Köln, 8. August 2024

Bundesamt für Verfassungsschutz

BfV CYBER INSIGHT

Die i-Soon-Leaks: Industrialisierung von Cyberspionage

Teil 2: Verbindungen von i-Soon zum chinesischen Sicherheitsapparat

Die i-Soon-Leaks: Industrialisierung von Cyberspionage

Teil 2: Verbindungen von i-Soon zum chinesischen Sicherheitsapparat

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 Angrei-fenden 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, dieser Bericht),**
- Konkrete Angriffsziele von i-Soon und betroffene Staaten (Teil 3),
- i-Soon-Produkte und deren Abnehmer (Teil 4).

2. i-Soons Einbindung in das nationale Schwachstellen-Mining der Volksrepublik China

Die veröffentlichten Dateien enthalten u.a. eine firmeneigene Präsentation zu Fähigkeiten und Dienstleistungen von i-Soon, aus der sich Bezüge des Unternehmens zum chinesischen Staatsapparat ergeben. So wirbt i-Soon beispielsweise damit, dass das Unternehmen am nationalen Schwachstellen-Mining[4] teilnimmt und sich in diesem Zusammenhang auch an der „China National Vulnerability Database“ (CNNVD) beteiligt.

China hatte im Juli 2021 verbindliche Regularien und Strukturen entwickelt, um das Schwachstellen-Mining zu institutionalisieren. Dadurch wird sichergestellt, dass staatliche Stellen an dieser Form der Informationsgewinnung weitreichend beteiligt werden. Alle in China tätigen Unternehmen müssen gefundene Schwachstellen innerhalb von 48 Stunden über festgelegte Meldewege mitteilen. Die Informationen werden in diversen Datenbanken zusammengeführt, auf die alle relevanten Akteure des chinesischen Sicherheitsapparats Zugriff haben (vgl. Abbildung 1).

4 Schwachstellen-Mining bezeichnet das (gezielte) Sammeln und Bereithalten von Schwachstellen in Software und vergleichbaren Produkten.

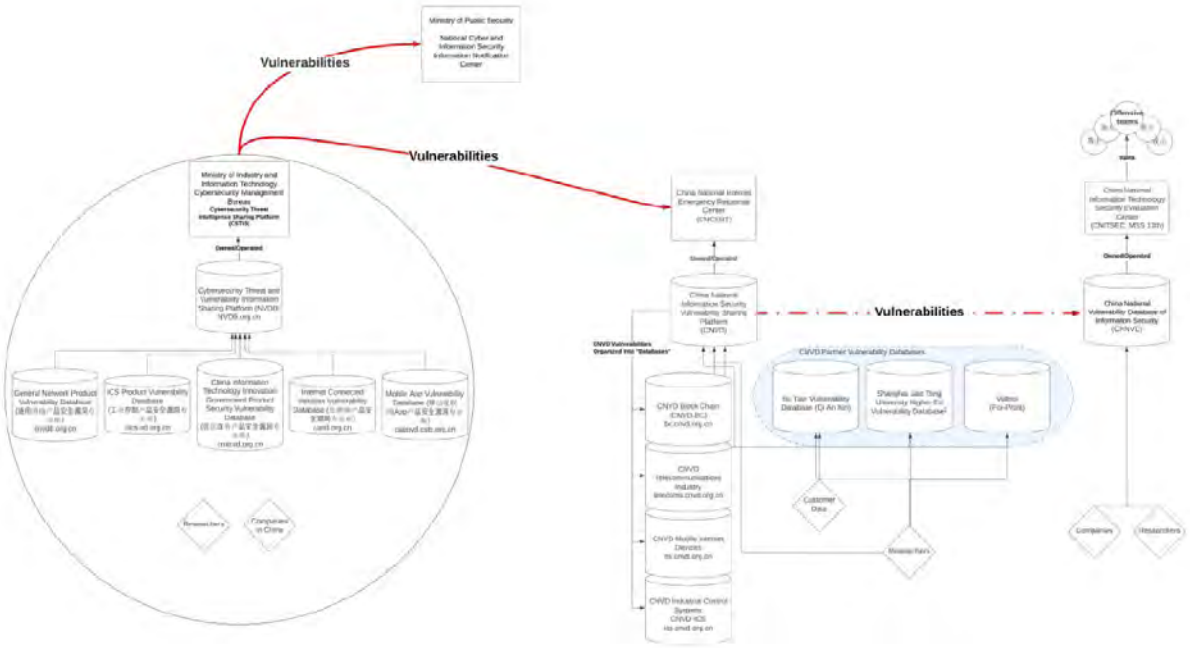

Abbildung 1: Schwachstellen-Mining[5]

Es ist untersagt, die sicherheitsrelevanten Informationen zu Schwachstellen anderweitig zu veröffentlichen. Die Datenbank CNNVD wird vom staatlichen „China National Information Technology Security Evaluation Center“ (CNITSEC)[6] betrieben und die Informationen (offensiven) Cyberakteuren zur Verfügung gestellt.

Um technischer Unterstützer des CNNVD zu werden, müssen sich Unternehmen wie i-Soon zuvor in einem Bewerbungsverfahren qualifizieren. Abhängig von der Größe und den Fähigkeiten eines Bewerbers erfolgt eine Zuordnung zu einem von drei Leveln (vgl. Abbildung 2).

5 Darstellung aus Atlantic Council (2023): Sleight of hand: How China weaponizes software vulnerabilities (Quelle: CNNVD Handbook).

6 Das China Information Technical Security Evaluation Center (CNITSEC) wurde im Jahr 1997 gegründet und versteht sich laut eigener Angaben als ein wesentlicher Bestandteil des Systems chinesischer Informationssi-cherheit. Im Speziellen sind dies die Analyse von Softwareschwachstellen und die Auswertung, Beurteilung und Zertifizierung von Softwarecode, Produkten mit Bezug zu IT-Sicherheit und Akteuren im chinesischen Cyberraum.

CNNVD Initial Application Requirements for Businesses Applying to be Technical Support Units

Category	Level 1	Level 2	Level 3
Responsbility for Security Services, Vulnerability Capability Team	The company's main business segment is information/cyber security. The business also maintains software vulnerability discovery and analysis capabilities, as well as incident response capabilities.		
	The vulnerability analysis and discovery team exceeds 20 people. The team's work is prolific.	The vulnerability analysis and discovery team exceeds 10 people. The team's work is good.	The vulnerability analysis and discovery team exceeds 5 people. The team's work is acceptable.
Technical Capabilities	The business has scientific research, engineering capabilities, and services related to cybersecurity.		
Submission of Novel Vulnerabilities	The company submits at least 20 "common" (通用型) novel vulnerabilities, from which at least 3 are considered "critical risk."	The company submits at least 15 "common" (通用型) novel vulnerabilities, from which at least 1 is considered "critical risk."	The company submits at least 3 "common" (通用型) novel vulnerabilities.
Vulnerability Early Warning Support	The business provides no fewer than 5 *critical* alerts.	The business provides no fewer than 5 alerts.	The business provides no fewer than 3 alerts.

Abbildung 2: Bewertungskriterien für Unternehmen zur Aufnahme in das CNNVD[7]

Die Partnerschafts-Level unterscheiden sich anhand der Menge und der Qualität der zu übermittelnden Schwachstellen, wobei Level 1 die Premium-Stufe darstellt. Hat sich ein Unternehmen nach den genannten Kriterien erfolgreich beworben, muss es jährliche Folgekriterien erfüllen (vgl. Abbildung 3).

Gemäß Eigendarstellung in seiner Präsentation ist i-Soon als „Tier-3“ Partner vermerkt und muss somit jährlich als Firma auf Level 3 mindestens fünf neue „gewöhnliche“ (also keine kritischen) Schwachstellen zuliefern sowie die anderen Voraussetzungen erfüllen. Dazu gehören Antworten auf Anfragen der CNNVD an das Unternehmen, denen die „Technical Support Units“ des jeweils angefragten Unternehmens Folge zu leisten haben. Entsprechende Ersuchen umfassen die gesamte Bandbreite von der Evaluation von Schwachstellen und ihrer Bewertung,

7 Darstellung aus Atlantic Council (2023): Sleight of hand: How China weaponizes software vulnerabilities (Quelle: CNNVD Handbook).

über technische Seminare und Datenanalysen bis hin zu spezieller, eventbasierter Unterstützung im Kontext der Schwachstellenausnutzung.[8]

CNNVD Annual Requirements for Technical Support Units

Category	Level 1	Level 2	Level 3
Data Coordination	Information submitted to the annual CNNVD Work Report is accurate and complete.		
Business Coordination	Coordination with the CNNVD is smooth and the business's attitude is energetic. There has never been an instance when the business point of contact is inaccessible or when an email has gone unanswered for too long.		
Annual Submission of Novel Vulnerabilities	The company submits at least 35 "common" (通用型) novel vulnerabilities, from which at least 5 are considered "critical risk."	The company submits at least 25 "common" (通用型) novel vulnerabilities, from which at least 1 is considered "critical risk."	The company submits at least 5 "common" (通用型) novel vulnerabilities.
Annual Vulnerability Early Warning Support	The business provides new fewer than 10 *critical* alerts.	The business provides no fewer than 10 alerts.	The business provides no fewer than 5 alerts.
Other Support	Enthusiatically respond to CNNVD requests related to vulnerability technology evaluation and judgement, technical seminars, data anaylsis support, and special event-based vulnerability support.		

Abbildung 3: Jährliche Anforderungen an Unternehmen des CNNVD[9]

3. i-Soons Ausbildungsinstitut und Zertifizierungen

Das Unternehmen i-Soon stellt Dienstleistungen für Cyberoperationen bereit und bildet mit dem Anxun College zudem Personen aus, damit diese befähigt werden, Cyberangriffe durchzuführen. Aus den geleakten Materialien geht hervor, dass jährlich mehr als 3.000 Studierende an dieser Fortbildungseinrichtung ausgebildet werden. Zu den Teilnehmerinnen und Teilnehmern gehören unter anderem

8 Vgl. Atlantic Council: „Sleight of hand: How China weaponizes software vulnerabilities“, Washington 2023, in: www. atlanticcouncil.org; abgerufen am 08.07.2024.

9 Darstellung aus Atlantic Council (2023): Sleight of hand: How China weaponizes software vulnerabilities (Quelle: CNNVD Handbook).

Studentinnen und Studenten an anderen Einrichtungen, Angehörige anderer Unternehmen sowie von staatlichen Einrichtungen oder Einrichtungen der öffentlichen Sicherheit. Das College wurde im Zuge der staatlichen Forderung gegründet, die Fähigkeiten im Bereich der Cybersicherheit zu verbessern. Zum Unterrichtsprogram gehören Offline-Material zum Selbststudium, Remote-Unterricht, personalisiertes Unterrichten sowie die Teilnahme an Wettbewerben. Diese Wettbewerbe der Fortbildungseinrichtung stellen für i-Soon eine wichtige Quelle für die Nachwuchsgewinnung dar. Zudem geht aus den Daten hervor, dass das Unternehmen bei Wettbewerben scoutet, um dort künftige Mitarbeiterinnen und Mitarbeiter auszukundschaften und zu gewinnen.

Darüber hinaus wirbt i-Soon in seiner Firmenpräsentation mit zahlreichen Zertifizierungen (vgl. Abbildung 4).

Abbildung 4: von i-Soon angegebene Zertifizierungen

- Level-2 Zertifikat für Verschlusssachen für Waffen und Ausrüstung (i.S.v. digitalen Diensten/Produkten) sowie Forschungs- und Entwicklungseinheiten,
- Level-1 Qualifizierung für Nationale Informationssicherheitsdienste,
- Nationale Qualifizierung für Dienste in der Informationssicherheit mit der Befähigung zur Bearbeitung von Notfällen in der Informationssicherheit auf dem Level-3,
- Level-3 Zertifizierung für Nationale Informationssicherheitsdienste durch das CNITSEC,
- technische Partnerschaft mit der CNNVD Level-3,

- Registrierung als professionelles Ausbildungszentrum für Informationssicherheit für Angriff und Verteidigung.

Diese Zertifizierungen erlauben die Ausführung eingestufter Aufträge bzw. Kooperationsformate wie etwa die Bereitstellung bestimmter Softwareprodukte oder die Durchführung spezieller Hacking-Operationen und bilden somit die (zertifizierte) Basis für die Zusammenarbeit mit staatlichen Stellen.

4. Personelle Verbindungen zum chinesischen Staat und in die nationale Hackingszene

Eine geleakte Liste von „Mitarbeitern für vertrauliche Inhalte“ weist zudem auf Verbindungen des Unternehmens i-Soon zum chinesischen Staatsapparat hin (vgl. Abbildung 5). Die Aufstellung bietet neben Namen auch Einblicke in die Aufteilung der einzelnen Arbeitsbereiche des Unternehmens. Mit vertraulichen Informationen ist i-Soon demnach in folgenden Unternehmensbereichen befasst:

- Information Management,
- Sales und Pre-Sales,
- Technical Services,
- Safety Evaluation,
- Administration,
- Confidentiality Office,
- Finance,
- Security Division,
- Human Resources,
- Software Development und
- Operation and Maintenance.

List of confidential personnel

Name	gender	nationality	Birthplace	Confidential positions	Position	Classification level	political status	major
[redacted]	male	Chinese	Yancheng	Legal Person/General Manager/Team Leader	Legal Person/General Manager/Team Leader	important	the masses	Electronic information engineering
[redacted]	male	Chinese	Huangyan, Zhejiang	Confidentiality Director Fu Team Leadez	Confidentiality Director Fu Team Leader	important	the masses	Calculation software technology and application
[redacted]	male	Chinese	Guang'an, Sichuan	Classified Computer Security Auditor	Head of Information Management Department	important	member	Calculation technology
[redacted]	male	Chinese	Ji'an, Jiangxi	Pre-sales engineer	Pre-sales engineer	generally	the masses	Logistics management
[redacted]	male	Chinese	Xingtai, Hebei	Director of Technical Services Department	Director of Technical Services Department and Manager of Government and Enterprise Division	generally	the masses	Calculation technology
[redacted]	male	Chinese	Dazhou, Sichuan	Safety evaluation engineer	Safety evaluation engineer	generally	party member	network engineering
[redacted]	female	Chinese	Zigong, Sichuan	Director of Confidentiality Office	Administration Manager and Director of the Confidentiality Office	important	the masses	international trade
[redacted]	female	Chinese	Chongqing Rongchang	Sales Assistant	Sales Assistant	important	member	English
[redacted]	female	Chinese	Chengdu, Sichuan	finance professional	finance professional	generally	the masses	Accounting
[redacted]	male	Chinese	Chengdu, Sichuan	Security Division Director	Security Division Director	generally	the masses	computer information management
[redacted]	female	Chinese	Chengdu, Sichuan	Human Resources Manager	human resources manager	generally	party member	e-commerce
[redacted]	female	Chinese	Chengdu, Sichuan	Confidentiality Administrator	Confidentiality Administrator	important	the masses	Tourism management
[redacted]	male	Chinese	Mianyang, Sichuan	Software Development Manager	Software Development Manager	important	member	/
[redacted]	male	Chinese	Chengdu, Sichuan	Software Development Engineer	Software Development Engineer	generally	the masses	Multimedia design and production
[redacted]	male	Chinese	Neijiang, Sichuan	Classified Computer Security Administrator	Operation and Maintenance Engineer	important	member	Mechanical equipment Co., Ltd., manufacturing and automation

Abbildung 5: Liste des Personals für vertrauliche Inhalte[10]

Aus der Auflistung geht zudem hervor, dass Kontakte oder Familien in „Übersee“ gemeldet werden müssen und unternehmensseitig nachgehalten werden. Für das aufgeführte Personal ist diese Spalte einheitlich leer, was darauf hindeuten könnte, dass Kontakte oder Familien in Übersee ein Ausschlusskriterium für die Arbeit in vertraulichen Bereichen des Unternehmens darstellen. Auch eine Mitgliedschaft in der Kommunistischen Partei Chinas (KPCh) ist vermerkt.

Darüber hinaus liefert die Auswertung der im Datenleak enthaltenen Textdateien umfangreiche Informationen zu Verbindungen konkurrierender Cybersecurity-Unternehmen untereinander. So tauchen in Chat-Protokollen neben dem Aliasnamen „shutd0wn“ des i-Soon-Gründers noch weitere Namen auf, die Überschneidungen zu bekannten APT-Gruppierungen oder ehemaligen Mitgliedern der patriotischen Hackerszene der Volksrepublik zeigen. Viele dieser ehemaligen Mitglieder haben ebenfalls Cybersicherheits-Firmen gegründet, die Dienstleistungen für chinesische Nachrichtendienste anbieten.

10 Darstellung zur besseren Übersicht gekürzt. Es fehlen die Spalten Alter, Abschluss und Familie in Übersee; zudem wurden die Namen geschwärzt.

5. Ein „grenzenloses“ Angebot in einem hart umkämpften Markt

Das i-Soon-Datenleak liefert wichtige Erkenntnisse zur vielschichtigen Struktur und Reichweite des chinesischen Cyber-Ökosystems. Die Analysen zeigen, wie komplex dieses System aufgebaut ist und wie professionell es funktioniert. Die dabei gewonnenen Erkenntnisse dürften im Wesentlichen auch auf andere Unternehmen in der Volksrepublik China übertragbar sein, die innerhalb dieser florierenden Branche agieren. Die Branche hat eine Eigendynamik entwickelt, von der auch staatliche Stellen vollumfänglich profitieren können. Es wird deutlich, auf welche umfassenden Leistungen und Angebote der Staat aus diesem Wirtschaftssektor zugreifen kann.

Das Unternehmen i-Soon bewirbt seine Fähigkeiten auf der Firmenhomepage mit dem bezeichnenden Slogan „Sicherheit ist grenzenlos“. i-Soons erfolgreiche Bewerbung um eine Teilnahme an der staatlichen Datenbank CNNVD und das Streben nach anderweitigen Zertifizierungen/Qualitätssiegeln belegen beispielhaft das starke Engagement, um einen Wettbewerbsvorteil gegenüber konkurrierenden Anbietern zu erlangen. Abnehmer bzw. Auftraggeber der Produkte und Dienstleistungen von i-Soon müssen nicht mehr eigenständig Fachpersonal rekrutieren, keine hohen Beträge in die Produktentwicklung investieren und sich nicht selbst um Aspekte der operativen Sicherheit bemühen.

Dieses Outsourcing im Cyberraum führt zu einer zunehmenden Professionalisierung auch staatlicher Kampagnen und erschwert insbesondere die Rückverfolgung zu spezifischen Akteuren im Hintergrund. Eine Zuordnung der einzelnen Cyberoperationen innerhalb dieses hochkomplexen Systems wird immer herausfordernder.

In den weiteren CYBER INSIGHT-Ausgaben zum i-Soon-Datenleak geht das BfV näher auf die Struktur und Vorgehensweise der APT-Einheiten von i-Soon ein (Teil 1), beschreibt die betroffenen Länder und die konkreten Angriffsziele von i-Soon (Teil 3) und beleuchtet die Kunden und Produkte von i-Soon (Teil 4).

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