Köln, 1. August 2024

Bundesamt für Verfassungsschutz

BfV CYBER INSIGHT

Die i-Soon-Leaks: Industrialisierung von Cyberspionage

Teil 1: Struktur und Vorgehensweise der APT-Einheiten von i-Soon

Die i Soon-Leaks: Industrialisierung von Cyberspionage

Teil 1: Struktur und Vorgehensweise der APT-Einheiten von i Soon

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 Cy-berangreifergruppen. 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, dieser Bericht),**
- Verbindungen von i-Soon zum chinesischen Sicherheitsapparat (Teil 2),
- Konkrete Angriffsziele von i-Soon und betroffene Staaten (Teil 3),
- i-Soon-Produkte und deren Abnehmer (Teil 4).

2. Das Unternehmen

Medienberichten zufolge wurde i-Soon 2010 gegründet. Das Unternehmen hat seinen Hauptsitz in Shanghai. Zudem soll es Büros in 32 weiteren Provinzen, Städten und Autonomiegebieten in China unterhalten.[4] Der Firmenbeschreibung auf seiner Homepage zufolge ist i-Soon als Cyber-Sicherheitsfirma tätig, die u.a. für die chinesische Regierung Hackerangriffe abwehrt und für die Sicherheit von Kundennetzwerken verantwortlich ist. Der Firmengründer soll ein ehemaliger Angehöriger des Green Corps sein – eine Gruppe aus Chinas „patriotischer“ Hacking-Szene. Ihre Angehörigen haben über die Jahre ein umfassendes Netzwerk von Cybersicherheitsfirmen aufgebaut, die auch im Auftrag chinesischer Sicherheitsdienste und Regierungsinstitutionen arbeiten.

4 Vgl. „Ist das Chinas Snowden-Moment?“ vom 23.02.2024, in: www .spiegel.de; abgerufen am 28.06.2024.

3. Struktur und Vorgehensweise

Die auf GitHub Anfang 2024 hochgeladenen Datensätze enthalten u.a. eine Präsentation zu den Fähigkeiten und angebotenen Dienstleistungen von i-Soon. So wird ein seltener Einblick in die Organisation selbst und das Verhältnis zu den Kunden des Unternehmens ermöglicht. Die Präsentation bewirbt u.a. firmeneigene APT-Einheiten, die für ihre Kooperationspartner gleichzeitig mehrere Angriffskampagnen im Ausland durchführen können. Demnach besteht das Team aus insgesamt mehr als 70 Personen, die in drei Einsatzbereichen organisiert sind: einem „Security Research Team“, drei „Penetration Teams“ und einem „Basic Support Team“ (vgl. Abbildung 1).

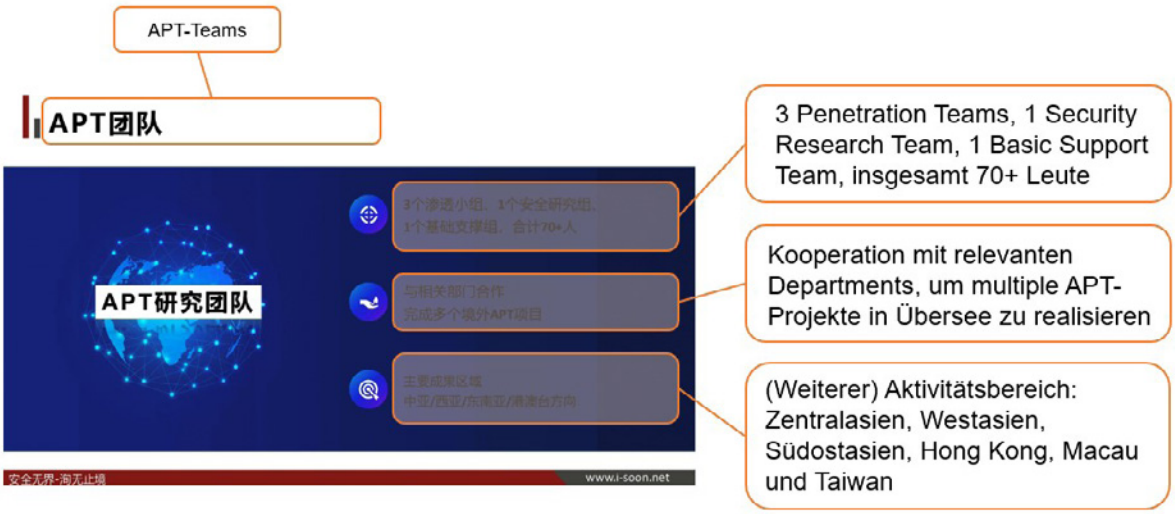

Abbildung 1: Aufbau der i-Soon-Teams

Die gewählten Begrifflichkeiten deuten auf einen hoch-spezialisierten und professionellen Ablauf zur Durchführung von Cyberangriffen hin. Das „Security Research Team“ ist vermutlich für die Auskundschaftung von Zielen im Vorfeld verantwortlich. Im Anschluss können die drei „Penetration Teams“ zielgerichtet agieren. Diese Teams dürften bereitstehen, um in die Sicherheitssysteme ausgewählter Zielobjekte einzudringen und dort die vorher klar definierten Ziele zu erreichen bzw. erwünschten Informationen abzuziehen. Das „Basic Support Team“ befasst sich mutmaßlich mit allen weiteren im Einsatzverlauf auftretenden technischen Unterstützungsfragen.

Neben organisatorischen Abgrenzungen unterteilt i-Soon gemäß Eigendarstellung die Fähigkeiten seiner APT-Einheiten in drei Dienstleistungsbereiche:

- „Target Penetration Services“,
- „Battle Support Services“ und
- „Intelligence Services“.

Als mögliche Ziele der „Target Penetration Services“ werden exemplarisch die Netzwerke von Regierungsorganisationen und -behörden inklusive deren Intranet aufgeführt. Hinzu kommt die Beschaffung von Datei-Server-Berechtigungen und PC-Berechtigungen von Regierungspersonal in Übersee (vgl. Abbildung 2). Neben dem Regierungssektor bewirbt i-Soon auch das „Bearbeiten“ der (zum Teil zur Kritischen Infrastruktur zählenden) Bereiche Telekommunikation, Energienetzwerke, Transportnetzwerke und medizinische Netzwerke.

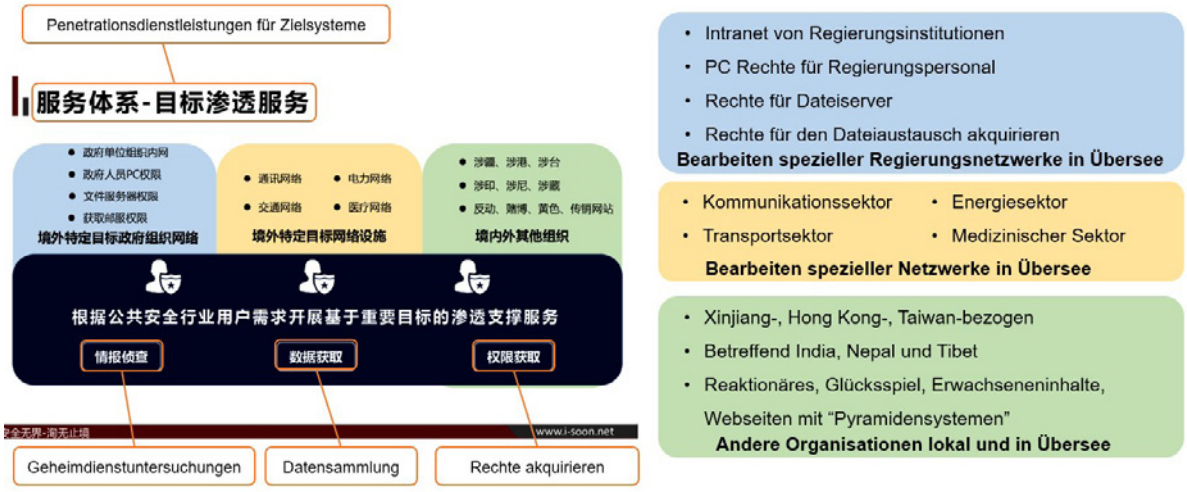

Abbildung 2: Dienstleistungsbereiche von i-Soon

Die angebotenen Leistungen decken sich dabei mit den mutmaßlichen Interessen staatlich gesteuerter chinesischer Cyberakteure. Es geht um den Zugang zu Informationen über außen-, sicherheits- und wirtschaftspolitische Absichten anderer Staaten durch das Eindringen in Netzwerke von deren Regierungseinrichtungen.

Über den Überblick zu den Dienstleistungen hinaus bieten die veröffentlichten Daten auch eine detaillierte Einsicht, wie i-Soon unternehmensintern Hacking-Kampagnen vorbereitet (vgl. Abbildung 3):

Abbildung 3: Ablauf einer i-Soon Hacking-Kampagne – technischer Prozess

- Im ersten Schritt werden anhand der Kundenvorgaben Angriffsziele ausgewählt und die mit den Angriffen verfolgten Zwecke definiert. Sofern es sich um gut gesicherte Hochwertziele handelt, wird i-Soon vom Kunden ggf. notwendiges Insiderwissen zur Verfügung gestellt, beispielsweise zu IT-Sicherheitsstandards des Ziels. Auf Basis der dem Unternehmen vorliegenden Informationen und Zielvorgaben erstellt i-Soon sodann einen vorläufigen Einsatzplan.
- Im zweiten Schritt werden bedarfsorientiert die APT-Teams zusammengestellt und ein zu nutzendes Toolset ausgewählt oder speziell entwickelt. Dieses variable und bedarfsorientierte Vorgehen lässt darauf schließen, dass das Unternehmen in der Lage sein dürfte, unterschiedliche Techniken, Taktiken und Prozeduren (TTPs) sowie Modi Operandi zu entwickeln und zu kombinieren, um so eine maximale Effizienz anzustreben.

- Im dritten Schritt erfolgt die Aktivität am Ziel selbst: Die zuvor festgelegten Daten werden akquiriert sowie ggf. weitere nützliche Hinweise und Informationen ermittelt.
- Im vierten Schritt erfolgt ein Backend-Support für den Kunden. Dieser kann eine weitere technische Unterstützung sowie anderweitige, nicht näher definierte Unterstützung im Zuge der weiteren Fallbearbeitung umfassen.

Das in der i-Soon-Präsentation geschilderte Vorgehen wird durch die im Datenleak enthaltenen Listen zu Produkten und Dienstleistungen, zu Vertragsbüchern sowie Cyberoperationen und Zielentitäten bestätigt. Diese Listen umfassen u.a. kundenseitige Zielvorgaben (vgl. Abbildung 4), die durch i-Soon angebotenen Toolsets, den Bearbeitungsstand der jeweiligen Cyberoperation sowie Angaben zur Zielerreichung durch das Unternehmen.

Abbildung 4: Beispiel Vertragsbestimmungen

4. i-Soon und das chinesische Cyber-Ökosystem

Weitere Erkenntnisse zur Arbeitsweise des Cybersecurity-Unternehmens konnte das BfV aus der Auswertung der im Datenleak enthaltenen Textdateien gewinnen. Die Chat-Protokolle bieten einen Einblick in die geschäftsorientierte Teilhabe von i-Soon am hochprofessionellen chinesischen Cyber-Ökosystem[5]. Aus ihnen geht

5 Der Begriff des Cyber-Ökosystems beschreibt die Involvierung verschiedener Sektoren in staatlich gestützte Cyberspionage. Betroffen sind unter anderem Entitäten, die in Bildung und Forschung sowie Dienstleistung und Produktentwicklung involviert sind und den chinesischen Diensten ihr jeweiliges Portfolio zur Verfügung stellen. Diese Kooperation kann entweder auf freiwilliger Basis erfolgen oder gemäß der gesetzlichen Grundlagen Chinas durchgesetzt werden.

hervor, dass das Unternehmen nicht nur im direkten Auftrag seiner Kooperationspartner tätig wird. Vielmehr führt i-Soon entweder eigeninitiativ Cyberoperationen durch oder beschafft zumindest innerhalb einer laufenden Cyberoperation mehr Daten als vertraglich vereinbart – vermutlich, um den erlangten Überschuss später gewinnbringend an andere Kunden zu veräußern. Die Protokolle enthalten beispielsweise eine Unterhaltung über durch i-Soon generierte Informationen aus dem Bereich des damaligen NATO-Generalsekretärs. Ein Entwurf sei Kunden gezeigt und die Daten zum Kauf angeboten worden, diese hätten jedoch Desinteresse signalisiert (vgl. Abbildung 5).

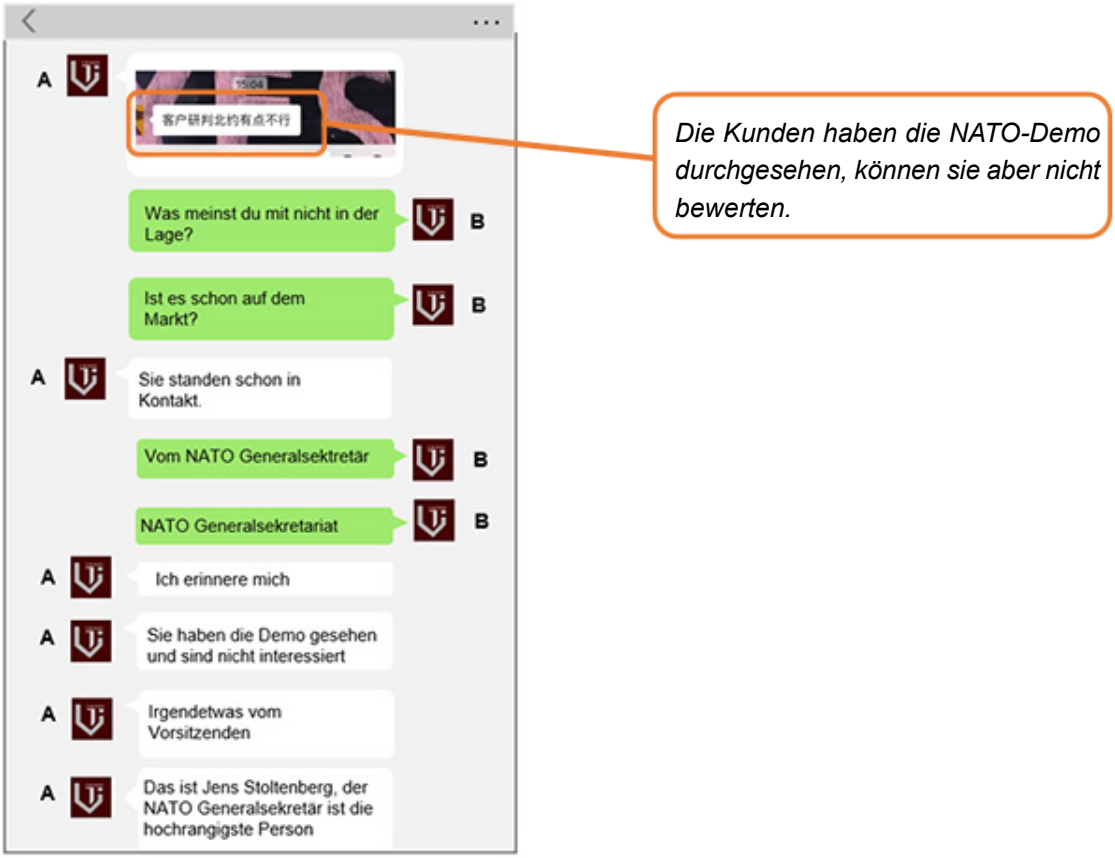

Abbildung 5: Chat zu angeblich erbeuteten NATO-Daten

Ferner scheint i-Soon unternehmensseitig Zugangsdaten auf dem Schwarzmarkt zu kaufen, mutmaßlich um damit Kundenaufträge ausführen zu können. Ein konkretes Beispiel dafür liefert eine Diskussion über gestiegene Kosten für Zugangsdaten zu Systemen des amerikanischen Federal Bureau of Investigation (FBI) (vgl. Abbildung 6).

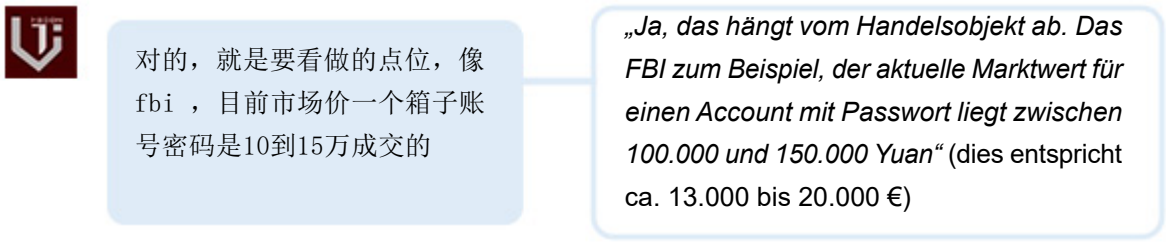

Abbildung 6: Chat zu FBI-Zugangsdaten

Insgesamt zeigt sich auf Basis der ausgewerteten Chat-Protokolle ein Bild eines hart umkämpften Cyber-Marktes: Die Löhne der Beschäftigten sind gering und stagnieren, der Wettbewerb mit Konkurrenten wird als intensiv beschrieben und für erbeutete Dokumente werden zum Teil anscheinend keine Abnehmer gefunden. Es wird um Personal gestritten und mittels Kooperationen mit lokalen Universitäten sowie mit Auftritten und Beteiligungen an chinesischen Cybersecurity-Wettbewerben versucht das Unternehmen, talentierten Nachwuchs zu rekrutieren.

5. Einblick in die chinesische Cyberlandschaft

In ihrer Gesamtheit geben die veröffentlichten Datensätze einen einzigartigen Einblick in die komplexe Struktur und das Ausmaß des chinesischen Cyber-Ökosystems:

i-Soon ist zwar nur ein einziges mittelständisches Unternehmen innerhalb eines in China florierenden und etablierten Wirtschaftszweigs, aber dennoch in der Lage, mit seinen APT-Einheiten zahlreiche Angriffsoperationen gleichzeitig durchzuführen. Insofern lässt sich erahnen, auf welchem technischen Niveau und in welchem Umfang diese Branche in China insgesamt agiert. Derartige IT-Firmen unterhalten zum Teil zahlreiche weitere Subunternehmen, die sich ihrerseits wieder in einzelnen Tätigkeitsfeldern spezialisieren. Dazu gehören Bereiche wie Software- und Hardware-Entwicklung, Infrastrukturbereitstellung, Malware-Entwicklung und APT-Services.

Zugleich lassen die durch das Leak eröffneten Einblicke auch das Bild eines unreglementierten Marktes aufscheinen, in dem einzelne Akteure offenbar unkontrolliert agieren können. Eine erste regulatorische Maßnahme der chinesischen

Regierung als Reaktion auf das Datenleak war die Erweiterung der Gesetzeslage, nun sind auch Daten im Kontext staatlicher Aufträge als Staatsgeheimnis einzustufen.

In den weiteren CYBER INSIGHT-Ausgaben zum i-Soon-Datenleak geht das BfV konkreter auf die Verbindungen zum chinesischen Sicherheitsapparat (Teil 2), bekannt gewordenen Angriffszielen (Teil 3) sowie Kunden und Produkten von i-Soon (Teil 4) ein.

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