Sicherheitshinweis zur Gefahr durch nordkoreanische Cyberaktivitäten gegen die Rüstungsbranche

Zusammenfassung

Das Bundesamt für Verfassungsschutz (BfV) der Bundesrepublik Deutschland und der National Intelligence Service Südkorea (NIS) der Republik Korea veröffentlichen ein zweites Joint Cyber Security Advisory (CSA), um auf Cyberspionagekampagnen aufmerksam zu machen, die mit hoher Wahrscheinlichkeit von nordkoreanischen Cyberakteuren gegen die Rüstungsbranche durchgeführt werden.

Die Demokratische Volksrepublik Korea (DVRK) legt großen Wert auf militärische Stärke und konzentriert sich auf den Diebstahl fortschrittlicher Rüstungstechnologien von Zielen auf der ganzen Welt. Nach Einschätzung des BfV und des NIS nutzt das Regime die militärischen Technologien, um konventionelle Waffen zu modernisieren und deren Leistung zu verbessern sowie neue strategische Waffensysteme einschließlich ballistischer Raketen, Aufklärungssatelliten und U-Boote zu entwickeln. Die DVRK verwendet Cyberspionage zunehmend als kostengünstiges Mittel, um an militärische Technologien zu gelangen.

Dieser gemeinsame Sicherheitshinweis enthält die Tactics, Techniques and

Procedures (TTPs) sowie Indicators of Compromise[1] (IoCs) der DVRK und stellt zwei beispielhafte Fälle eines Eindringens in die IT-Infrastruktur von Einrichtungen der Rüstungsbranche vor.

Das BfV und der NIS attribuieren die in diesem Sicherheitshinweis beschriebenen Vorfälle einerseits zu der Advanced Persistent Threat (APT)-Gruppe LAZARUS sowie einer weiteren mutmaßlich nordkoreanischen Cybergruppierung. Obwohl diese Gruppierung im ersten Beispielfall überwiegend für den Einsatz von Spear-Phishing-Angriffen gegen Experten aus Diplomatie und Sicherheitspolitik bekannt ist, scheint sie ihre Zielfläche auch auf den Rüstungs- und Finanzsektor auszuweiten. Die Gruppierung LAZARUS wiederum ist ein bekannter und technologisch versierter Cyberakteur, der aufgrund seiner Beteiligung an einer ganzen Bandbreite von Cyberangriffen internationale Aufmerksamkeit auf sich gezogen hat. LAZARUS ist bekannt für seine versierten und komplexen Angriffsmethoden und die Beteiligung an besonders spektakulären Vorfällen. Dazu gehören u.a. finanziell-motivierte Diebstähle im Cyberraum, Ransomware-Kampagnen und Cyberspionage. Erfolgreiche Cyberangriffe gegen die Rüstungsbranche ebnen der DVRK den Weg zur Stärkung ihres Militärs, indem die weltweit erbeuteten sensiblen und vertraulichen Daten zum Vorteil der DVRK verwendet werden.

Da die Cyberakteure ihre Infrastruktur häufig wechseln und weltweit Einrichtungen angreifen, gehen das BfV und der NIS von einer vergleichbaren Entwicklung in der Zukunft aus und nehmen an, dass der Cyberakteur auch weiterhin aktiv sein wird. Dieser gemeinsame Sicherheitshinweis wird in der Absicht veröffentlicht, vor allem

[1] Bei Indicators of Compromise handelt es sich um spezifische Merkmale oder Anzeichen, die auf mögliche Angriffe oder Kompromittierungen von Computersystemen hinweisen können. Diese dienen dazu, verdächtige Aktivitäten zu identifizieren, um potenzielle Bedrohungen frühzeitig zu erkennen.

die Rüstungsbranche für Cyberangriffe dieser Art zu sensibilisieren. Darüber hinaus dient er der Aufklärung anderer Wirtschaftsbereiche sowie der Öffentlichkeit.

Technische Beschreibung

Im folgenden Abschnitt werden zwei Beispielfälle für gezielte Angriffe gegen die Rüstungsbranche skizziert. Ausgehend von den angewendeten TTPs der Angriffe handelt es sich im ersten Fall um eine Angriffskampagne gegen ein Forschungszentrum der Rüstungsbranche. Im zweiten Fall wird beschrieben, wie LAZARUS Social Engineering einsetzt, um Rüstungsunternehmen anzugreifen.

① Eindringen in ein Forschungszentrum der Rüstungsbranche über ein Webseiten-Wartungs- & Reparatur-Unternehmen

Die DVRK priorisiert seit kurzem die Erhöhung der Leistungsfähigkeit ihrer Marine. Im Zuge dessen wurde im September 2023 ein neues U-Boot fertiggestellt. Davor war Ende 2022 ein vermutlich nordkoreanischer Cyberakteur in die Netze eines Forschungszentrums für See- und Schifffahrtstechnologien eingedrungen. Der Cyberakteur führte einen Supply-Chain-Angriff durch und infiltrierte zunächst einen Dienstleister, der für die Wartung eines Webservers des Forschungszentrums

zuständig war, um anschließend das eigentliche Ziel zu kompromittieren. Der Cyberakteur drang anschließend weiter in die Forschungseinrichtung ein, indem er ferngesteuerte Malware über ein Patch-Management-System (PMS) des Forschungszentrums auslieferte und verschiedene Zugangsdaten für Geschäftsportale sowie E-Mail-Inhalte stahl. Der Angriff wird mittels MITRE ATT&CK[2] beschrieben:

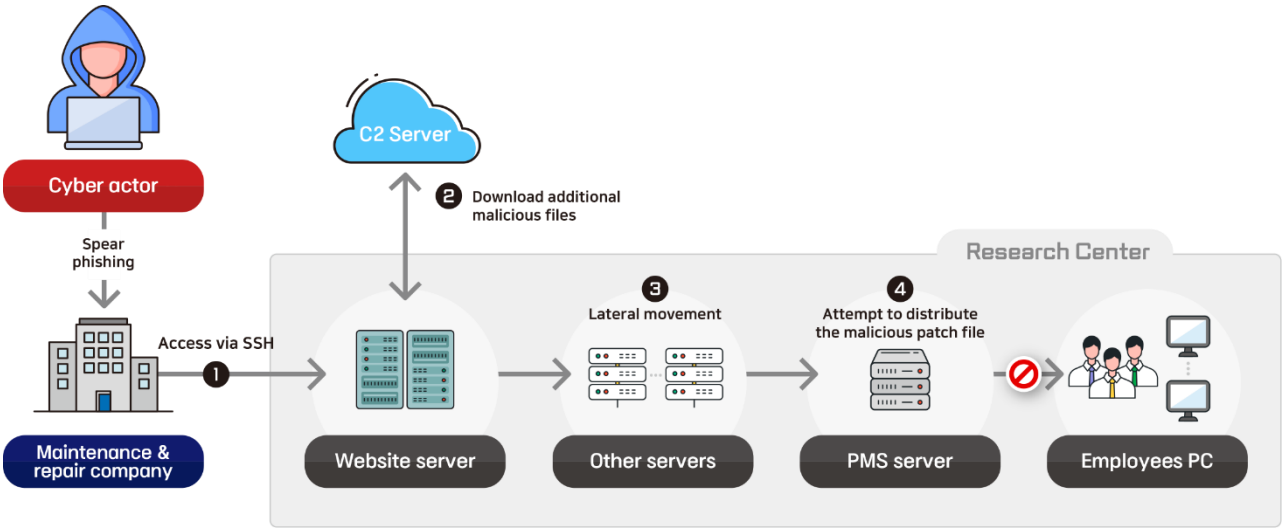

Abbildung 1 - Übersicht über den Ablauf des Supply-Chain-Angriffs

Ablauf des Supply-Chain-Angriffs

1. Der Cyberakteur drang in ein Unternehmen ein, das für die Wartung des Webservers seines Ziels verantwortlich war, und stahl SSH-Zugangsdaten. Dann erfolgte ein Zugriff aus der Ferne auf den Webserver (Linux) des Forschungszentrums durch den Angreifer (T1133).

[2] Bei MITRE ATT&CK handelt es sich um eine global verfügbare Datenbank, in der spezifische Angriffsmethoden und -techniken von Cyberakteuren nachgehalten werden.

2. Der Akteur verwendete legitime Programme einschließlich curl, um maliziöse Dateien von C2-Servern herunterzuladen wie etwa ein Tunneling-Tool für den Fernzugriff (Ngrok) und ein Base64-kodiertes Python-Skript, das als Downloader diente.

3. Für die weitere Ausbreitung (*lateral movement*) im Netzwerk stellte der Angreifer eine SSH-Verbindung zu weiteren Servern des Forschungszentrums her, die in Verbindung mit der Webseite standen. Der Akteur schnitt anschließend Netzwerkpakete der Server mithilfe von tcpdump mit und erlangte so weitere Informationen über das Netzwerk und stahl Anmeldeinformationen für Accounts der Mitarbeiter des Ziels (T1040, T1046, T1021).

4. Der Cyberakteur verwendete anschließend die Anmeldedaten eines Sicherheitsmanagers und erhielt so Zugriff auf dessen E-Mail-Konto, um Informationen zu einem Verfahrensablauf des PMS zu erlangen. Der Akteur gab sich als der Sicherheitsmanager aus und sendete eine E-Mail an den PMS-Dienstanbieter mit dem Auftrag, eine Patch-Datei mit maliziösen Funktionen zu erstellen. Trotz der Tarnung als legitime Datei erkannte der echte Sicherheitsmanager den Versuch, die maliziöse Patch-Datei über das PMS zu verteilen und wehrte ihn erfolgreich ab. Der maliziöse Code enthielt Funktionen zum Up- und Download von Dateien, dem Ausführen von Programmen, der Sammlung von Systeminformationen usw. (T1041, T1001, T1071).

5. Auch nachdem das Forschungszentrum die Sicherheitsmaßnahmen bereits erhöht hatte, setzte der Cyberakteur seine Angriffsversuche fort. Er lud unter

Ausnutzung einer Upload-Schwachstelle eine Webshell auf einem Webserver hoch und sendete Spear-Phishing-E-Mails.

MITRE ATT&CK Matrix für Enterprise Linux Plattform (v14)

Tactics	Techniques	Beschreibung
Initial Access (TA0001)	External Remote Service (T1133)	SSH
Execution (TA0002)	Command and scripting interpreter (T1059)	tcpdump, ngrok and curl
Persistence (TA0003)	Valid Accounts (T1078)	Server admin account, Email account, SSL-VPN account
Defense Evasion (TA0004)	Indicator removal (T1070) Obfuscated Files or Information (T1140)	Files delete, File encryption and decoding
Credential Access (TA0006)	Network Sniffing (T1040)	tcpdump
Discovery (TA0007)	Network Sniffing (T1040) & Network Service Discovery (T1046)	tcpdump
Lateral movement (TA0008)	Remote Services (T1021)	SSH
Collection (TA0009)	Data from Information Repositories (T1213)	Website source code, Server configuration information
Command and control (TA0011)	Data Obfuscation (T1001) Application Layer Protocol (T1071) Protocol Tunneling (T1572)	AES-256, Use of HTTP protocol, ngrok
Exfiltration (TA0010)	Exfiltration Over C2 Channel (T1041)	HTTP C2 server

Wichtige Erkenntnisse

Statt der direkten Kompromittierung eines Zielsystems führte der Cyberakteur zunächst Angriffe gegen einen Dienstleister des Forschungszentrums durch. Da es während der COVID-Pandemie schwierig wurde, Wartungs- und Reparaturdienste für die Serverinfrastruktur vor Ort zu gewährleisten, wurden stattdessen Remote-Dienste angeboten. Fehlende Sicherheitsmaßnahmen ermöglichten jedoch den sogenannten unbeaufsichtigten Zugriff auf Server ohne Zugriffsbeschränkungen.

In den meisten Fällen stellt ein Cyberakteur seine Aktivitäten ein, sobald er erkannt wurde. In dem hier geschilderten Fall unternahm der Angreifer jedoch auch nach der Blockierung der PMS-Distribution und des SSH-Fernzugriffs verschiedene Versuche, die Persistenz aufrechtzuerhalten, indem er Spear-Phishing-E-Mails an die Mitarbeiter des Ziels sendete und versuchte, eine Web-Shell auf die Webseite hochzuladen.

Darüber hinaus verzichtete der Akteur auf die Durchführung eines direkten Angriffs auf sein Ziel, welches ein hohes Sicherheitsniveau aufrechterhielt, und griff ersatzweise zunächst dessen Dienstleister - das Wartungs- und Reparaturunternehmen - an. Dies zeigt, dass der Akteur die vertrauensvolle Beziehung zwischen den beiden Parteien kannte und bewusst zu seinem Vorteil ausnutzte.

Weitere Informationen und Hinweise für staatliche und öffentliche Organisationen der Republik Koreas bezüglich der Inanspruchnahme von Fernwartungs- und Reparaturdienstleistungen durch externe Dienstleister finden Sie in Artikel 26 (Security of Service Providers) der Basic Guidelines for National Intelligence Security

of the Republic of Korea. Deutsche staatliche und öffentliche Organisationen können diesbezüglich die Richtlinien OPS.2.1 und OPS.1.2.5 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu Rate ziehen.

② Social Engineering-Angriffe der DVRK

Im zweiten Fall werden die besonderen Fähigkeiten der Gruppierung LAZARUS im Bereich Social Engineering dargestellt. Seit mindestens Mitte des Jahres 2020 nutzt die DVRK diesen Angriffsvektor, um Rüstungsunternehmen zu infiltrieren. Aufgrund der Tatsache, dass die angegriffenen Mitarbeiter der Unternehmen in allen

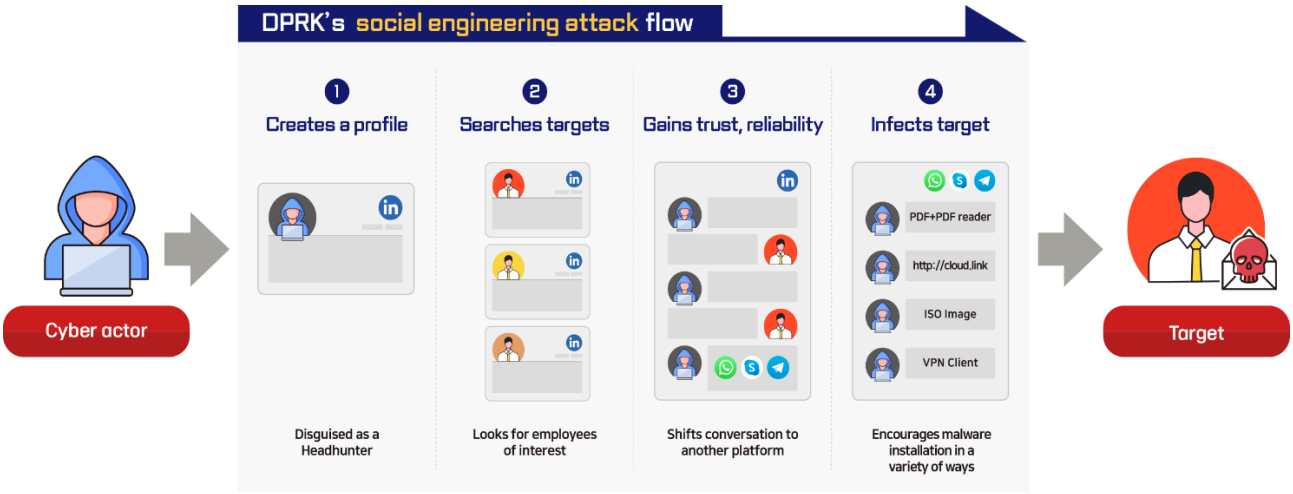

Abbildung 2 - Übersicht über den Ablauf eines Angriffs

beobachteten Fällen maliziöse Dateien erhielten, die durch Bezugnahme auf Stellenangebote getarnt waren, wurde die Kampagne schnell als „Operation Dream Job“ bekannt. Inzwischen führt LAZARUS diese Art von Angriff seit mehr als drei Jahren gegen die Rüstungsbranche durch und hat sich als ein geschickt operierender und technisch sehr versierter Akteur erwiesen, der nicht nur eine ernstzunehmende Bedrohung im Cyberraum, sondern für die globale Sicherheit darstellt.

Ablauf eines Social Engineering-Angriffs

Bezogen auf Cyberangriffe ist Social Engineering eine nicht-technische Methode, die menschliches Vertrauen, Neugier, Angst, Gier oder Zeitdruck ausnutzt, um maliziöse Absichten zu verwirklichen, zum Beispiel zum Zwecke des Diebstahls von Zugangsdaten. Im Laufe der Zeit hat Social Engineering sich als hochwirksames Mittel erwiesen, um Schwächen der menschlichen Psyche auszunutzen und Individuen zu Handlungen zu bewegen, die Sicherheitskompromittierungen auslösen können. Die anhaltende Nutzung von Social Engineering könnte dem Umstand geschuldet sein, dass die getroffenen Sicherheitsvorkehrungen der Security Operations Center (SOCs) heutzutage eine oftmals nahezu unüberwindbare Barriere für Cyberakteure darstellen. Obwohl sich das technische Vorgehen der Gruppierung LAZARUS während der Kampagne bereits mehrfach änderte, blieb die Strategie des Social Engineerings immer gleich.

1. Im ersten Schritt legt LAZARUS ein Profil auf einem Online-Jobportal an. Die bisher festgestellten Profile waren entweder gestohlene Profile real existierender Personen oder Profile, die mit gefälschten Daten erstellt wurden. In beiden Fällen soll das Profil wie das eines Headhunters mit einem breiten Netzwerk von Kontakten zu Personen aussehen, die in der Rüstungsbranche arbeiten. Sobald das Profil täuschend echt aussieht, fährt der Akteur mit dem nächsten Schritt fort.

2. LAZARUS sucht nach möglichen Zielen, indem Profile von Personen durchsucht werden, die für eines der in Frage kommenden Unternehmen arbeiten. Unter diesen Personen sucht der Akteur nach denjenigen, die Zugang zu wertvollen Ressourcen wie beispielsweise internen Systemen haben könnten.

3. Sobald LAZARUS einen geeigneten Mitarbeiter gefunden hat, werden dem Angreifer-Profil mitunter Kontakte aus dem Umfeld des Ziels hinzugefügt, um vertrauens- und glaubwürdiger zu erscheinen. Anschließend wird über die Nachrichtenfunktion des Jobportals Kontakt zum Mitarbeiter aufgenommen und die Unterhaltung zumeist auf Englisch geführt. Der darauffolgende geschäftliche Smalltalk mit dem Mitarbeiter kann Tage bis Wochen oder sogar Monate dauern und soll Vertrauen schaffen. Im Verlauf dieses Austauschs wird der Zielperson ein Job angeboten. Auch wenn der ausgewählte Mitarbeiter kein Interesse zeigt, nimmt sich der Angreifer Zeit, ihn zu überzeugen - beispielsweise indem er das großzügige Gehalt der angebotenen Position hervorhebt. Unter dem Vorwand einen diskreten Einstellungsprozess einzuleiten wird das Ziel aufgefordert, die Kommunikation auf einen anderen Kanal zu verlegen (z.B. WhatsApp, Telegram, Skype, Discord oder andere).

4. Für den Fall, dass der ausgewählte Mitarbeiter erfolgreich zu einem anderen Kommunikationskanal gelockt wurde, hat LAZARUS verschiedene Ansätze entwickelt, um die Sicherheitsmaßnahmen des Unternehmens zu umgehen.

   a. Der Akteur übermittelt eine PDF-Datei mit einem lukrativen Jobangebot, das auf die Interessen des ausgewählten Mitarbeiters zugeschnitten ist, und einen manipulierten PDF-Reader, der versteckte Schadsoftware enthält.

   b. LAZARUS übermittelt eine Datei mit allgemeinen Informationen zu der Stelle. Sobald der Mitarbeiter weitere Details erfahren möchte, sendet der Angreifer im Anschluss einen Link zu einer Datei mit detaillierten Informationen an die Unternehmens-E-Mail-Adresse und stellt so sicher, dass sich der Mitarbeiter

zum Zeitpunkt der Bereitstellung des Links in seiner Arbeitsplatzumgebung befindet. Die damit verknüpfte Datei ist auf einem Cloud-basierten Dienst gespeichert und enthält die erste Stufe der Schadsoftware.

c. In den jüngsten Fällen der Kampagne wurden die Stellenangebote vorrangig an Programmierer adressiert. Dabei übermittelt LAZARUS Zip-Dateien mit einem Iso-Image einer Programmieraufgabe, die angeblich im Rahmen des Rekrutierungsprozesses gelöst werden muss. Sobald der Programmierer die Aufgabe ausführt, wird die Maschine mit der ersten Stufe der Schadsoftware infiziert.

d. Eine weitere Möglichkeit, mit der die Gruppierung LAZARUS versucht, Zugriff auf das Netzwerk des Unternehmens zu erhalten, ist die Übermittlung eines maliziösen VPN-Clients in einer Zip-Datei.

Wichtige Erkenntnisse

Die Tatsache, dass Mitarbeiter normalerweise nicht mit ihren Kollegen oder Arbeitgebern über neue Jobangebote sprechen, spielt hierbei dem Angreifer in die Hände. Die LAZARUS-Gruppierung hat im Verlauf der Kampagne ihre Werkzeuge mehrfach verändert und mehr als einmal demonstriert, dass sie in der Lage ist, innovativ und flexibel vorzugehen.

Sicherheitsmaßnahmen

Die folgenden Präventionsrichtlinien des gemeinsamen Sicherheitshinweises beruhen auf Beobachtungen des BfV und des NIS.

Informieren Sie Ihre Mitarbeiter regelmäßig über die neuesten Entwicklungen bei Cyberangriffen. So kann das Verständnis für die sich ständig weiterentwickelnde Vorgehensweise von Cyberakteuren verbessert werden und eine schnelle Reaktion durch die Mitarbeiter gewährleistet werden, sollte es tatsächlich zu einem Eindringen in die Systeme des Unternehmens kommen.

Da die meisten Angriffe der Cybereinheiten der DVRK durch Social Engineering und Supply-Chain-Angriffe erfolgen, regen das BfV und der NIS folgende Sicherheitsmaßnahmen an.

Sicherheitsmaßnahmen gegen indirekte Angriffe über einen Dienstleister

- Zugriffsrechte sollten sich nur auf die dafür notwendigen Systeme erstrecken, wenn Sie Fernwartungs- und Reparaturdienste nutzen. Bevor Benutzerberechtigungen und -privilegien erteilt werden, sollte eine Authentifizierung durchgeführt werden.

- Speichern und pflegen Sie Audit-Protokolle[3] einschließlich der Zugriffe auf ein System und überprüfen Sie diese regelmäßig, um einen Zugriff außerhalb der Norm zu erkennen und ggf. analysieren zu können.

- Da das PMS leicht zum Ziel für Supply-Chain-Angriffe durch Cyberakteure werden kann: Etablieren Sie ein geeignetes PMS-Verfahren, um Benutzerauthentifizierungen zu verifizieren und implementieren Sie entsprechende Verifizierungen sowie Zustimmungsprozesse bezüglich der finalen Distributionsphase.

[3] Audit-Protokolle ermöglichen eine nachträgliche Betrachtung des Nutzerverhaltens in einem Netzwerk, z.B. durch Aufzeichnung von erfolgreichen/erfolglosen Anmeldeversuchen.

- Verwenden Sie beim Erstellen von Webseiten immer SSL/TLS, um einen illegitimen Zugriff auf kritische Daten wie Benutzerinformationen zu verhindern - selbst wenn es dem Cyberakteur gelingen sollte, Logdateien mitzuschneiden.

- Sollten Mitarbeiter eine VPN-Verbindung nutzen, um aus dem Home-Office zu arbeiten, wird eine Multi-Faktor-Authentifizierung zusätzlich zu der Authentifizierung durch Benutzerkennung und Passwort empfohlen. Dabei müssen sensible Informationen wie einmalig verwendbare Passwörter (OTP) und Authentifizierungsschlüssel vor der Weitergabe an Dritte geschützt werden.

- Bitte beachten Sie auch den Abschnitt „Sicherheitsmaßnahmen“ des ersten BfV-NIS Joint Advisory für detaillierte Präventionshinweise zu Spear-Phishing-Angriffen, das im März 2023 veröffentlicht wurde.

Social Engineering-Angriffe: Sicherheitsmaßnahmen und Best Practices

- Eine geeignete Maßnahme um Social Engineering-Angriffe zu erschweren, ist die Aufklärung der Mitarbeiter über die bekanntesten Vorgehensweisen beim Social Engineering. Dazu zählt Wachsamkeit gegenüber verdächtigen passwortgesperrten Dokumenten oder Links. Ebenso sollte eine Fehlerkultur etabliert werden, die Mitarbeiter ermutigt, Sicherheitsvorfälle zu melden ohne Konsequenzen fürchten zu müssen, weil sie Opfer eines Social Engineering-Angriffs geworden sind.

- Ein weiterer wichtiger Bestandteil zur Reduzierung des Risikos von Social Engineering-Angriffen ist die möglichst restriktive Vergabe von Privilegien und Zugriffsrechten auf sensible Daten.

- Um Schwachstellen in Netzwerksystemen zu beseitigen, sollte eine konsequente Update- und Patch-Routine etabliert werden.

- Es wird empfohlen, diese Sicherheitsmaßnahmen auf alle inländischen und ausländischen Zweigstellen Ihres Unternehmens anzuwenden, einschließlich derer, die möglicherweise als unbeteiligt am Tagesgeschäft gelten.

Kontakt

Bitte wenden Sie sich an die jeweils zuständige Behörde, wenn Sie den Verdacht haben, dass Ihre Organisation möglicherweise Ziel eines staatlich gesteuerten Cyberangriffs geworden ist.

Ansprechpartner in Deutschland:

Bundesamt für Verfassungsschutz

(www.verfassungsschutz.de,+ 49 (0) 30-18 / 792-3322)

Ansprechpartner in der Republik Korea:

National Intelligence Service (www.nis.go.kr, + 82 111)

Indicators of Compromise (IoCs)

IoCs der Cyberspionagekampagne gegen ein Webseite-Wartungs- & -Reparatur-Unternehmen der Rüstungsbranche

Eigenschaft	IoC	Anmerkung
C2	connection.lockscreen.kro[.]kr/index.php	C2 URL
	updating.dothome.co[.]kr/microsoft/app/google	C2 URL
MD5	3c2aa3687ac9f466ce909e2cb12b07a5	Remote control (EncryptModule_Patch.exe)
	4631ef8db9c36b0f2534ac7193f2587e	Malicious script (JSE)
	607a2a8d2863c3144b8e901a16a76c33	Webshell (_banner.jsp)

IoCs der Social Engineering-Kampagne von LAZARUS gegen die Rüstungsbranche

Eigenschaft	IoC	Anmerkung
Domain	chrysalisc[.]com	Domain
	sifucanva[.]com	Domain
	thefrostery.co[.]uk	Domain
	rginfotechnology[.]com	Domain
	job4writers[.]com	Domain
	contact.rgssm[.]in	Domain
SHA-1	7da62cdb447a7ae3ae7b5f67a511e7cf2b26c7df	Boeing_Asia_ERP_IT_SA.zip
	2e0d374f1e706ae1fa24558b54c5a1630302eab1	Boeing_Asia-ERP_IT_SA.iso
	294706ae0585abaf4e6c5e66a7f5141ac4281d57	Amazon VNC.exe

	127ced578e041f53b5988a7fefaa6e09e64f4bf9	AmazonVNC Viewer.exe
	3bc8acdd07c6d91652101d9c8b3326bee372a007	
	7906270679014234b70aa63dd89e8282a945919c	
	7b4d0d8e3bfcd634bc7d7a17fb546b7e8316a681	Amazon VNC.zip
	d5c8edb84e4ff33aea8865676ffe801ff0a71701	AMAZON_BSA_SKILL_ASSESSMENT_V2.ZIP
	ac9021eb798de8323702a5aeb7c590f1ebaa3786	
	d5c8edb84e4ff33aea8865676ffe801ff0a71701	Amazon_BSA_SA_v2.iso
SHA-256	F3482A38BEFDCD7D0B87D86F24CDB209028BD8471BAA6610548FB721086F5B85	Accenture_IT_SA.zip
	47999FA014B6CC5A2A71BE590C93830371E259242DFDBA7FFA2698F1900919EC	Accenture_IT_SA.iso

YARA[4]-Regel zur Identifizierung von Operation Dream Job-Dateien

Die folgende YARA-Regel entstand aus der Untersuchung der Funktion einer Amazon VNC Viewer Datei und kann mindestens die drei - mit den oben genannten Hashwerten - verschiedenen Amazon VNC Viewer Samples feststellen. Diese Regel zeigt, wie die zur Verfügung gestellten IoCs bei korrekter Anwendung zur Aufdeckung von Cyberbedrohungen genutzt werden können.

[4] Eine YARA-Regel enthält Signaturen und Bedingungen, um Dateien oder Prozesse nach bestimmten Mustern zu durchsuchen und Schadsoftware erkennen zu können.

(Die eckigen Klammern in der unten aufgeführten URL dienen dem Schutz vor versehentlichem Anklicken eines maliziösen Links und müssen entfernt werden, damit die Yara-Regel angewendet werden kann.)

```
rule operation_DREAMJOB_AMAZON_VNC {
meta:
        target_entity = “file”
condition:
        for any vt_behaviour_command_executions in vt.behaviour.command_executions:
                ( vt_behaviour_command_executions ==
                “C:\\Windows\\System32\\wuapihost.exe -Embedding”
        or
        vt_behaviour_command_executions == “\”%SAMPLEPATH%\\AmazonVNC
                Viewer.exe\” “)
        and
        for any vt_behaviour_http_conversations in vt.behaviour.http_conversations: (
                vt_behaviour_http_conversations.url == https://sifucanva[.]com/wp-
                includes/fonts/public/common.php)
}
```