RPU Objekt

Dragon AI

Verschlüsselungs-KI hybrider Architektur mit adaptiver Datenverdrängungstechnologie

Inhaltsverzeichnis

Kurzbeschreibung

Die **Dragon AI** gilt als eines der komplexesten und gleichzeitig gefährlichsten Razz-Verschlüsselungssysteme im zivilen Grauzonenbereich. Sie wurde um das Jahr **2950** von einem bislang nicht offiziell identifizierten Cyberentwickler unter dem Alias **GhostForce** im Umfeld von **Levski** (Nyx-System) geschaffen. Der Entwickler war bereits unter mehreren Decknamen aktiv – unter anderem als *ArcticRazz*, bekannt für modulare Blacknet-Werkzeuge wie den *ColdSplinter Injector* und das *Spectral ChainBreaker Suite*, welche primär in kriminellen und dissidenten Netzen kursierten.

Technologische Architektur: Die Dragon Bubble

Im Zentrum der Dragon AI steht die sogenannte **DragonBubble** – ein sich selbst reorganisierender, mehrschichtiger Datenraum, der **post-quantenbasierte Verschlüsselungsprotokolle**, **biometrisch-randomisierte Hash-Mapping-Algorithmen** sowie eine eigenständig lernfähige **Semi-Intelligenz** nutzt, um Datenzugriffe nicht nur zu verhindern, sondern auch proaktiv umzuleiten, zu zerstreuen und in Echtzeit neu zu verschlüsseln.

Die Dragon AI ist keine klassische Software – sie ist ein sich weiterentwickelndes System mit sogenannter **Adaptiver Datenverdrängung (ADV)**. Diese Technologie erkennt Zugriffsversuche auf bestimmte Datencluster und reagiert mit **versetzter Schattenspeicherung**, wodurch Inhalte nicht gelöscht, sondern in höherdimensionale Datenebenen innerhalb der Bubble ausgelagert werden. Das bedeutet im Klartext: Jeder nicht autorisierte Zugriff vertieft die Verschlüsselung – exponentiell.

Der God Key

Laut mehreren verschlüsselten Einträgen auf obskuren **Spectrum-Knotenpunkten** – insbesondere im Thread-Archiv von *BlackSymmetry_2949* – behauptet GhostForce selbst, dass nur er in der Lage sei, die Dragon AI vollständig zu entschlüsseln. Dies sei ausschließlich mit einem von ihm selbst generierten **God Key** möglich. Sein God Key ist **nicht reproduzierbar**, da er auf einem **neuronalen Seed-Scan seiner eigenen kortikalen Architektur** basiert – angeblich erzeugt durch eine manipulierte Version eines medizinischen NeuroScans, den er sich in der *Free Clinic* von Delamar beschafft haben soll.

Gerüchten zufolge besteht der God Key aus einer **triangulierten Datenstruktur**, kombiniert aus:

1. **Einem fragmentierten DNS-Biomatrixschlüssel**
2. **Einer sequentiell rekursiven Time-Loop-Verschlüsselung (RT-Loop Layering)**
3. **Einem lokalisierten Frequenzrauschmuster (White Noise Keyprint), das nur mit einem bestimmten Transistorarray dechiffrierbar ist**

Sicherheits- und Gefahreneinschätzung

Die **UEEN Cyber Division** sowie mehrere inoffizielle Analysten vermuten, dass Dragon AI in der Lage wäre, konventionelle Sicherheitsframeworks sogar innerhalb der **UEE Naval Intelligence** zu infiltrieren, sollten entsprechende Installationen existieren. Entsprechende Nachweise wurden nie offiziell bestätigt. In kriminellen Netzwerken wird jedoch regelmäßig gewarnt, dass ein kompromittierter Zugriff auf eine aktive DragonBubble nicht nur die Daten, sondern auch benachbarte Systeme irreversibel beschädigen kann – insbesondere bei *Deep-Root Installationen* auf mobilen Systemkernen.

Aktuelle Verwendung und Verbreitung

Die Dragon AI wurde bisher in mehreren hochgradig verschlüsselten Geräten sichergestellt – darunter in **Data-Crypt Ports**, **Mobiglas-Splits**, **Remote Uplink Crates** und sogar modifizierten **blackbox-fähigen Flugdatenspeichern**. Die Herkunft dieser Module ist meist nicht rekonstruierbar – viele tauchten nach Blackout-Einsätzen oder in Zusammenhang mit **Verschwinden von Frachtbesatzungen** in Randgebieten wie Pyro oder Cathcart auf.

Ein besonders brisanter Fund war ein **DataCrypt Core** auf einer verlassenen *Versipellis Sica*-Frachtroute in Pyro I, dessen DragonBubble zwar isoliert werden konnte, jedoch binnen Sekunden nach Zugriffserkennung den Zugriffspunkt elektromagnetisch zerstörte.

> Zitat
>
> Die Dragon AI steht exemplarisch für die nächste Stufe krimineller, autonom lernfähiger Softwaretechnologien im Grenzbereich zwischen **Cyberdefense und kybernetischem Terrorismus: Sie ist nicht knackbar – es sei denn, man besitzt den God Key. Und den kann angeblich nur ihr Schöpfer erzeugen.**