Cologne, 10 August 2023

Bundesamt für Verfassungsschutz

BfV Cyber-Brief No. 01/2023

Advisory on cyber espionage against critics of the Iranian regime in Germany

Published by:
Bundesamt für Verfassungsschutz
Cyber Defence
☎ +49 30 18792 3322

Advisory on cyber espionage against critics of the Iranian regime in Germany

In 2022 several IT security service providers reported on APT group[1] Charming Kitten[2], which is said to be involved in spying on Iranian opposition members and Iranians in exile.[3] The cyber attacks were mainly directed at dissident organisations and individuals – such as legal practitioners, journalists or human rights activists – in Iran and abroad.

Based on its current intelligence, BfV assumes that the attacker group Charming Kitten is concretely involved in espionage activities against Iranian individuals and organisations in Germany. To this end, the APT group uses elaborate social engineering[4] and uses online identities that are tailor-made to target victims.

To better protect against such spying attempts, BfV recommends a number of concrete measures that are easy to put into practice.

[1] Advanced Persistent Threat (APT): APT is a term for complex and targeted threats directed at one or several victims. The concrete attacks in the context of these threats are laborately prepared by the attackers, are highly developed (advanced) and carried out over a long period (persistent).

[2] Also known as APT42, Phosphorus, Cobalt Illusion, Yellow Garuda and Mint Sandstorm, among others.

[3] See Mandiant (2022): Ein Profil der Hackergruppe APT42: hinterhältige Akteure und heikle Angriffe (A profile of the hacker group APT42: devious actors and dangerous attacks); URL: https://www.mandiant.de/resources/blog/apt42-charms-cons-compromises, accessed on 9 August 2023, see Proofpoint (2022): Look What You Made Me Do: TA453 Uses Multi-Persona Impersonation to Turn FOMO Into a Cybersecurity Risk; URL: https://www.proofpoint.com/us/blog/threat-insight/ta453-uses-multi-persona-impersonation-capitalize-fomo, accessed on 9 August 2023 and see Certfa Lab (2022): Charming Kitten: “Can We Have A Meeting” URL: https://blog.certfa.com/posts/charming-kitten-canwe-wave-a-meeting, accessed on 9 August 2023.

[4] Social engineering: exploitation of human qualities such as helpfulness, trust, fear of or respect for authority in order to make individuals do certain things.

Background

The cyber group Charming Kitten uses spear-phishing methods to obtain confidential data of its victims. The objective is to gain access to online services such as email accounts, cloud storage services or messenger services used by the potential victim.

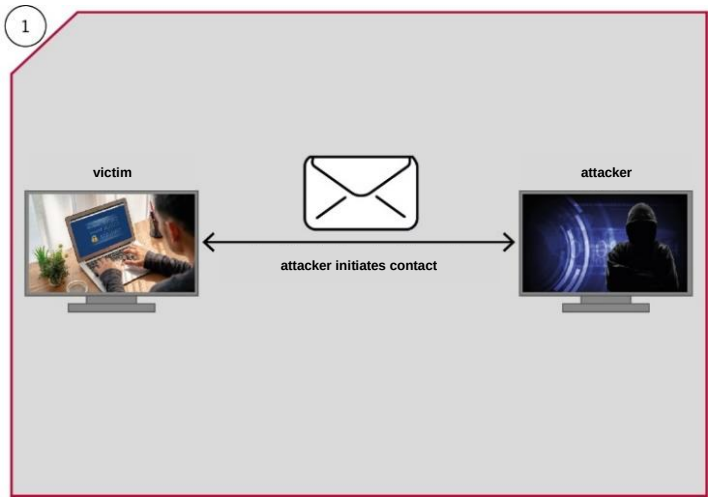
In a first step, the attacker gathers intelligence on the target's preferences and interests, including in the political field. Openly accessible publications on the internet or on social media platforms offer an easy way to obtain personal information.

In a second step, personal contact is established; the attacker attempts to manipulate the victim through social engineering and makes false promises in order to induce incautious behaviour. When a connection has been made and a conversation started, the attacker then sends an invitation to an online video chat. In order to access the video chat, the victim must click on the link supplied. On the log-on screen, the victims enter their log-in data, enabling the attacker access to the online services they use.

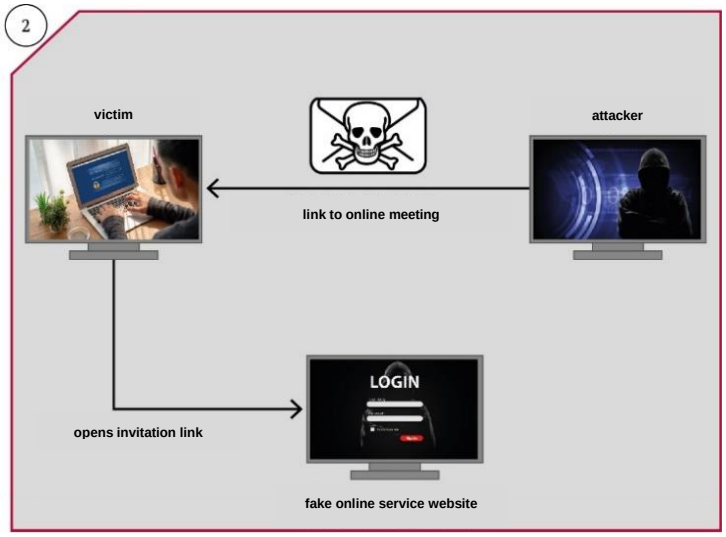
Through the previous social engineering, the attacker group Charming Kitten can establish a seemingly harmless contact in a targeted manner by referring to issues or individuals which are known to the victim or appear legitimate. Charming Kitten's toolkit also comprises email spoofing: Victims are made to believe that they use communicating with real individuals, some of them publicly known, such as journalists or employees of NGOs.

How the spear-phishing attacks work:

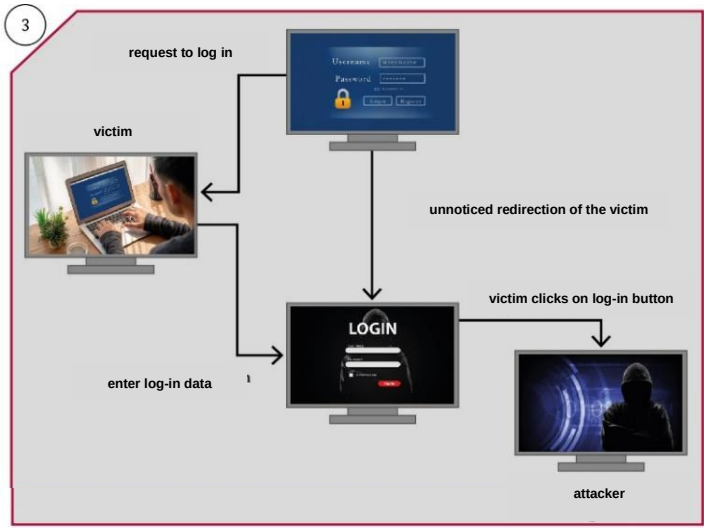
1. Charming Kitten initiates contact with potential victim. At first, targeted messages of non-malicious and relevant content are sent in order to build trust and enhance the attack's prospects of success.



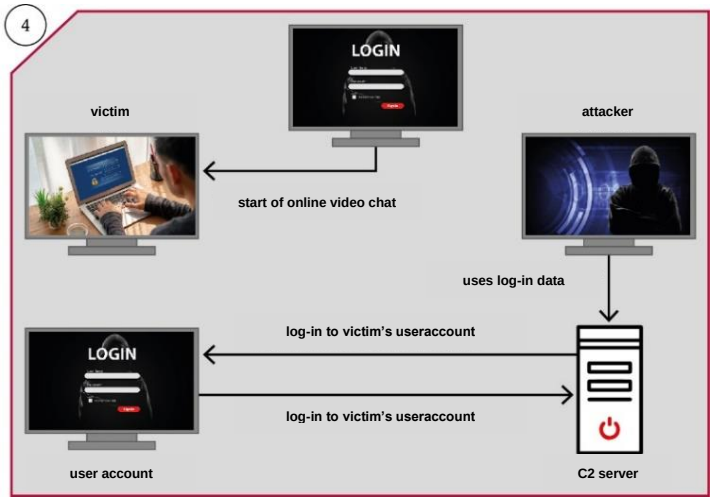
2. In a second step, Charming Kitten sends an invitation to an online video chat. The link leads to a seemingly legitimate website of an online service provider such as Google or Microsoft. The attacker uses the possibilities these providers offer to create user-generated content. Therefore, the link redirects to a legitimate page of the selected provider. Websites such as sites.google.com, drive.google.com or onedrive.live.com contain no official content of the provider.



3. After clicking on the link, the victim is asked to log in. Thereby, it is redirected unnoticed to the attacker's malicious website. The log-in data is entered on this phishing website. In some cases, the victims are asked to use two-factor authentication[5]. The code, however, is supplied by the real provider.



4. If an online video chat occurs, it serves to conceal the attack. After logging in to the victim's user account from a C2 server[6], the attacker is able to download the entire user data, e.g. by means of Google Takeout.



[5] Two-factor/multi-factor authentication: proof of identity to an online service by use of a combination of factors, e.g. password and transaction number (TAN, usually supplied via text message or a separate app).

[6] C2 server (command & control): control server which allows the attackers to communicate with the malware.

General security measures and best practices

For protection against the above mentioned cyber attacks, BfV recommends the following precautions:

Protection against spear phishing

- You should regard approaches by unfamiliar contacts and unusual requests by established contacts with a healthy dose of scepticism.
- In case of unknown contacts or approaches, please verify the contact's identity. For example, arrange communication via a second channel that is provably official. One option could be to initiate a call via a telephone number that can be verified as belonging to the contact's stated organisation.
- Check email addresses for conspicuous details. Be wary if established contacts want to communicate via a new email address or if official letters of an organisation are sent from a non-official email provider address, such as gmail.com or outlook.com.
- Do not open any links of which you are unsure of. Watch out for links with user-generated content, such as sites.google.com.
- If you are unsure whether you have opened a malicious link, you should check your browser history using the attached indicators of compromise.[7]

Protection of online services

- Use only official log-in pages to access online services. Familiarise yourself with the official log-in pages of the online services you use. Check the address bar and the website certificate; in case of inconsistencies, do not enter your access data.
- Set up multi-factor authentication for all online services.
- For the online services you use on a regular basis, check whether unknown devices have been connected and/or whether unauthorised access has

[7] See p. 8.This overview lists public known C2 domains, but it is not closed.

occurred. If your online services send you security alerts, please take them seriously and follow them up. In case of doubt, be quick to change your passwords.

- Use different accounts for different purposes; for instance, keep private matters separate from sensitive ones.

For general recommendations on cyber security and account protection, please refer to the security advice provided by the Bundesamt für Sicherheit in der Informationstechnik (BSI).[8] Furthermore you can find additional information, e.g. on the topic „Business Travel Security“, on the BfV's website. It is recommended that you consider leaving your private devices at home when travelling abroad, especially to Iran.[9]

BfV can currently not confirm that individuals are monitored in further ways, such as location tracing via mobile devices. For the sake of completeness, however, please note that according to public reports, some of the described malware allows attackers to trace their targets' location.

[8] See BSI „Cyber Security Recommendations“, URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html, accessed on 8 August 2023 and see BSI „Protection for Online Accounts“ URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Accountschutz/accountschutz_node.html, accessed on 9 August 2023.

[9] See BfV „Business Travel Security“, URL: https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/prevention/2020-05-25-prevention-travel-security.html, accessed on 9 August 2023.

Contact

For further information about threats from espionage and sabotage, terrorism or violence-prone extremism and in case of concrete security-related questions or cases of suspicion, please contact BfV's section responsible for prevention/economic security. Be assured that your information will always be treated confidentially:

Phone: +49 30 18792-3322

or

Email: praevention@bfv.bund.de

Of course, you can also contact the domestic intelligence service of the German federal state you live in. An overview and contact adresses of these can be found on the BfV's website.

Indicators of Compromise (IoCs / IOC)

Type	IOC	Remarks
attack infrastructure	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

Publication information

Published by
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

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

Date of information
August 2023