Köln, 15. August 2024

Bundesamt für Verfassungsschutz

BfV CYBER INSIGHT

Die i-Soon-Leaks: Industrialisierung von Cyberspionage

Teil 3: Konkrete Angriffsziele von i-Soon und betroffene Staaten

Die i-Soon-Leaks: Industrialisierung von Cyberspionage

Teil 3: Konkrete Angriffsziele von i-Soon und betroffene Staaten

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 Angreifen-den aufwändig vorbereitet, sind hochentwickelt („advanced“) und dauern lange an („persistent“).

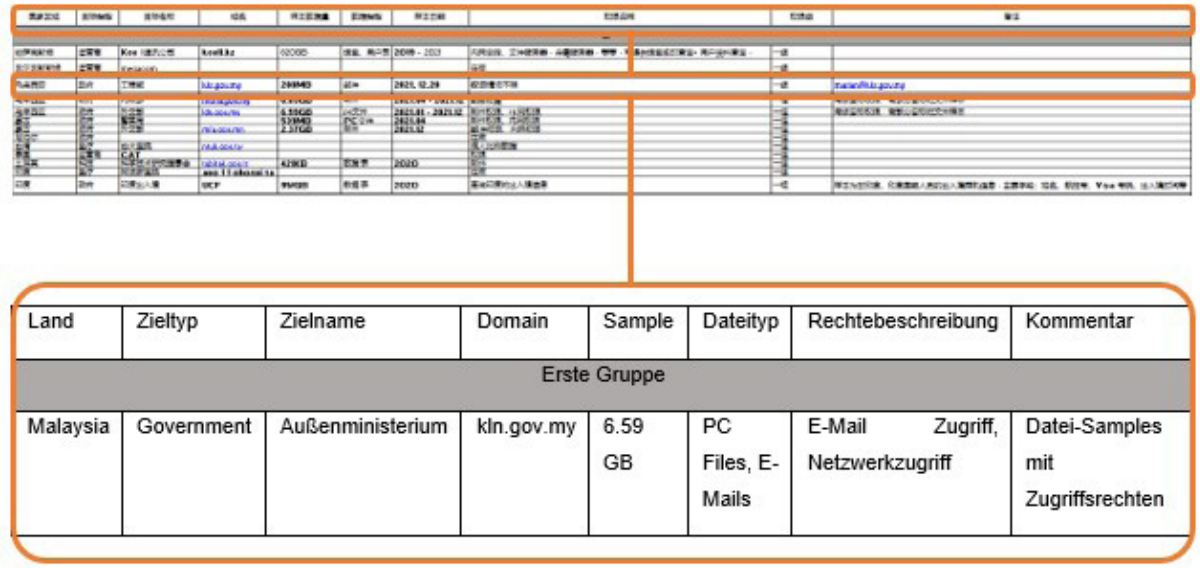
3 Zur Veranschaulichung wurden diverse Screenshots aus dem Leak übersetzt.

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, dieser Bericht),**
- i-Soon-Produkte und deren Abnehmer (Teil 4).

2. Zielregionen und -länder

Die im Leak enthaltenen Daten umfassen unter anderem eine Präsentation zu den Fähigkeiten und Dienstleistungen von i-Soon. Den eigenen Angaben zufolge fokussiert sich das Unternehmen mit seinen Cyberoperationen auf die Regionen Westasien, Südostasien sowie Hong Kong, Taiwan, Indien, Nepal und Tibet. Die in den Datensätzen enthaltenen Listen zu durchgeführten Cyberoperationen bestätigen diese Angaben. Zudem enthalten die geleakten Daten auch Hinweise auf Aktivitäten gegen EU-Institutionen und -Mitgliedsstaaten. Die Einträge zeigen laufende Operationen und ermöglichen so einen tiefen Einblick in das Management der APT-Aktivitäten von i-Soon (vgl. Abbildung 1).



Land	Zieltyp	Zielname	Domain	Sample	Dateityp	Rechtebeschreibung	Kommentar
Erste Gruppe							
Malaysia	Government	Außenministerium	kln.gov.my	6.59 GB	PC Files, E-Mails	E-Mail Zugriff, Netzwerkzugriff	Datei-Samples mit Zugriffsrechten

Abbildung 1: Auszug aus einer Liste mit Cyberoperationen

Ein Auszug zur Opferfläche zeigt Operationen vor allem gegen Hong Kong, Kasachstan, Malaysia, die Mongolei, Taiwan und Thailand. Zu den weiteren von Angriffen betroffenen Nationen gehören darüber hinaus Kirgisistan, Nepal, Türkei, Indien, Pakistan, Ägypten, Frankreich, Kambodscha, Uganda, Rwanda, Indonesien, Vietnam, Philippinen, Südkorea, China, Nigeria, Afghanistan und Myanmar (vgl. Abbildung 2).

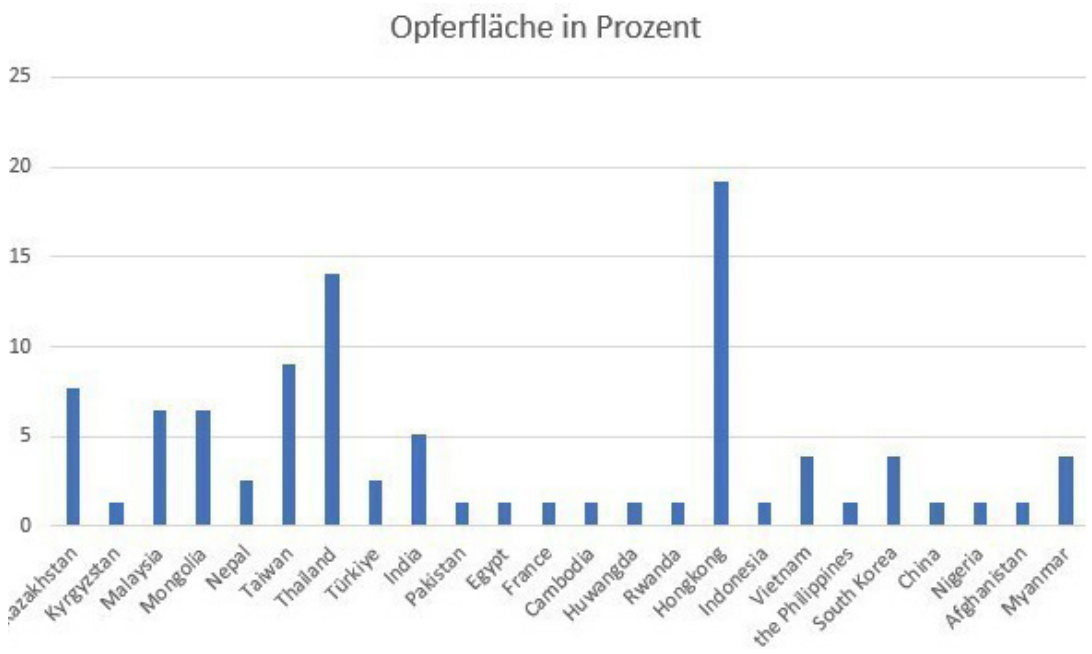


Abbildung 2: Verteilung betroffener Länder nach eigener Auswertung (N = 78)

Der Datensatz enthält keine Hinweise auf betroffene Stellen in Deutschland. Es bestehen jedoch Anhaltspunkte für Kompromittierungen mit Bezug zu EU-Institutionen sowie Angriffe gegen europäische Staaten und EU-Mitgliedstaaten.

3. Konkrete Angriffsziele

In einer im Leak enthaltenen Präsentation zu den Fähigkeiten und Dienstleistungen von i-Soon werden die Möglichkeiten des Unternehmens zur Kompromittierung von Netzwerken des Regierungs-, Medizin-, Transport-, Energieversorgungs- und des Telekommunikationssektors beworben. Diese Schwerpunkte werden in weiteren Daten des Leaks zu konkreten Cyberoperationen und Zielen bestätigt. So geben Datensätze zu Regierungseinrichtungen, Telekommunikations-

dienstleistern, Einrichtungen in Wissenschaft und Bildung, medizinischen Einrichtungen sowie verschiedene Datensammlungen zur Bevölkerung und religiösen Einrichtungen Aufschluss über die von i-Soon angegriffenen Stellen.

Regierungseinrichtungen nehmen mit über 43% den mit Abstand größten Anteil ein, gefolgt von Telekommunikationsdienstleistern mit fast 25% (vgl. Abbildung 3).

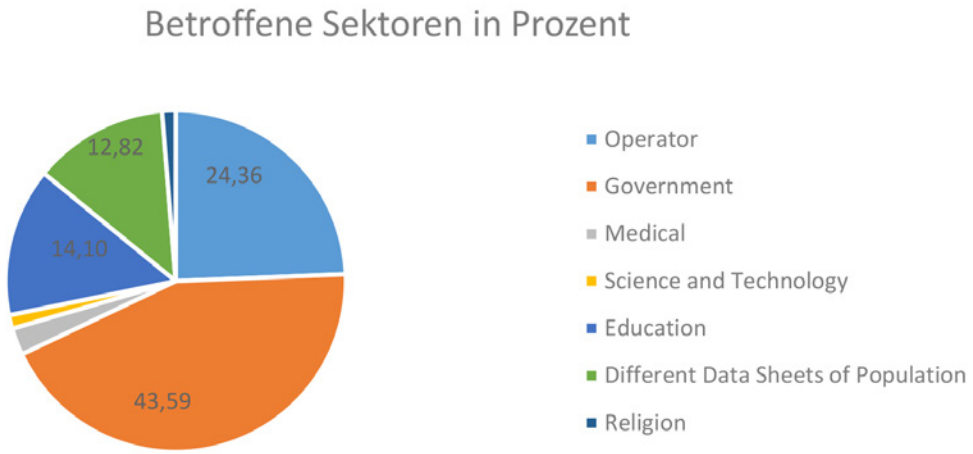


Abbildung 3: Verteilung der von Kampagnen betroffenen Sektoren (in Prozent)

Die geleakten Daten belegen einmal mehr eine Hacking-Industrie, die sowohl professionell als auch zielgerichtet agiert: In einer Liste wird in zehn Spalten unterteilt der aktuelle Bearbeitungsstand der konkreten Angriffsoperationen dokumentiert (vgl. Abbildung 4).

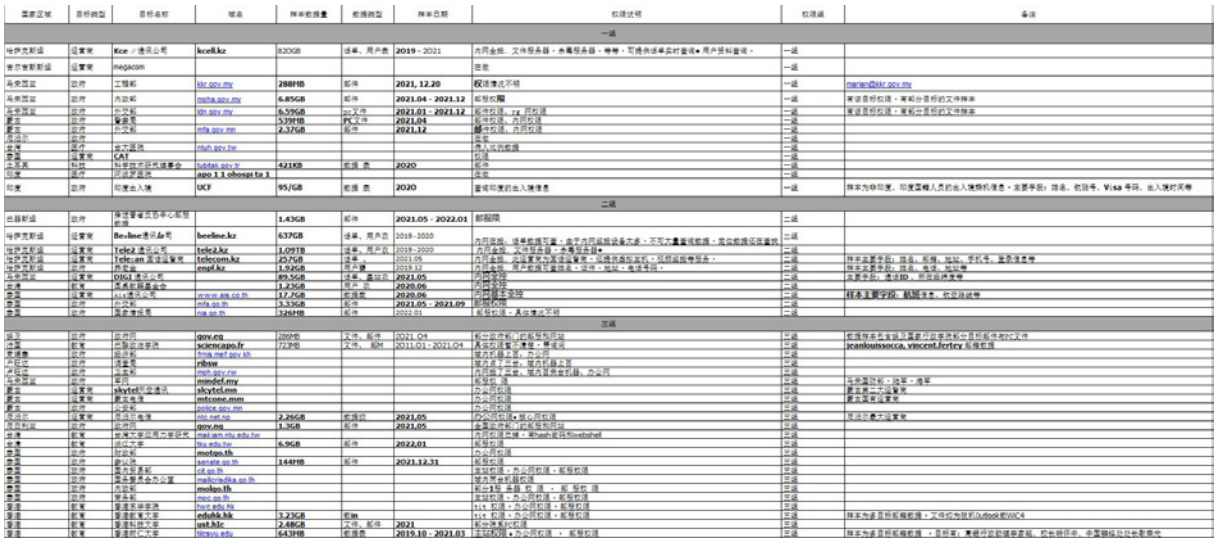


Abbildung 4: Liste von geleakten Cyberoperationen

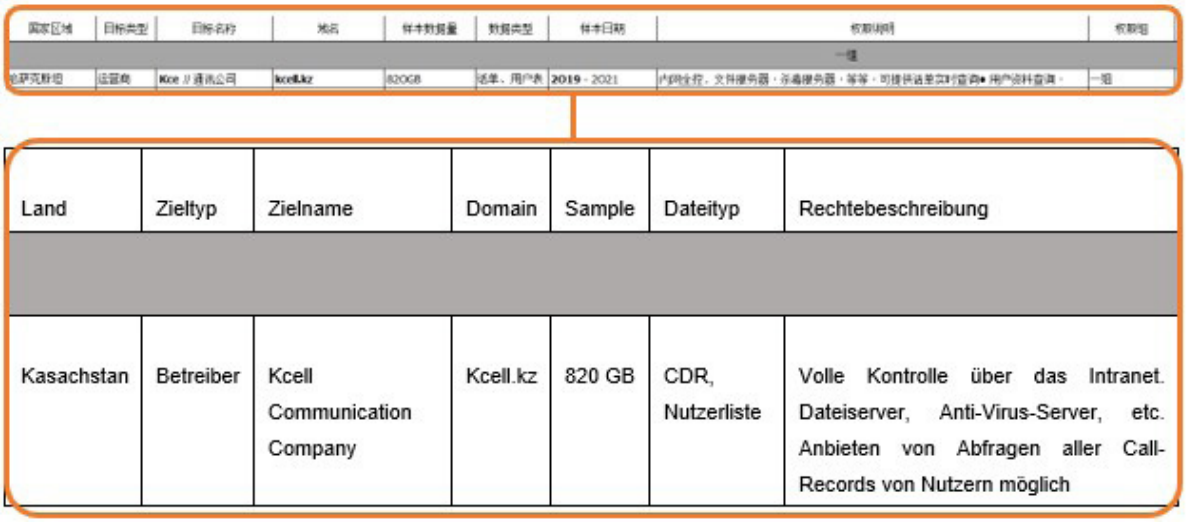
Die einzelnen Spalten enthalten Informationen über

- Zielland,
- Zieltyp,
- Zielname,
- Domain,
- Größe des Datei-Samples,
- Datum des Samples,
- Art der Daten,
- Beschreibung der Zugriffsmöglichkeiten,
- Rechtegruppe und
- Kommentare der bearbeitenden Stelle.

Die Daten bilden einen Zeitraum von bis zu zwei Jahren ab, in denen sich i-Soon mutmaßlich Zugang zu den Netzwerken der betroffenen Stellen verschafft hat. Aus geleakten Chat-Protokollen geht hervor, dass die hier vermerkten Datenauszüge an Kunden zur Bewertung und Vorauswahl verschickt wurden. Im Falle der Zustimmung des Auftraggebers übermittelt i-Soon ein vollständiges Datenset; im Falle einer Ablehnung werden andere Daten erbeutet.

In ihrer Gesamtheit geben die veröffentlichten Datensätze entscheidenden Aufschluss über das tatsächliche Ausmaß der Cyberoperationen. Die Kompromittierungen währten nicht nur lange, sondern sind auch hinsichtlich des erlangten Zugriffs oftmals weitreichend. Sie ermöglichen den Auftraggebern umfassende Befugnisse in den infiltrierten Netzwerken sowie eine detaillierte Einsicht in interne Vorgänge.

Die Tragweite lässt sich exemplarisch am Fall eines kasachischen Telekommunikationsdienstleisters nachvollziehen: Damit auftraggebende Klienten einen ersten Eindruck über Art und Umfang möglicher Daten gewinnen können, bietet i-Soon ihnen einen insgesamt 820 GB großen Datenauszug an. Als mögliche Leistungen werden die volle Kontrolle über das firmeninterne Intranet inklusive Dateiserver, Antiviren-Server etc. sowie Echtzeit-Abfragen zu Call-Records von Nutzern angeboten (vgl. Abbildung 5).



Land	Zieltyp	Zielname	Domain	Sample	Dateityp	Rechtebeschreibung
Kasachstan	Betreiber	Kcell Communication Company	Kcell.kz	820 GB	CDR, Nutzerliste	Volle Kontrolle über das Intranet. Dateiserver, Anti-Virus-Server, etc. Anbieten von Abfragen aller Call-Records von Nutzern möglich

Abbildung 5: Daten-Beispiel zu kasachischem Telekommunikationsunternehmen[4]

Aus der weiteren Auswertung der geleakten Screenshots können zusätzliche Erkenntnisse zu den konkreten Angriffszielen von i-Soon gewonnen werden. Sie enthalten u.a. Chatverläufe und Ordnerverzeichnisse mit mutmaßlichen Opferdaten, die auch Aktivitäten gegen u.a. EU-Institutionen und -Mitgliedsstaaten implizieren. Wenngleich weiterführende Bearbeitungsvermerke zu den einzelnen Angriffsoperationen fehlen, deuten allein die im Datenleck enthaltenen Screenshots auf die Möglichkeiten von i-Soon hin, in interne Netzwerke von Regierungsorganisationen einzudringen und diese zu kompromittieren.

Eine Abbildung eines Ordnerverzeichnisses zeigt beispielsweise Dateien, die allem Anschein nach aus einer französischen Betroffenheit stammen. Die abgebildeten EU-Dokumente sind als Verschlusssache gekennzeichnet und enthalten das Stichwort ZEUS (vgl. Abbildung 6). Dieses steht für „ZED! For European Union Security“. ZED! ist ein von der französischen Firma Prim’X Technologies entwickeltes Verfahren zur Verschlüsselung von Dokumenten und wird von Institutionen und Mitgliedstaaten der EU für den Versand eingestufter Dateien verwendet. Das Verfahren findet auch Anwendung für Dateien der NATO.

4 Die dargestellte Tabelle ist zur besseren Übersicht gekürzt. Einträge zum Datum der Operation und der Rechtegruppe sind nicht enthalten.

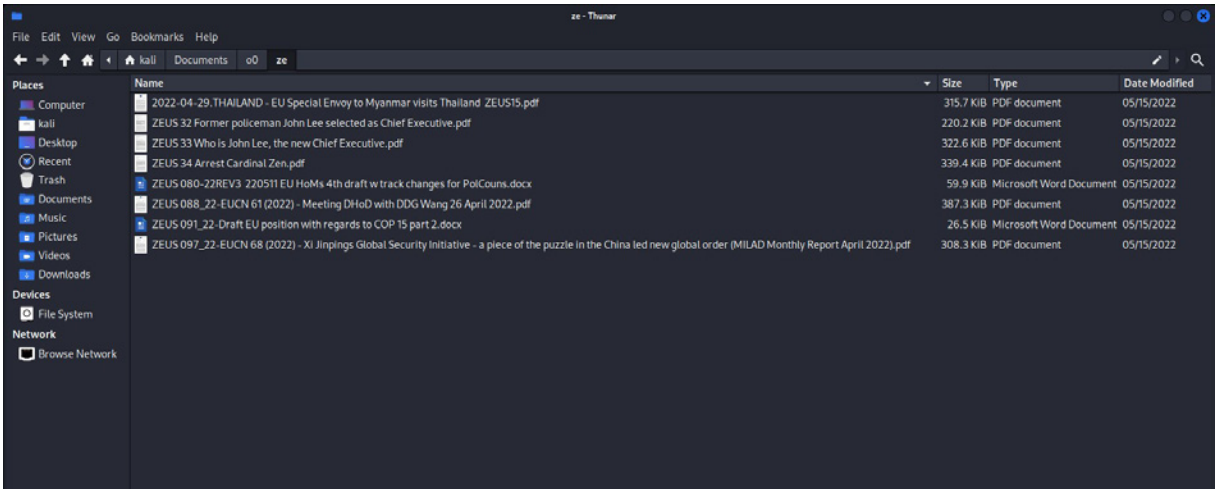


Abbildung 6: Opferdateien mit Bezug zur EU

Die Screenshots der mutmaßlich erbeuteten Daten deuten auf ein anhaltendes Interesse der Angreifer an Informationen im EU-Kontext hin. Zudem zeigen sie, dass private Hackerfirmen und Schadsoftware-Anbieter flexibel agieren, um an gewünschte Informationen zu kommen. Innerhalb eines Chatverlaufs der Cyberakteure wurde sich beispielsweise darüber ausgetauscht, ob bei (erbeuteten) Dokumenten auftauchende Abkürzungen für „das (europäische) Parlament“ oder „den (europäischen) Rat“ stünden (vgl. Abbildung 7).

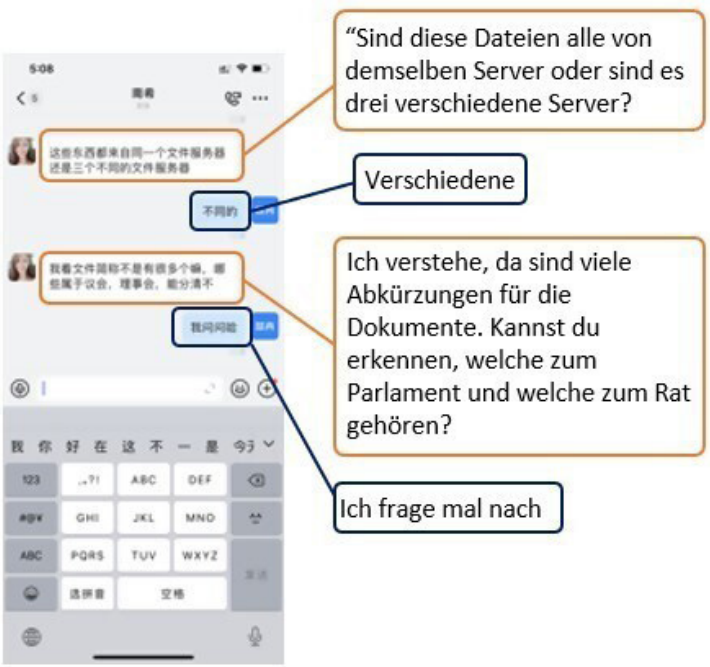


Abbildung 7: Chat zu erbeuteten Dokumenten

Weitere Screenshots von Opferdateien geben Hinweise auf Kompromittierungen in Nordmazedonien. Dateiordner mit der Bezeichnung „Notizen des Sekretariats für Europäische Angelegenheiten in Nordmazedonien“ implizieren, dass Informationen über die Beitrittsverhandlungen des Landes mit der EU im Fokus der Angreifer standen. Der maschinell übersetzte Dateiname „Nord Mazedonien öffentliche Anleitung zu Steuerdiensten” belegt das weitgehende Interesse an öffentlichen Einrichtungen in Nordmazedonien.

Abbildung 8: Ordner zur Kampagne gegen Nordmazedonien

Ein Screenshot enthält die Abkürzung „mvz“ im Verzeichnispfad, welche möglicherweise auf das Außenministerium der Tschechischen Republik hinweist (Ministerstva zahranicnich veci). Auch hier wird das Interesse der Angreifer an EU-Themen deutlich. Die abgebildeten Dokumente beziehen sich u.a. auf die Präsidentschaft im Ministerrat der EU für die zweite Jahreshälfte 2022 (vgl. Abbildung 9).

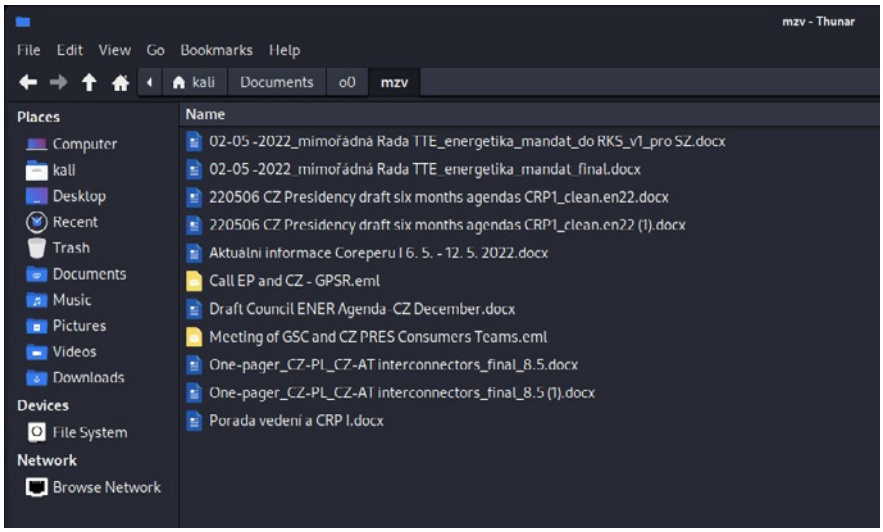


Abbildung 9: Dateien mit Bezug zur Tschechischen Republik

Ein weiterer Screenshot zeigt exemplarisch eine mögliche Zielauswahl für Angriffskampagnen in Großbritannien (vgl. Abbildung 10). Hier werden ebenfalls Angriffsziele mit Bezug zur Außenpolitik erkennbar. Daneben werden weitere, scheinbar zufällig zusammengestellte Institutionen aufgeführt. Eine mögliche Erklärung hierfür ist, dass die Angreifer dort potentiell weniger gut gesicherte Netzwerke vermuten, von wo aus sie einfacher in hochwertige Bereiche vordringen könnten.

Abbildung 10: Mögliche Ziele in Großbritannien[5]

4. Angriffsziele folgen geopolitischen Interessen Chinas

Die i-Soon-Leaks ermöglichen einen knappen Einblick in die verborgenen Machenschaften eines einzigen, mittelständischen Unternehmens. Auf dieser Basis lässt sich schlussfolgern, dass neben i-Soon eine unbekannte Anzahl an weiteren Akteuren in ähnlicher Weise beauftragt wird, staatliche Stellen sowie Unternehmen und Dienstleister ins Visier zu nehmen. Die APT-Aktivitäten eines ganzen Industriezweigs richten sich dabei gegen Angriffsziele auf der ganzen Welt. In ihrer Gesamtheit weisen sowohl die durch die i-Soon-Leaks bekannt gewordenen Zielländer als auch die konkreten Angriffsziele auf ein erhöhtes Interesse an politischen

5 Einige Zeilen wurden aufgrund schlechter Lesbarkeit nicht übersetzt.

Zielen hin. Die meisten Kompromittierungen bleiben dabei durch das professionelle Vorgehen der Akteure vermutlich weitestgehend unbemerkt.

Die regionale Schwerpunktsetzung auf Hong Kong, Thailand, Taiwan, Kasachstan, Malaysia und die Mongolei sowie die Fokussierung der Angriffe auf Regierungseinrichtungen und Telekommunikationsanbieter decken sich mit den geopolitischen Interessen der Volksrepublik China. Die Zielauswahl der vorgenannten Länder belegt, dass die Cyberaktivitäten ein wichtiges Instrument zur politischen Informationsgewinnung sind.

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 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