

Predator

Intelligence Extraction System



Technical Description

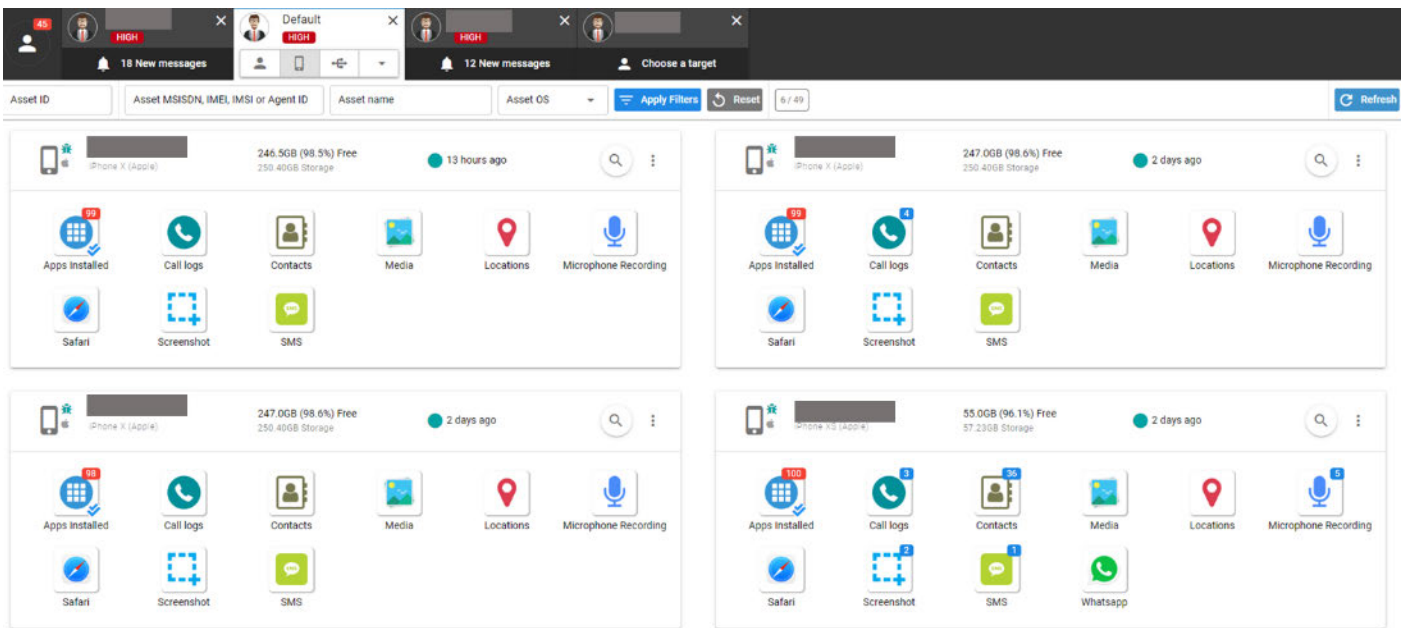


Information Type	Application	Data Extracted
Device Information	Device system information	Device model OS Version Build, IMEI, IMSI, MAC Browser information
	Installed Application list	All Applications
Call related Data	Phone calls	Call Logs
	Contacts	Contacts
	SMS / MMS	SMS / MMS
On-device Data	Browser	Browsing History Cookies Bookmarks
	Media	Photos Videos Voice Memos
Active Collection Management	Location	Current Location
	Microphone	Open Mic recording Time-triggered Mic recording
	Screenshots	Take screenshots Time-triggered screenshot
Instant Messaging	WhatsApp Telegram Viber Line	Text VOIP Images and videos Voice messages Video message Shared Locations Shared Contacts Call logs

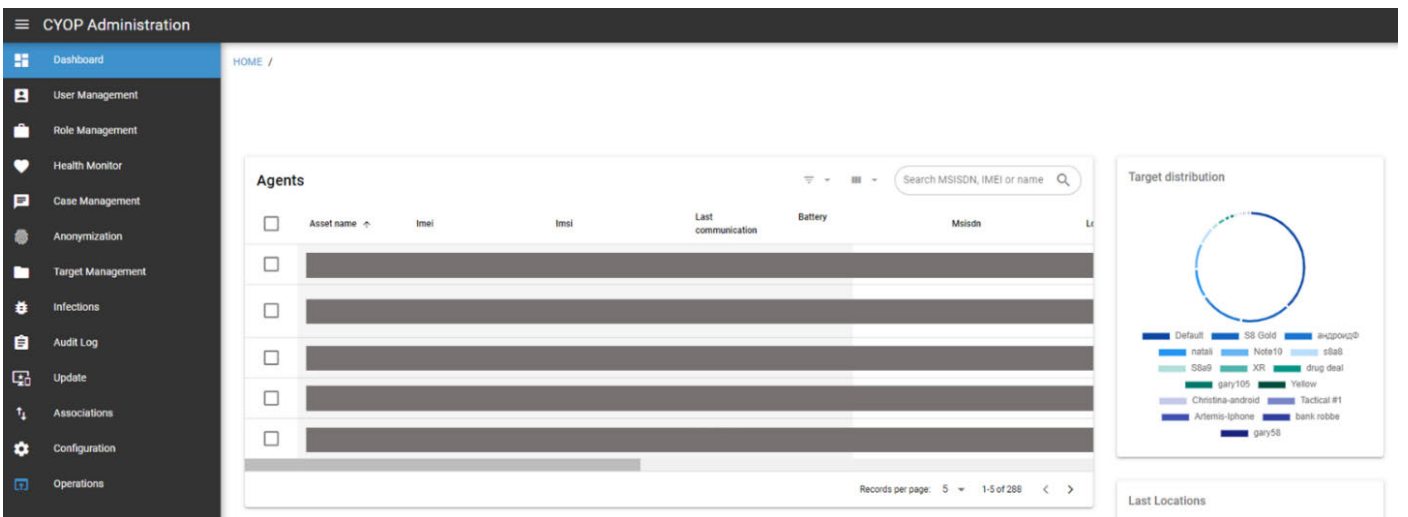
Table 1: Predator-Data extraction capabilities

Eine Übersicht über die Daten, auf die via Predator zugegriffen werden kann.

Dieses PDF enthält einzelne Bilder, die das Predator-Überwachungssystem beschreiben.
Zusammengefügt von WOZ – Die Wochenzeitung.



Die abgesaugten Daten der verschiedenen Zielgeräte werden im «Predator Control Panel» organisiert.



Über «Predator's Cyop Administration View» wird die Überwachung praktisch gesteuert.

Dieses PDF enthält einzelne Bilder, die das Predator-Überwachungssystem beschreiben.
 Zusammengefügt von WOZ – Die Wochenzeitung.

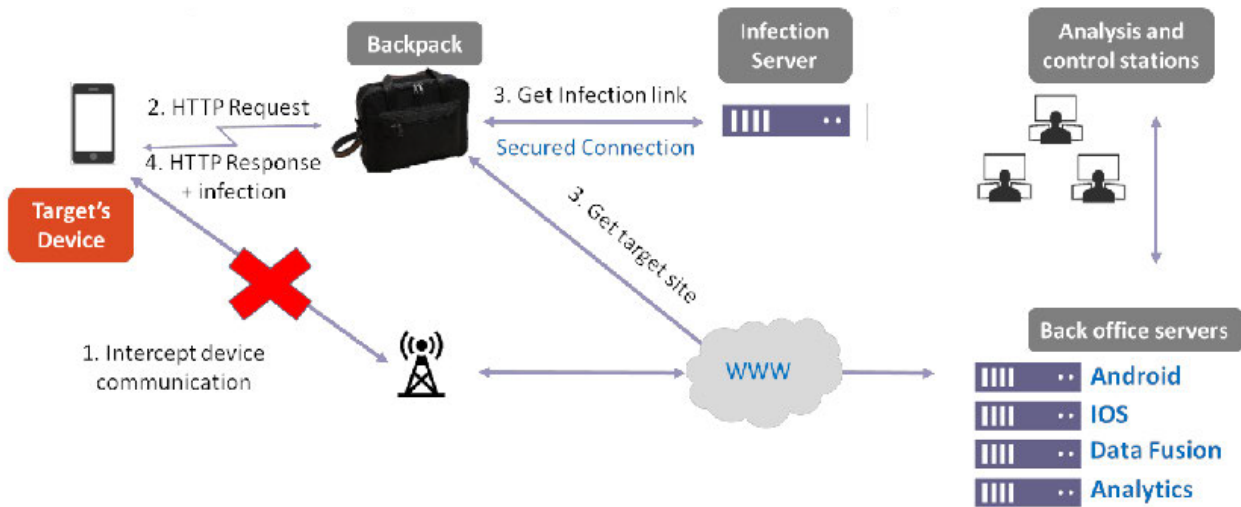


Figure 7: Predator Tactical Interception solution scheme

Die Infektion kann im «Null-Klick-Modus» erfolgen, ohne dass die Zielperson auf einen Link klicken muss. Entweder über einen IMSI-Catcher, beispielsweise versteckt in einer Tasche, oder über das Abfangen von Wifi-Signalen.

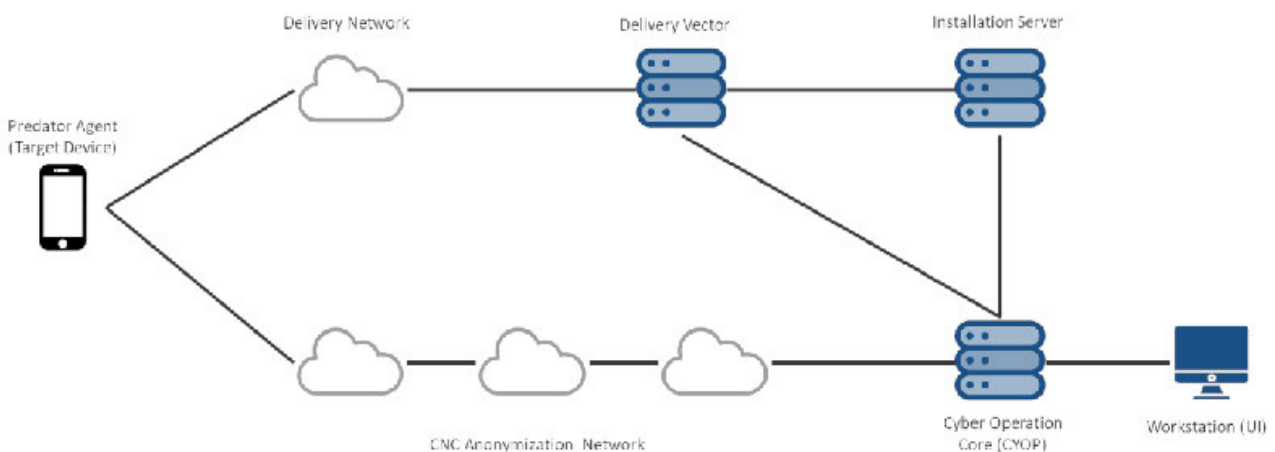


Figure 1: Predator - High-Level Architecture

Die Grafik zeigt die einzelnen Komponenten des Predator-Überwachungssystems. Dazu gehören unter anderem die Cyop-Plattform, Installationsserver, ein Zustellvektor, der eine Verbindung zum Zielgerät herstellt, um dieses zu infizieren.

Dieses PDF enthält einzelne Bilder, die das Predator-Überwachungssystem beschreiben.
Zusammengefügt von WOZ – Die Wochenzeitung.

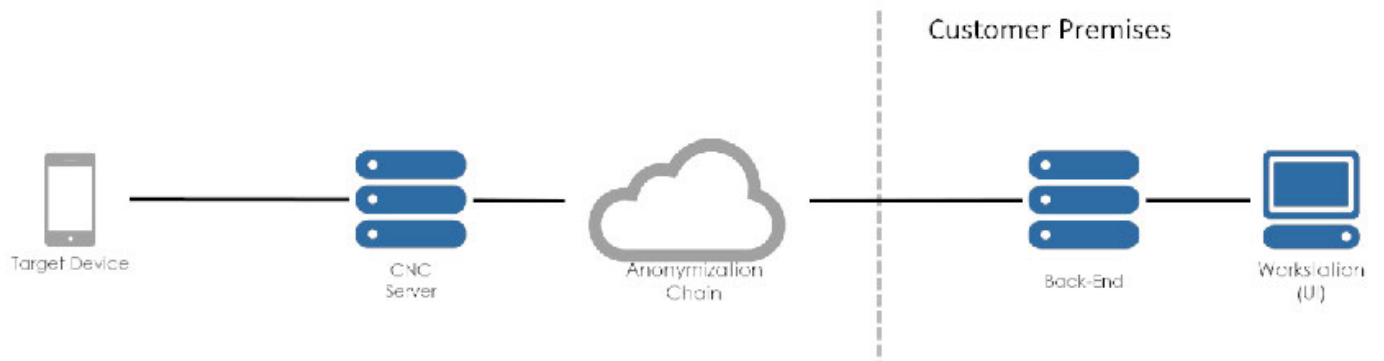


Figure 3: Predator CNC Anonymization Network

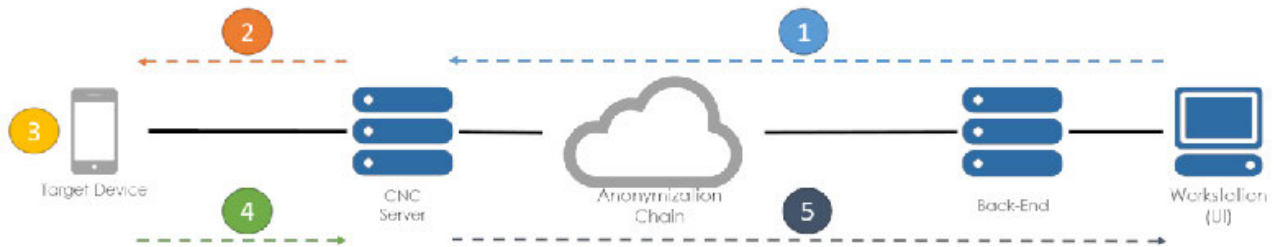


Figure 4: Predator - Ongoing Operation - Command & Control Flow

Der durch Predator ausgelöste Datenfluss wird durch verschiedene Schritte verschleiert, um die Identität der Überwacher:innen anonym zu halten.