ist weltweiter Standard in der Betrugsprävention. In deutschen Banken ist dieser Standard bisher nicht angekommen.
- Aufgrund der Digitalisierung hat das Device-Fingerprinting eine kritische Rolle in der Betrugserkennung und im Schutz der Kunden.
- Device Ident liefert einen erheblichen Mehrwert bei der Formulierung von Regeln zur Betrugserkennung.


RISK
IDENT
www.riskident.com
Kontakt
Dirk Mayer
Senior Consultant Fraud Prevention
0151 20 106 068
dirk.mayer@riskident.com

RISK IDENT

www.riskident.com

Kontakt
Dirk Mayer
Senior Consultant Fraud Prevention
0151 20 106 068
dirk.mayer@riskident.com

SAVE THE DATE

20. SEPTEMBER 2018

ONLINE FRAUD FORUM