Köln, 22. August 2024

Bundesamt für Verfassungsschutz

BfV CYBER INSIGHT

Die i-Soon-Leaks: Industrialisierung von Cyberspionage

Teil 4: i-Soon Produkte und deren Abnehmer

Die i-Soon-Leaks: Industrialisierung von Cyberspionage

Teil 4: i Soon Produkte und deren Abnehmer

Inhalt

1. Einleitung

Am 16. Februar 2024 veröffentlichten Unbekannte auf der Plattform GitHub[1] einen Datensatz, der Details zur Kooperation des chinesischen Cybersecurity-Unternehmens i-Soon mit der chinesischen Regierung bzw. deren Nachrichtendiensten enthält. Dieser und drei weitere Berichte des BfV gehen auf die Inhalte des Leaks und der mit ihnen offengelegten Möglichkeiten Chinas für Hacking-Operationen ein. Die Auswertungen belegen eine Industrialisierung von Cyberspionage durch privatwirtschaftlich organisierte Unternehmen, die im staatlichen Auftrag Cyberangriffe verüben.

Das Leak umfasst über 570 Dateien, Bilder und dokumentierte Chatverläufe in chinesischer Sprache, darunter sind:

- eine Präsentation zu Fähigkeiten und Diensten des Unternehmens i-Soon,
- Listen zu Unternehmensangehörigen, Produktinformationen und Dienstleistungen, Vertragsbüchern sowie Cyberoperationen und Zielentitäten,
- Screenshots von mutmaßlich erbeuteten Daten und
- Call-Logdateien kompromittierter asiatischer Telekommunikationsdienstleister.

Das BfV hat die veröffentlichten Informationen ausgewertet. Wenngleich die Daten keine Hinweise auf betroffene Stellen in Deutschland enthalten, bieten sie dennoch gezielte Einblicke in die Arbeitsweise privater Hackerfirmen sowie in die Verbindungen von Schadsoftware-Anbietern zum chinesischen Staat. Sie verdeutlichen, wie APT-Gruppierungen[2] agieren und mit staatlichen Stellen zusammenarbeiten.[3]

1 GitHub ist ein Onlinedienst zur Softwareentwicklung und Versionsverwaltung für Softwareprojekte.

2 Mit Advanced Persistent Threats (APT) werden komplexe und zielgerichtete Bedrohungen bezeichnet, die sich gegen ein oder wenige Opfer richten. Es handelt sich in der Regel um ressourcenstarke, staatlich gesteuerte Cyberangreifergruppen. Die konkreten Angriffe im Rahmen dieser Bedrohungen („threats“) werden von Angreifenden aufwändig vorbereitet, sind hochentwickelt („advanced“) und dauern lange an („persistent“).

3 Zur Veranschaulichung wurden diverse Screenshots aus dem Leak übersetzt.

Das BfV stellt die Auswertungsergebnisse in vier Berichten dar, die wie folgt strukturiert sind:

- Struktur und Vorgehensweise der APT-Einheiten von i-Soon (Teil 1),
- Verbindungen von i-Soon zum chinesischen Sicherheitsapparat (Teil 2),
- Konkrete Angriffsziele von i-Soon und betroffene Staaten (Teil 3),
- **i-SoonProdukte und deren Abnehmer (Teil 4, dieser Bericht).**

2. Ausgewählte Produkte und Dienstleistungen

Der i-Soon-Datenleak umfasst auch eine Liste mit Produktinformationen und von i-Soon angebotenen Dienstleistungen. Sie enthält Angaben zu

- den einzelnen Produkten und Produktversionen,
- den Verkaufseinheiten,
- Preisen und
- Kommentaren zum Produkt insgesamt (vgl. Abbildung 1).

Die angebotenen Produkte sind in drei Kategorien unterteilt: „Public Safety“, „Blockchain Security“ und „Enterprise Security“. Der Großteil der Produkte ist der Kategorie „Public Safety“ zugeordnet. Enthalten sind 22 Produkte – inklusive Preisgestaltung – die je nach Nutzungsdauer, Bestellmenge oder als individuelle Pakete bepreist werden. Mitunter werden Analysetools, Verschleierungstools[4] und

4 Verschleierungstools sollen Herkunft, Richtung und Art der Operationen verbergen und erhöhen so die Operative Sicherheit des Angreifers. Darunter fallen insbesondere Anonymisierungsnetzwerke.

Penetration-Testing-Tools[5] für unterschiedliche Betriebssysteme und Software-Hersteller, Sandbox-Systeme[6] und Produkte zur Überwachung aufgelistet.

Abbildung 1: Auszug Produktliste

Zu einigen dieser Tools werden Benutzerhandbücher oder Produktbeschreibungen angeboten. Die Kundschaft kann entweder i-Soon mit der Entwicklung eigener Produkte beauftragen oder auch Nutzungslizenzen erwerben. Die Preise bewegen sich dabei je nach Aufwand zwischen 30.000 ¥ und 800.000 ¥ (ca. 3.500 € bis ca.103.000 €).

Die nähere Betrachtung der angebotenen Produkte gibt Aufschluss über die Fähigkeiten von i-Soon aber auch über die potentielle Kundschaft, die sich für solche

5 Ein Penetrationstest beschreibt das umfangreiche Testen einzelner Computer, von Netzwerken oder Anwend ungen auf Schwachstellen. Die dafür genutzten Werkzeuge spiegeln gängige Angriffsmethoden wieder. Aus diesem Grund werden solche Tests meistens im Auftrag der zu testenden Stelle beauftragt und autorisiert.

6 Sandbox-Systeme sind isolierte (virtuelle) Maschinen, in denen potentiell unsichere Software ausgeführt werden kann, ohne Wirkung nach außen zu entfalten und Schaden anzurichten.

Produkte interessiert. Nachfolgend werden einige der Produkte im Bereich „Public Safety“ kurz dargestellt.

2.1 Integrated Combat Platform

Bei der „Integrated Combat Platform“ handelt es sich um eine Softwarelösung zur Durchführung von Cyberoperationen. Die Software beinhaltet einen abgeschotteten internen Teil zur Operationsverwaltung und einen externen Teil mit offensiven Tools (vgl. Abbildung 2 und 3). Die „Integrated Combat Platform“ ermöglicht durch ihre Prozessoptimierung, Ressourcenverteilung und Planungs- und Steuerungsmöglichkeiten, Cyberoperationen im großen Stil durchzuführen.

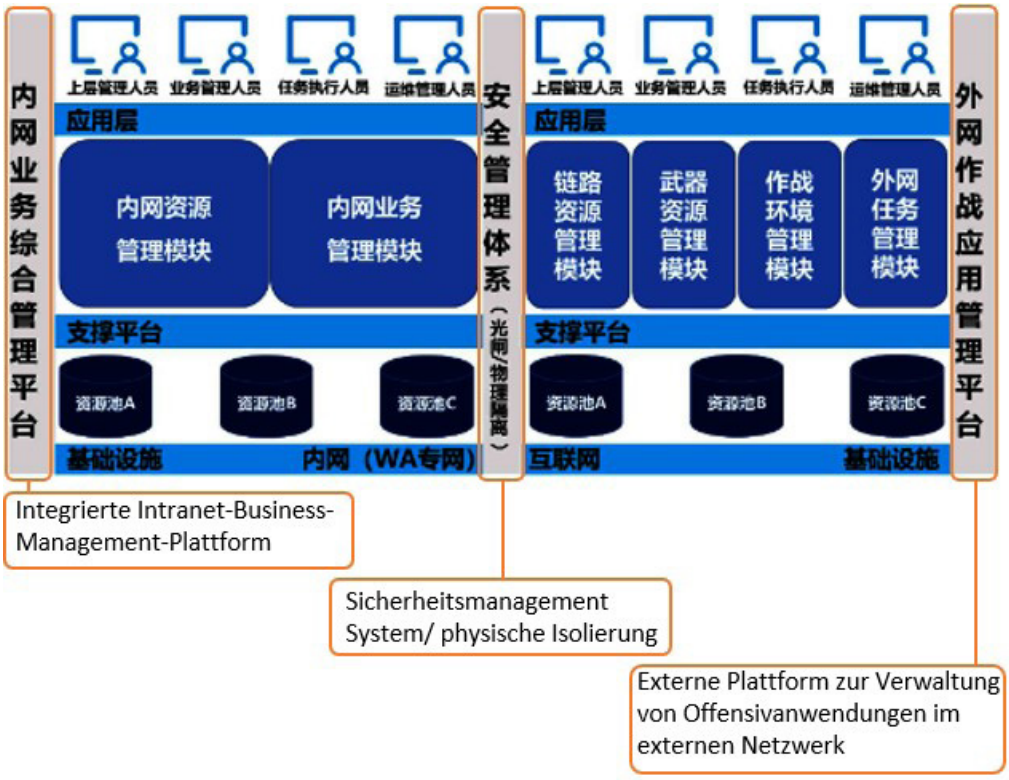

Abbildung 2: Aufbau der Integrated Combat Platform (Teil 1)

In der dazugehörigen Produktbeschreibung werden die grundlegende Systemarchitektur sowie die vielzähligen Funktionen der Software und deren Funktionsweisen beschrieben. Zu den Funktionen gehören die Nutzungsverwaltung, Wartung und Anpassung, das Bereitstellen von Testumgebungen, Funktionen zum

Management von VPS-Konten[7] und Funktionen für die Verwaltung externer Konten. Durch den modularen Aufbau können Nutzer die Anwendungen je nach Bedarf konfigurieren und für ihre Zwecke nutzen. Die Software ist dafür ausgelegt, bei Operationen den Urheber zu verschleiern. So ist auch eine Funktion integriert, die die Software nach Nutzung unwiderruflich zerstört.

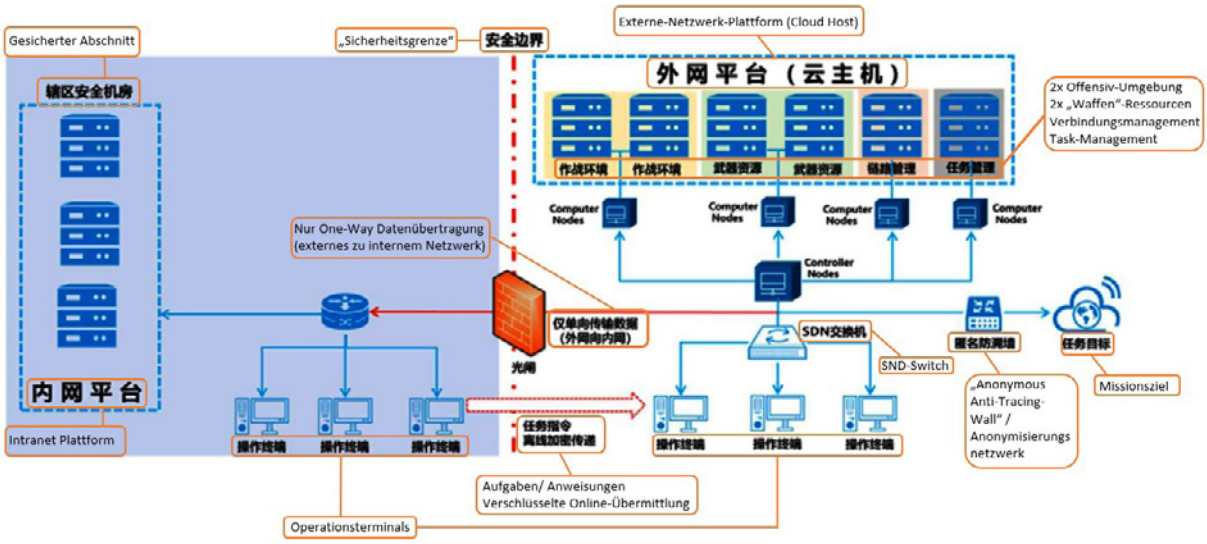

Abbildung 3: Aufbau der Integrated Combat Platform (Teil 2)

2.2 Automated Penetration Testing Platform

Bei der „Automated Penetration Testing Platform" handelt es sich um ein modular aufgebautes und dadurch vielseitiges System (Abbildung 4). Grundsätzlich ermöglicht das Produkt, die eigenen Fähigkeiten passgenau auf ein Ziel abzustimmen, wobei Penetrationstests gegen eine Vielzahl von Systemen eingesetzt werden können. Sollte während einer laufenden Cyberoperation eine bestimmte Funktion benötigt werden, kann diese bei Bedarf nachträglich hinzugefügt werden. Durch einen hohen Automatisierungsgrad sollten auch technisch weniger versierte Nutzer die Plattform bedienen können. Sehr wahrscheinlich ist das angebotene Produkt ein Dual-Use-Tool, also ein Produkt, welches zu legitimen als auch maliziösen

7 Ein virtueller privater Server (VPS) ist ein Server, der alle Software und Daten hostet, die zum Ausführen einer Anwendung oder Webseite erforderlich sind. Die Bezeichnung virtuell rührt daher, weil nur ein Teil der zugrunde liegenden physischen Ressourcen des Servers verbraucht wird.

Zwecken genutzt werden kann. Die Plattform kann dabei nahezu sicher auch für offensive Cyberoperationen genutzt werden.

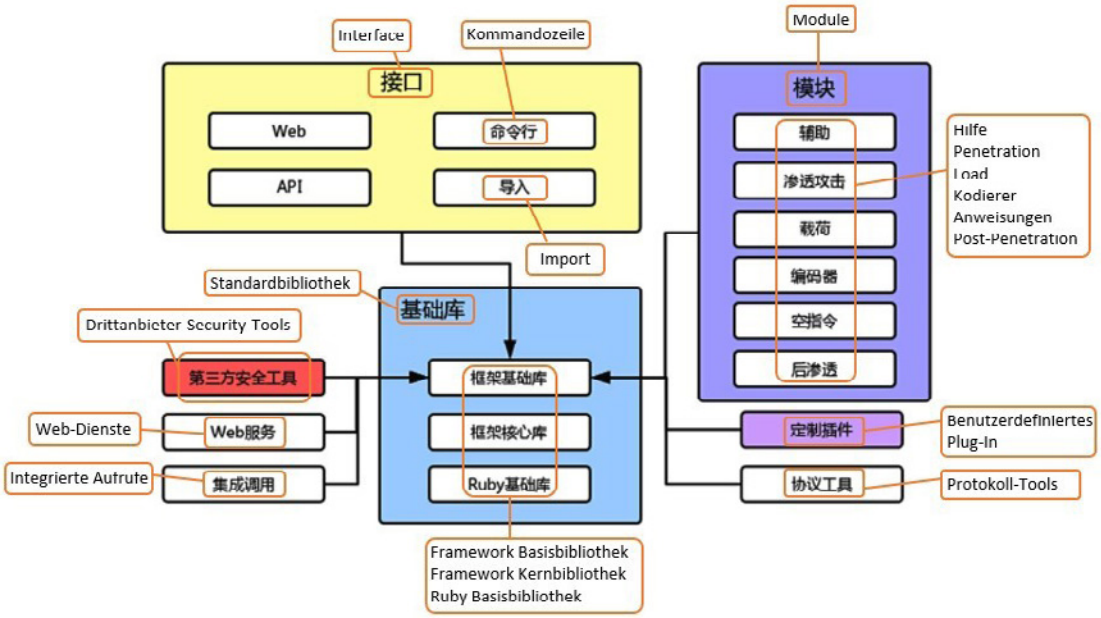

Abbildung 4: Aufbau der Automated Penetration Testing Platform

2.3 Microsoft E-Mail Encryption Platform

Die „Microsoft E-Mail Encryption Platform“ ist in der Lage, Microsoft E-Mail-Postfächer zu kompromittieren und Daten auszuleiten. Ferner soll die Software die Zwei-Faktor-Authentifizierung umgehen können und so ohne Kenntnis des Opfers Zugriffe ermöglichen (vgl. Abbildung 5).

Dabei wird ein durch die Plattform generierter Phishing-Link an ein Opfer versandt. Nachdem dieses auf den Link geklickt hat, erhält der Angreifer automatisch Zugriff auf das Microsoft Outlook-Konto der betroffenen Person. i-Soon gibt an, dass die Plattform für die Kriminalitätsbekämpfung genutzt werden soll. Grundsätzlich scheint es aber keine Nutzungseinschränkung zu geben, so dass die Plattform daher mutmaßlich auch für offensive Cyberoperationen genutzt werden kann.

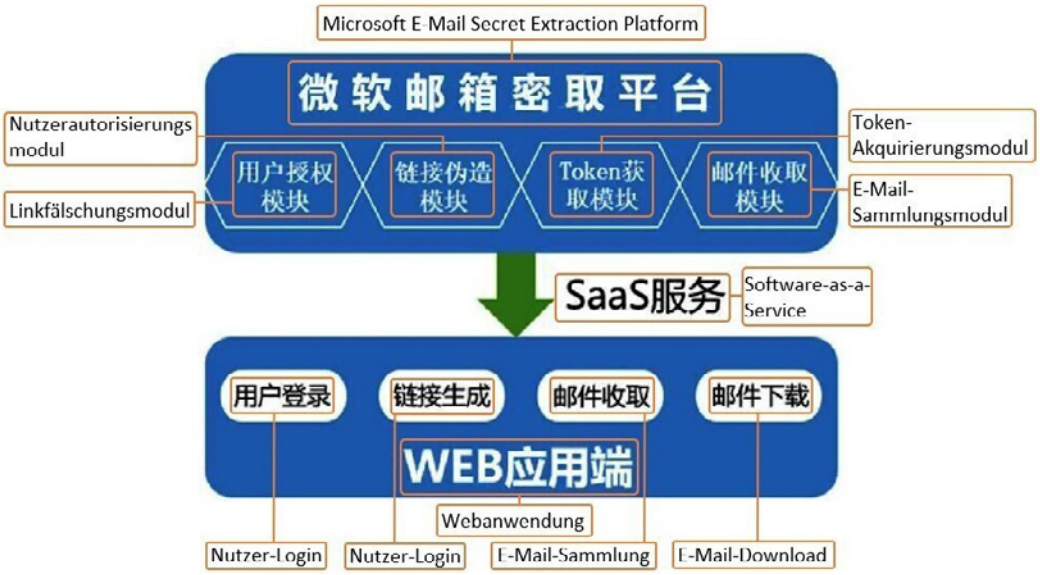

Abbildung 5: Übersicht Microsoft E-Mail Encryption Platform

2.4 E-Mail Analysis Intelligence Decision Making Platform

Bei der „E-Mail Analysis Intelligence Decision Making Platform“ handelt es sich um ein fortgeschrittenes System zum Auslesen von E-Mail-Konten und der Auswertung großer Datenmengen. Es soll in der Lage sein, E-Mail-Anhänge automatisiert auszuwerten und Beziehungsmodelle von Nutzern basierend auf ihrer E-Mail-Kommunikation zu erstellen (vgl. Abbildung 6).

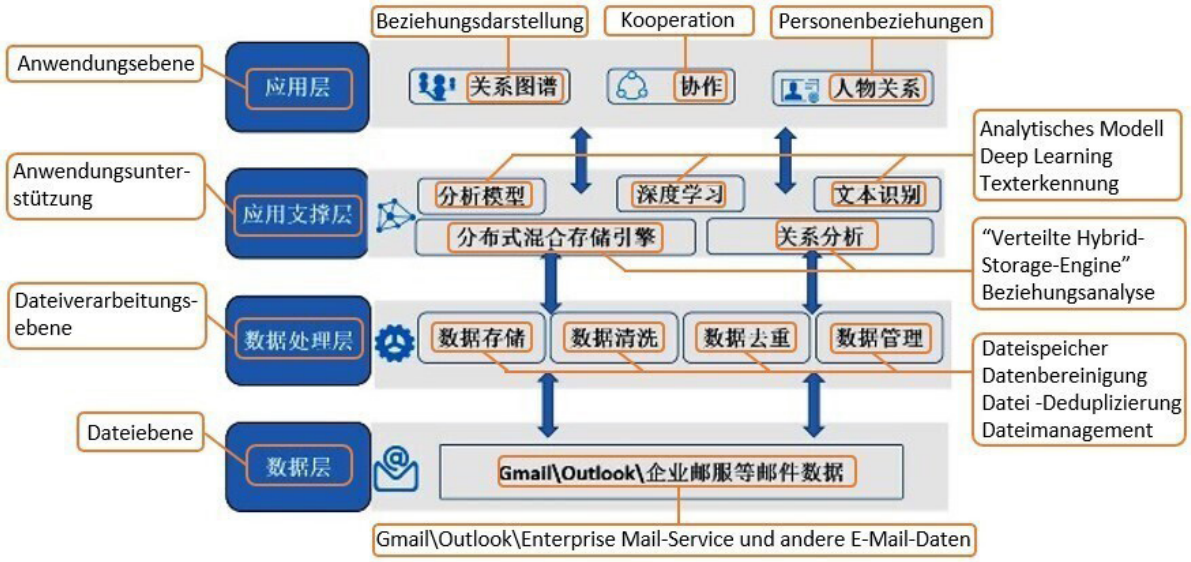

Abbildung 6: Übersicht E-Mail Analyse Produkt

2.5 Anonymous Anti-Tracing Wall

Bei der „Anonymous Anti-Tracing Wall“ handelt es sich um einen Anonymisierungs-Dienst, der zusätzlich Zugriffe auf das Darknet (Invisible Web) ermöglicht. Softwareseitig werden vier verschiedene Module bereitgestellt: eines für den Internetzugriff, eines zur Anonymisierung, eines um Verbindungsmöglichkeiten zu anderen Systemen darzustellen und eines, um auf das Darknet zugreifen zu können. Die einzelnen Module werden als Paket mit einer Nutzungszeit von mindestens einem Jahr vertrieben.

Neben dem herkömmlichen Zugriff auf das Internet (Clear Web) wird durch das Paket die Anonymisierung der eigenen Aktivitäten ähnlich des TOR-Browsers oder anderer VPN-Dienste[8] ermöglicht. Nutzer können zur Verschleierung frei aus den beiden Möglichkeiten TOR oder VPN-ähnlich wählen (vgl. Abbildung 7).

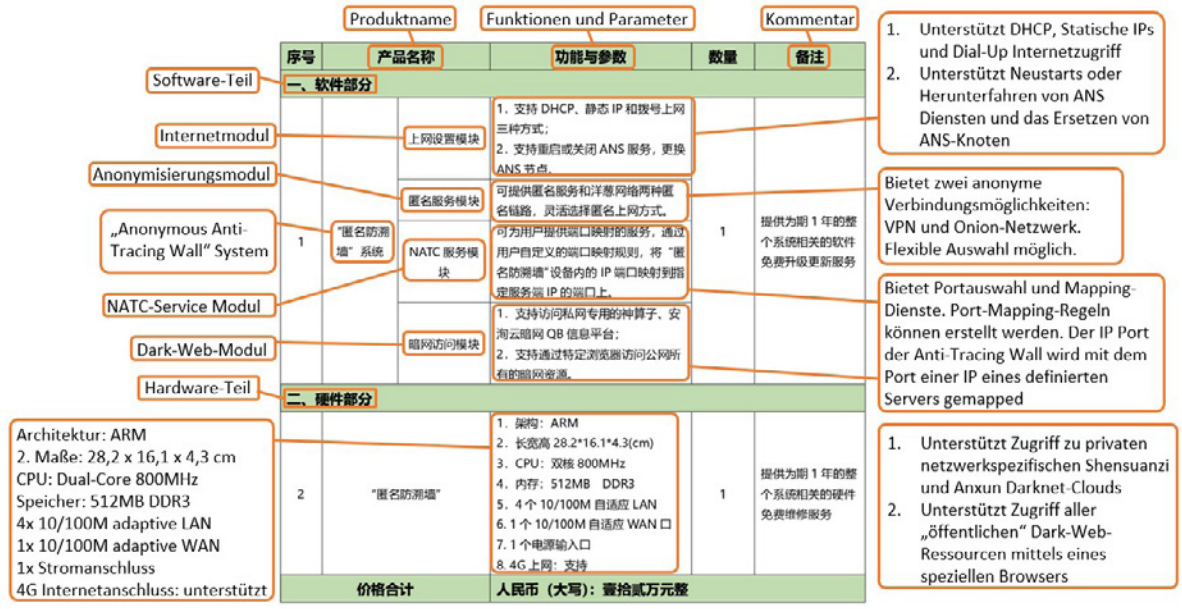

Abbildung 7: Übersicht Anti-Tracing Wall

8 TOR ist ein Netzwerk zur Anonymisierung von Verbindungsdaten, das seine Nutzer vor der Analyse des Datenverkehrs schützt. Auch Virtual Private Network-Dienste (VPN) erlauben die anonymisierte Kommunikation im Internet. Das TOR-Netzwerk leitet dabei Daten über zufällige, von Freiwilligen bereitgestellte Server, während ein VPN Daten über einen einzigen vom Nutzer ausgewählten Server leitet.

2.6 Individual (Soldier) Toolbox

Die „Individual (Soldier) Toolbox“ dient als Penetration-Testing-Lösung und wird als mobile Lösung für leistungsfähige Laptops vertrieben (Abbildung 8). Viele der Funktionen werden im Allgemeinen für Penetration-Testing genutzt, eignen sich jedoch ebenfalls für den maliziöses Einsatz. Auffällig bei diesem Produkt sind Funktionen, die dem allgemeinen Verständnis von Penetration-Testing widersprechen bzw. den hierbei üblichen Werkzeugkasten übersteigen. Dazu gehören beispielsweise die Funktion zum Abfangen von Datenpaketen und deren Modifizierung, der Einsatz von Webshells, die einen Fernzugriff ermöglichen und Funktionen zum aktiven Ausnutzen von Schwachstellen.

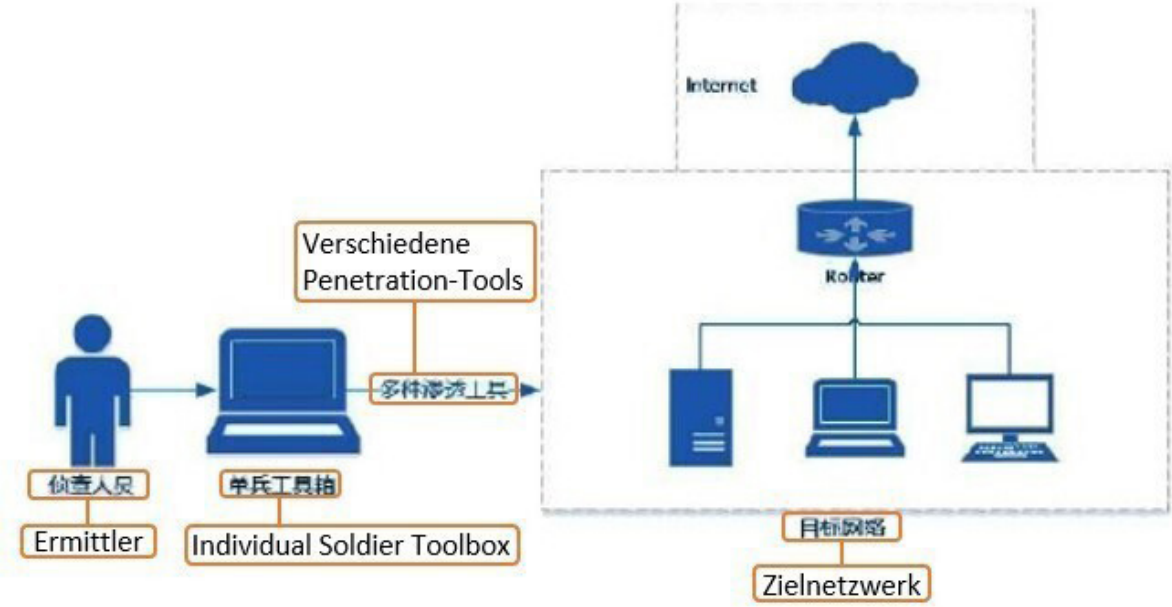

Abbildung 8: Übersicht Individual (Soldier) Toolbox

2.7 Integrated Training Platform

Unter der Bezeichnung „Integrated Training Platform“ wird ein Werkzeug zur Verarbeitung großer Datenmengen vertrieben. Mithilfe der Plattform soll es möglich sein, Daten effizient zu klassifizieren, strukturiert abzulegen und besser durchsuchbar zu machen. Nutzer können hierdurch Informationen schneller abrufen und verwerten (Abbildung 9).

Die Bezeichnung als „Training-Platform“ ist dabei irreführend: Aus den vorliegenden Informationen ist zu entnehmen, dass der Funktionsumfang die Verarbeitung großer Mengen personenbezogener Daten umfasst. Das Produkt wäre demnach für Cybersecurity-Unternehmen von Interesse, um offensive und defensive Cyberoperationen durchzuführen beziehungsweise nachzubereiten und auszuwerten.

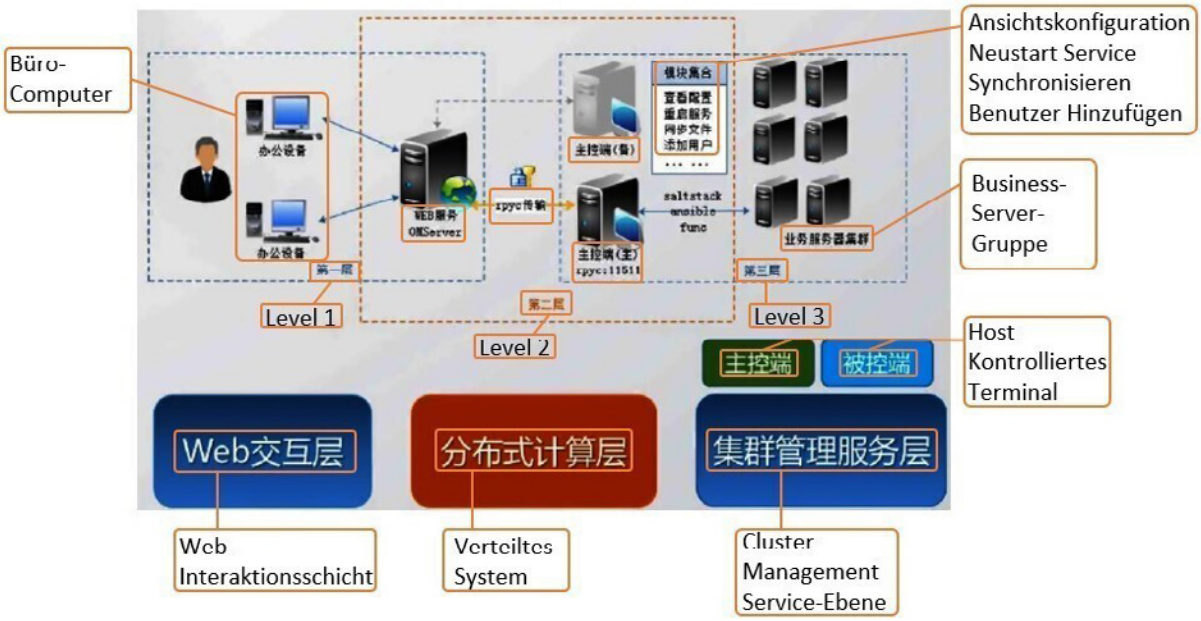

Abbildung 9: Übersicht Integrated Training Platform

3. Vertragsbücher

Die Zielgruppe der angebotenen Produkte und Dienstleistungen lässt sich anhand der im Datenleak enthaltenen Vertragsbücher von i-Soon gut nachvollziehen. Dabei teilt i-Soon seine Bedarfsträger in vier Kundentypen ein:

- Public Security / 公安 (wahrscheinlich Ministerium für Öffentliche Sicherheit[9] / 公安部, engl. „Ministry of Public Security“/ MPS),

9 Ministerium, das für die öffentliche und politische Sicherheit verantwortlich ist. Es ist die übergeordnete Behörde der Polizeien und nimmt zusätzlich Aufgaben im Bereich der Spionageabwehr wahr.

- Safety 安全 (wahrscheinlich das Ministerium für Staatssicherheit[10] 安全部, engl. „Ministry of State Security“/ MSS),
- Military (wahrscheinlich Volksbefreiungsarmee der VR China, engl. „Peoples Liberation Army“ / PLA),
- Enterprise (Privatunternehmen, die ähnlich zu i-Soon Dienstleistungen und Produkte im Cyberraum anbieten).

In den Vertragsbüchern werden zudem Vertragstitel und -partner, Endnutzer, Datum des Vertragsabschlusses, Kaufpreis sowie eine kurze Zusammenfassung der vertraglichen Dienstleistungen festgehalten. Die Informationen belegen, dass das MSS – auch unter Einbindung sogenannter contract hacker – Cyberoperationen in Übersee durchführt und hierzu mitunter Anonymisierungsnetzwerke einsetzt. Vor diesem Hintergrund erklären sich auch die aufgeführten Vertragstitel, die etwa lauten:

- **„Network Technology Service Contract“** (ein Vertrag für technische Netzwerkdienstleistungen, im Vertragsbuch als Akquise diverser E-Mail-Konten vermerkt),
- **„Technical Cooperation Agreement“** (mit „technische Kooperationsvereinbarung“ ist vermutlich ein Hacking-Auftrag gemeint),
- **„Overseas Data Inquiry“** (vermutlich Cyberoperationen in Übersee),
- **„Data Purchase Contract“** (der Ankauf spezieller Zieldaten) und
- **„Anti-Tracing Sales Contract“** (hier werden Anonymisierungsnetzwerke zur Verschleierung von Cyberoperationen angeboten).

4. Breites Arsenal an Angriffstools und Dienstleistungen im Cyberraum

Die im i-Soon-Datenleak enthaltenen Produktlisten und Produkthandbücher zeigen das weitreichende Arsenal potenter Cybertools von i-Soon. Die Schwerpunktsetzung im Bereich der öffentlichen Sicherheit („public safety“) legt nahe, dass die

10 Ziviler Nachrichtendienst und Geheimpolizei. Zuständig für Auslandsspionage, Spionageabwehr und politische Sicherhei

Angebote von i-Soon sich an Sicherheitsbehörden richten. Dabei wird deutlich, dass um wettbewerbsfähig zu sein und bei der Vergabe staatlicher Aufträge berücksichtigt zu werden, Unternehmen wie i-Soon bemüht sind, ihre Produkte stets zu verbessern und Preise attraktiv zu gestalten. Profiteure sind potentielle Auftraggeber wie staatliche Stellen, die für ihre Bedürfnisse von den zahlreichen miteinander konkurrierenden Unternehmen auf maßgeschneiderte Produkte zum Bestpreis zurückgreifen können.

Die Analyse der Produktverzeichnisse zeigt zudem, dass einige von i-Soons-Hacking-Tools modular konzipiert sind. Sie können variabel miteinander kombiniert werden und ermöglichen somit ein effizientes Vorgehen hinsichtlich ausgewählter Zielobjekte und gewünschten Zielsetzungen. Darüber hinaus sind sie so konzipiert, dass selbst ungeübte Anwender sie bedienen können. Die niederschwellige Anwendung wird durch einfache Benutzeroberflächen erleichtert.

Die Analyse der geleakten Produkthandbücher und verfügbaren Hacking-Werkzeuge offenbart aber auch die Gefahr, die von den i-Soon-Produkten ausgeht. Allein die durch den Leak bekannt gewordene Zahl betroffener Länder und Stellen[11] zeigt, dass diese Tools bereits für weltweite Kampagnen erfolgreich eingesetzt werden.

Die Erkenntnisse aus dem i-Soon-Leak verdeutlichen, dass eine Industrialisierung von Cyberspionage und des chinesischen Cyber-Ökosystems bereits weitreichend stattgefunden hat. Es hat sich ein Markt entwickelt mit vielen Anbietern, die einfach zu bedienende und effiziente Angriffstools entwickeln und ihre Dienstleistungen im Cyberraum anbieten. Dies führt zu einer fortlaufenden Innovation und einer stetigen Professionalisierung des chinesischen Cyber-Marktes.

In den weiteren CYBER INSIGHT-Ausgaben zum i-Soon-Datenleak geht das BfV näher auf die Struktur und Vorgehensweise der APTEinheiten von i-Soon ein (Teil 1), untersucht die Verbindungen zum chinesischen Sicherheitsapparat (Teil 2) und thematisiert die konkreten Angriffsziele und betroffene Staaten von i-Soon (Teil 3).

11 Vgl. „Die i Soon-Leaks, Teil 3: Konkrete Angriffsziele von i Soon und betroffene Staaten“

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Abteilung 4
Merianstraße 100
50765 Köln
poststelle@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0) 228/99 792-0
Fax: +49 (0) 228/99 792-2600

Bildnachweis
Titelbild: BfV, KI-erzeugt

Stand
Juli 2024