Newsletter September 2022

- Crime as a Service 2.0
- Verräterischer Facebook Chat
- Twitter verliert Nutzerdaten
- Neues von den Domains: .be, .gl, .nl, .lat, .tr und Verisign

Crime as a Service 2.0

Die technische Weiterentwicklung bleibt auch bei Kriminellen nicht stehen. Bereits bekannt sind Dienste, die nach einem Baukastenprinzip erlauben, Viren und Trojaner zu erstellen und diese als Massenmail unter die Leute zu bringen. Allerdings war es dann noch nötig, die so infizierten Systeme gewinnbringend einzusetzen, was ‚Kontroll- und Kommando-Server' erfordert.
Genau diese bietet ein neuer Anbieter jetzt als Clouddienst an. Die Server stehen dabei teilweise offen in Ländern mit schlechter Rechtsdurchsetzung, teilweise operieren sie über das Tor-Anonymisierungsnetzwerk. Zugehörig ist ein ‚Content Delivery Network', das die Schadprogramme vorhält, die nach dem Eindringen in ein System nachgeladen werden, um den eigentlichen Angriff auszuführen. In weniger schlimmen Fällen werden die Systeme für die Suche nach Bitcoins missbraucht und treiben ‚nur' die Stromrechnung in die Höhe. Schwerwiegender sind Angriffe wie Identitätsdiebstahl oder die Verschlüsselung aller irgendwie erreichbaren Daten und Übermittlung der Lösegeldforderungen.
Auf einer Weltkarte lässt sich komfortabel nachverfolgen, wo sich das eigene Baukastenvirus besonders ausbreitet. Einsteigerfreundlich ist auch der Preis, der bei 10€ pro Monat liegt. Bisher gibt es einige tausend registrierte Nutzer. Bei den geringen Einstiegshürden dürfte es nicht lange dabei bleiben.

Verräterischer Facebook Chat

Wie berichtet war nach den teilweisen Einschränkungen des Abtreibungsrechts in konservativen US Bundesstaaten zu erwarten, dass Netzwerkanbieter von den Gesetzeshütern in die Pflicht genommen werden, bei der Aufklärung von Verstößen mitzuwirken. Der erste in diesem Zusammenhang bekannt gewordene Fall betrifft eine 17-jährige Schwangere aus Nebraska nebst ihrer Mutter. Beide hatten sich über den Facebook Chat darüber unterhalten, ob und wann das unter der Hand besorgte Abtreibungsmedikament einzunehmen sei.
Die Polizei wurde durch einen anonymen Tipp auf die Facebook Chats aufmerksam und beschlagnahmte daraufhin sämtliche Internetgeräte im Haus der Familie. Die Auswertung der Daten dauert noch an. Die Staatsanwaltschaft hat derweil Anklage gegen Mutter und Tochter erhoben.

Twitter verliert Nutzerdaten

Nachdem ein unbekannter Hacker die Daten von über fünf Millionen Nutzern im Darknet angeboten hatte, musste Twitter einräumen, dass diese echt sind und wohl im Rahmen einer bereits geschlossenen Sicherheitslücke beim Anmeldeprozess abgegriffen wurden. Zur Lücke hatte Twitter eigentlich ausgesagt, dass es keine Anzeichen von Fremdzugriff gegeben habe. Diese Aussage war offensichtlich nicht zutreffend. Immerhin seien keine Kreditkartendaten betroffen. Sagt Twitter.
Betroffene Nutzer wurden von Twitter informiert. Gleichzeitig wurde für den Einsatz von Zwei-Faktor-Authentifizierung geworben.

Neues von den Domains

.be

Die belgische Registry beginnt einen offenen Konflikt mit ICANN und kürzt seine ICANN-Beiträge um zwei Drittel, insgesamt jährlich 50.000 US-Dollar. Grund ist das ‚selbstherrliche' Auftreten ICANNs, das seine europäischen Partner auffordert, von den ICANN Mitgliedern erarbeitete Richtlinien umzusetzen, selbst aber nur sehr geringe Bemühungen zeige, europäische Standards wie die DSGVO anzunehmen. ICANN sei ein Institutionsmoloch geworden, der von seinem eigenen Gewicht erdrückt werde.
ICANN reagierte verschnupft und suggerierte in einer öffentlichen Antwort, dass die Belgier wohl versuchen würden, in wirtschaftlich schwierigen Zeiten Geld zu sparen. Die Quartalsberichte der Belgier lassen nicht erkennen, dass die Registry wirtschaftliche Kompromisse eingehen muss.

.gl

Grönland nutzt bald die Registry-Technik von Centralnic für seine Länderendung. Damit folgen sie .fo, den Färöer Inseln, die bereits seit längerem von Centralnic betreut werden.

.nl

Die Niederländer bieten unter der Webadresse https://check.veiliginternetten.nl einen Informationsdienst in holländischer Sprache, der betrügerische Webseiten identifizieren soll, an. Grund ist der starke Anstieg von Onlinebetrug, der alleine bei unseren Nachbarn bereits im Milliardenbereich liegt.

.lat

Die TLD für Lateinamerika wird in Zukunft ebenfalls von Centralnic verwaltet. Die Betreiber erhoffen sich durch die Marketingmöglichkeiten Centralnics eine stärkere Verbreitung ihrer Endung.

.tr

Der türkische Staat wird am 14.09. den Registrybetrieb an das Infrastrukturministerium übertragen (wir berichteten). Ab diesem Tag können auch 2nd Level Domains in der Form ihre-firma.tr registriert werden. Besitzer von .com.tr, net.tr und org.tr werden bevorzugt behandelt. Vorbestellungen nehmen wir ab sofort entgegen.

Verisign

Versign plant für chinesische Interessenten für .com und .net Domains, dass diese einen von der Regierung vergebenen Code beibringen müssen, um eine Domain zu erhalten. Damit folgt Verisign der lokalen Gesetzgebung. Bemerkenswert ist dabei, dass eine Registry eine offene Ungleichbehandlung von Domainbesitzern auf technischer Ebene einführt. Dies kann sehr wohl Auswirkungen auf andere Registries haben.

Mit freundlichen Grüßen,

Ihr Global Village Team