Köln, 10. August 2023

Bundesamt für Verfassungsschutz

BfV Cyber-Brief Nr. 01/2023

Warnhinweis zu Cyberspionage gegen Kritiker des iranischen Regimes in Deutschland

Kontakt:
Bundesamt für Verfassungsschutz
Cyberabwehr
☎ 030 18792 3322

Warnhinweis zu Cyberspionage gegen Kritiker des iranischen Regimes in Deutschland

Im Jahr 2022 berichteten mehrere IT-Sicherheitsdienstleister über die APT-Gruppierung[1] Charming Kitten[2], die an der Ausforschung von iranischen Oppositionellen und Exil-Iranern beteiligt sein soll.[3] Die Cyberangriffe richteten sich vor allem gegen Dissidentenorganisationen und Einzelpersonen – wie Juristinnen und Juristen, Journalistinnen und Journalisten oder Menschenrechtsaktivistinnen und -aktivisten – innerhalb und außerhalb des Iran.

Nach aktuellen Erkenntnissen des Bundesamtes für Verfassungsschutz (BfV) ist von konkreten Ausspähversuchen der Gruppierung Charming Kitten gegen iranische Personen und Organisationen in Deutschland auszugehen. Hierzu verwendet die Gruppierung ein ausgefeiltes Social Engineering[4] und entwickelt auf die Opfer zugeschnittene Online-Identitäten. Das BfV empfiehlt zum Schutz vor den hier genannten Ausspähversuchen eine Reihe von einfach umsetzbaren konkreten Maßnahmen.

[1] Advanced Persistent Threat (APT): Unter APT werden komplexe, zielgerichtete Bedrohungen verstanden, die sich gegen ein oder mehrere Opfer richten. Die konkreten Angriffe im Rahmen dieser Bedrohungen („threats“) werden von Angreifenden aufwändig vorbereitet, sind hoch entwickelt („advanced“) und dauern lange an („persistent“).

[2] Auch bekannt als APT42, Phosphorus, Cobalt Illusion, Yellow Garuda, Mint Sandstorm.

[3] Vgl. Mandiant (2022): Ein Profil der Hackergruppe APT42: Hinterhältige Akteure und heikle Angriffe, in: www.mandiant. de/resources/blog/apt42-charms-cons-compromises, abgerufen am 08.08.2023, vgl. Proofpoint (2022): Look What You Made Me Do: TA453 Uses Multi-Persona Impersonation to Turn FOMO Into a Cybersecurity Risk, in: www.proofpoint.com/us/blog/threat-insight/ta45Social3-uses-multi-persona-impersonation-capitalize-fomo, abgerufen am 08.08.2023 und vgl. Certfa Lab (2022): Charming Kitten: “Can We Have A Meeting”, in: https://blog.certfa.com/posts/charming-kitten-can-we-wave-a-meeting, abgerufen am 08.08.2023.

[4] Unter Social Engineering wird das Ausspionieren des persönlichen Umfelds durch zwischenmenschliche Beeinflussung bzw. durch geschickte manipulative Fragestellung, meist unter Verschleierung der eigenen Identität und Absichten, verstanden. Social Engineering hat das Ziel, unberechtigt an personenbezogene Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen. Siehe auch „Schutz vor Social Engineering – Hinweise für Beschäftigte“ und „Proctection against Social Engineering – Information for employees“, in: www.verfassungsschutz.de, abgerufen am 08.08.2023.

Hintergrund

Die APT-Gruppierung Charming Kitten versucht mittels Spear-Phishing an vertrauliche Daten ihrer Opfer zu gelangen. Ziel ist es, Zugang zu Onlinediensten wie E-Mail-Konten, Cloudspeicher oder Messenger-Diensten zu erhalten, die vom potenziellen Opfer genutzt werden.

In einem ersten Schritt werden die Vorlieben und Interessen, auch politischer Natur, durch den Angreifer ausgeforscht. Dabei dienen Veröffentlichungen im Internet oder auf Plattformen sozialer Medien als unkomplizierte Möglichkeiten, um Informationen zu Personen zu erlangen.

Im zweiten Schritt findet die persönliche Kontaktaufnahme statt, bei der das Opfer durch Social Engineering manipuliert und mit falschen Versprechungen zu sicherheitskritischem Verhalten verleitet werden soll.

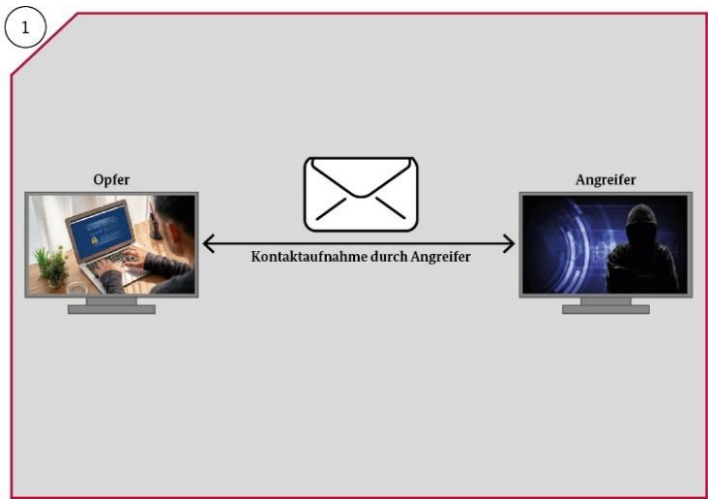
Sobald sich die Konversation etabliert hat, sendet der Angreifer in einem dritten Schritt eine Einladung zu einem Online-Videochat. Um am Videochat teilnehmen zu können, muss das Opfer auf den vom Angreifer versendeten Link klicken. In der Anmeldemaske geben die Opfer ihre Login-Daten ein und ermöglichen dem Angreifer Zugriff auf die von ihnen genutzten Onlinedienste.

Durch das im Vorfeld erfolgte Social Engineering kann Charming Kitten zielgerichtet einen scheinbar unbedenklichen Kontakt etablieren, indem sich die Gruppierung auf Personen bezieht, die den Opfern bekannt sind oder Themen anspricht, die den Opfern schlüssig erscheinen. Zum Werkzeugkasten der Gruppierung gehört ebenfalls das E-Mail-Spoofing[5]. So täuscht Charming Kitten Opfern vor, sie würden mit real existierenden, zum Teil öffentlich bekannten Personen kommunizieren, wie Journalistinnen und Journalisten oder Mitarbeitenden einer NGO.

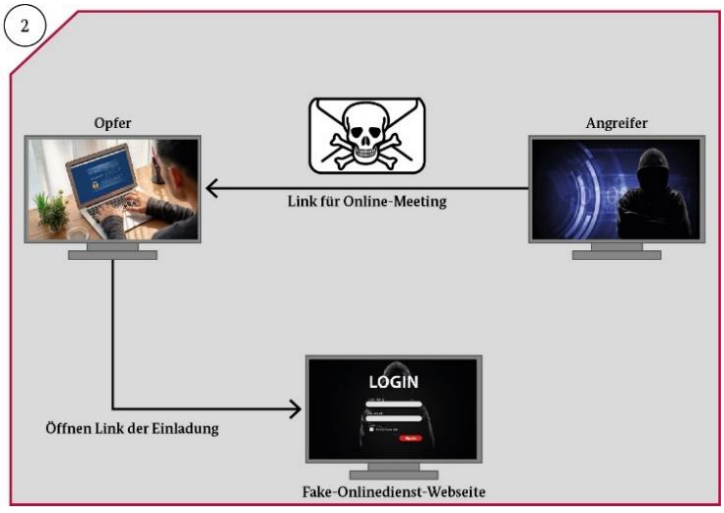
[5] Spoofing (von to spoof, auf Deutsch: manipulieren, verschleiern oder vortäuschen) nennt man in der IT verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

Ablauf der Spear-Phishing-Angriffe:

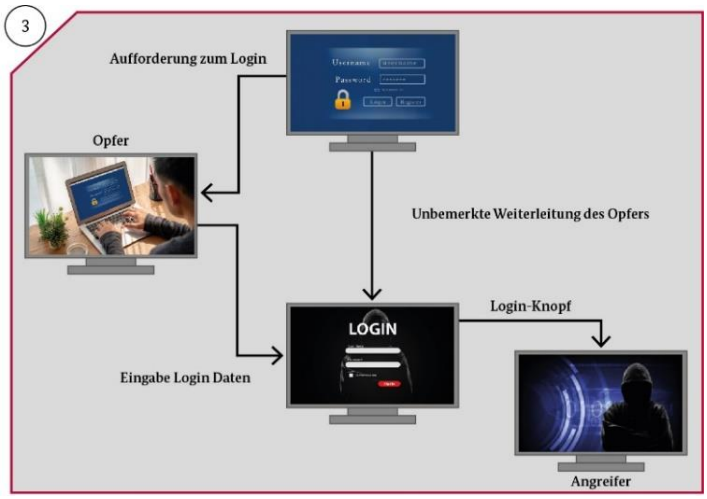
1. Der Akteur Charming Kitten initiiert den Kontakt zum potenziellen Opfer. Zur Steigerung der Erfolgsaussichten des Angriffs werden zunächst zielgerichtete und thematisch passende Nachrichten ohne maliziösen Inhalt verschickt, um eine Vertrauensbasis zu schaffen.



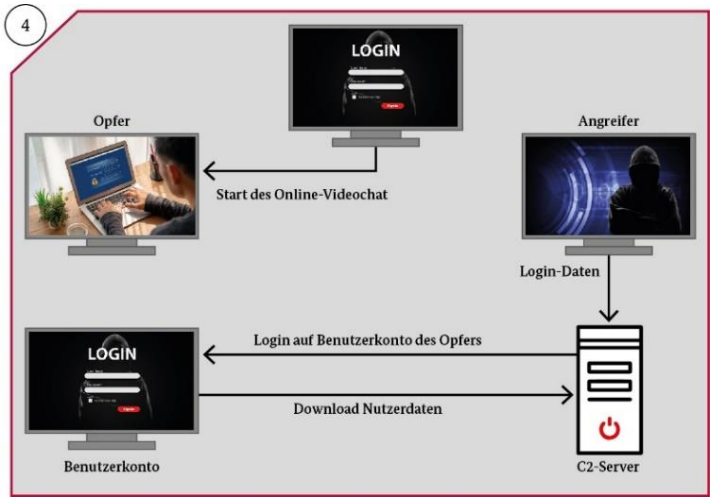
2. Im zweiten Schritt wird durch die Gruppierung Charming Kitten eine Einladung für einen Online-Videochat versendet. Der Link führt zu einer vermeintlich legitimen Webseite eines Online-Dienstanbieters wie Google oder Microsoft. Der Angreifer bedient sich der Möglichkeit, nutzergenerierte Inhalte bei diesen Anbietern zu erstellen. Dadurch enthält der versendete Link eine Weiterleitung zu einer legitimen Seite des genutzten Anbieters. Webseiten wie sites.google.com, drive.google.com oder onedrive.live.com enthalten keine offiziellen Inhalte des jeweiligen Anbieters.



3. Folgt das Opfer dem Link, wird es aufgefordert, sich einzuloggen. Dabei wird es unbemerkt zur maliziösen Webseite des Angreifers weitergeleitet. Auf dieser Phishing-Webseite erfolgt die Eingabe der Zugangsdaten. Möglicherweise folgt die Aufforderung für eine Zwei-Faktor-Authentisierung[6]. Die Bereitstellung des Codes dafür erfolgt durch den tatsächlichen Dienstleister.



4. Sofern im Anschluss ein Online-Videochat stattfindet, dient dieser der Verschleierung des Angriffs. Der Angreifer loggt sich von einem C2-Server[7] in das Nutzerkonto des Opfers ein und ist damit in der Lage, die gesamten Nutzerdaten herunterzuladen, zum Beispiel mittels eines Programms wie Google Takeout.



6 Zwei/Multi-Faktor-Authentisierung*:* Nachweisen der eigenen Identität anhand einer Kombination von Merkmalen gegenüber einem Online-Dienst, z.B. Passwort und Transaktionsnummer (TAN, meist per SMS oder separater App zugestellt).

7 C2-Server (Command & Control): Steuerungsserver, über den die Angreifer mit dem Schadprogramm kommunizieren können.

Weitergehende Formen der Überwachung von Personen, wie die Nachverfolgung von Aufenthaltsorten über mobile Endgeräte, können durch das BfV derzeit nicht bestätigt werden. Der Vollständigkeit halber sei jedoch auf die Eingangs verwiesene öffentliche Berichterstattung verwiesen, nach der die dort beschriebene Schadsoftware teilweise auch das Nachverfolgen der Aufenthaltsorte erlaubt.[8]

Allgemeine und empfohlene Sicherheitsmaßnahmen

Zum Schutz vor den in diesem BfV Cyber-Brief genannten Cyberangriffen empfiehlt das BfV folgende Maßnahmen:

Schutz vor Spear-Phishing

- Behalten Sie bei jeder Kontaktaufnahme von nicht etablierten Kontakten oder ungewöhnlichen Bitten etablierter Kontakte eine gesunde Skepsis.
- Prüfen Sie bei unbekannten Kontakten oder Kontaktaufnahmen die Identität. Vereinbaren Sie zum Beispiel ein Gespräch über einen zweiten, nachweislich offiziellen Kanal. Eine Möglichkeit wäre, ein Telefonat über eine Telefonnummer zu initiieren, die nachweislich zur angegebenen Organisation des Kontakts gehört.
- Prüfen Sie die Absender von E-Mail-Adressen auf Auffälligkeiten. Seien Sie skeptisch, wenn bereits etablierte Kontakte eine Kommunikation über eine unbekannte Adresse führen möchten oder offizielle Anschreiben einer Organisation über eine nicht-offizielle Adresse erfolgen wie die Adresse eines E-Mail-Providers, zum Beispiel gmail.com oder outlook.com.
- Öffnen Sie keine Links, bei denen Sie sich unsicher sind. Achten Sie auf Links mit nutzergenerierten Inhalten wie sites.google.com.
- Sollten Sie sich unsicher sein, ob Sie einen schädlichen Link geöffnet haben, empfiehlt sich die Prüfung Ihrer aufgerufenen Domains. Dazu prüfen Sie die

[8] Siehe FN 3.

Adresszeile Ihres Browsers oder den Verlauf Ihrer besuchten Internetseiten auf ein Vorkommen der in diesem BfV Cyber-Brief aufgelisteten Domains.[9]

Schutz von Onlinediensten

- Nutzen Sie nur offizielle Login-Seiten zur Anmeldung bei Onlinediensten. Machen Sie sich mit der offiziellen Login-Seite der von Ihnen genutzten Onlinedienste vertraut. Gleichen Sie die Adresszeile sowie das Webseitenzertifikat ab und sehen Sie bei Ungereimtheiten von einer Eingabe der Zugangsdaten ab.

- Richten sie eine Multi-Faktor-Authentifizierung bei allen Onlinediensten ein.

- Prüfen Sie für die regelmäßig von Ihnen verwendeten Onlinedienste, ob unbekannte Geräte verknüpft wurden und/oder unberechtigte Zugriffe erfolgt sind. Nehmen Sie Sicherheitsbenachrichtigungen der Onlinedienste ernst und gehen Sie ihnen nach. Ändern Sie im Zweifel kurzfristig Ihre Passwörter.

- Nutzen Sie unterschiedliche Konten von Onlinediensten und trennen Sie beispielsweise private Angelegenheiten von sensiblen Sachverhalten.

Für weitere allgemeine Handlungsempfehlungen zu den Themen Cybersicherheit[10] und Accountschutz[11] verweist das BfV auf die online abrufbaren Sicherheitshinweise des Bundesamtes für Sicherheit in der Informationstechnik in der Rubrik „Sicher im digitalen Alltag“. Darüber hinaus finden Sie zusätzliche Informationen, wie beispielsweise zum Thema „Sicherheit auf Geschäftsreisen“, auf der BfV-Website in den Informationsblättern des BfV Wirtschaftsschutzes.[12] So wird empfohlen, die Mitnahme von privaten Endgeräten bei Reisen in das Ausland, insbesondere in den Iran, abzuwägen.

[9] Vgl. S. 8. Hierbei handelt es sich um eine nicht abgeschlossene Auflistung öffentlich bekannter C2-Server-Domains.

[10] Vgl. „Basistipps zur IT-Sicherheit“, in: www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html, abgerufen am 09.08.2023.

[11] Vgl. „Online-Account schützen“, in: www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Accountschutz/accountschutz_node.html, abgerufen am 09.08.2023.

[12] Vgl. „Informationen ‚Sicherheit auf Geschäftsreisen‘“, in: www.verfassungsschutz.de, abgerufen am 09.08.2023.

Kontakt

Für Informationen zu Bedrohungen durch Spionage und Sabotage, Terrorismus oder gewaltbereiten Extremismus sowie für konkrete Sicherheitsanfragen oder Verdachtsfälle kontaktieren Sie den Bereich Prävention des BfV. Ihre Angaben werden vertraulich behandelt.

Tel.: 030 18792 3322

oder

E-Mail: praevention@bfv.bund.de

Natürlich steht Ihnen auch die Landesbehörde für Verfassungsschutz in Ihrem Bundesland als Ansprechstelle zur Verfügung. Eine Übersichtsliste der Landesbehörden finden Sie auf der BfV-Website unter der Rubrik „Verfassungsschutz“.

Indicators of Compromise (IoCs / IOC)

Art	IoCs	Bemerkung
Angriffs-infrastruktur	beape[.]live	Domain name
	beape[.]live	Domain name
	beasze[.]live	Domain name
	beeasaze[.]top	Domain name
	bnt2[.]live	Domain name
	check-control-panel[.]live	Domain name
	check-reload-page[.]live	Domain name
	cover-home-page[.]xyz	Domain name
	cover-home-panel[.]xyz	Domain name
	direct-view-check[.]live	Domain name
	direct-view-panel[.]xyz	Domain name
	ksview[.]top	Domain name
	load-panel[.]online	Domain name
	node-dashboard[.]site	Domain name
	node-panel[.]site	Domain name
	panel-review-check[.]live	Domain name
	stellar-stable-faith[.]top	Domain name
	view-direct-panel[.]live	Domain name
	view-direct-panel[.]xyz	Domain name
	view-home-panel[.]xyz	Domain name

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
© maxsim | fotolia.com
© ccvision.de
© Clker-Free-Vector-Images | pixabay.com
© AchinVerma | pixabay.com
© Muhammad Ali | freepik.com

Stand
August 2023