January 22, 2023

To whom it may concern

Dear sir/madam,

Re: **Article known as** "Zaupanje v programsko opremo za zaščito pred kibernetskimi napadi" **which was published on January 13, 2023**

Cynet Security Ltd. including any of its affliates (collectively "**Cynet**") respone to the article published at www.telefoncek.si on January 13, 2023 is as followis:

1. **Factual errors** – According to the article, Cynet was founded in Israel but today it is based in the USA. The facts are as follows: Cynet's HQ is **based in Israel** not in the USA. Cynet has a subsidiary in the USA, that distributes its services to customers in the American region.

2. **Misleading suggestions** – According to the article, Cynet is connected to Mr. Shlomo Kramer which was in the past a member of the cyber intelligence unit of the Israeli army, and that such connection can seriously affect the strategic interests of the country in which Cynet's services are installed.

   Cynet **never shares** any information about its customers with any third parties (except to its sub-processors and in accordance with applicable privacy laws (including the GDPR)) including, Mr. Shlomo Kramer and/or any state-controlled agencies of any kind.

   In addition, it should be mentioned most of the leading companies in the cyber security market are "connected" to individuals, which used to work for state controlled cyber units around the world (including USA).

   However, the article decided to make negative suggestion to Israel's cyber intelligence unit and specifically to Cynet and not to other companies from Israel or the world that have similar "connections".

   Accordingly, such a claim is baseless and unjustly makes false suggestions about Cynet's linkage to parties which can negatively affect the interests of any of its customers.

3. **Technical Response**
   a. Claim: Usage of default passwords, implementation of a mandatory change of the default password:
      Response: As many other software and devices (like Routers for example), Cynet also has a default password. This password is only relevant for On-Premise customers and not for SaaS customers. On-Premise customers are advised during on-boarding to change their default password. However, in the article's case, the

environment which was tested by SRLabs was a test environment, and therefore the default password was not changed by the customer, prior to SRLabs tests.

b. **Claim:** Researchers have discovered three security vulnerabilities in the Cynet 360 solution.
Response:
Cynet is a leading cybersecurity vendor receiving high accolades in industry tests (MITRE). However, like other security vendors we do find loopholes in the system and work rapidly to fix them so that our customers are secure.
All vulnerabilities were fixed and deployed promptly for SaaS customers.

We have also released an on-premise version for our non-SaaS customers, most of these vulnerabilities **do NOT allow** remote code execution or modification of the applied settings.

Due the low risk of the vulnerabilities and the prior access that they require, the likelihood of someone actually exploiting these vulnerabilities is negligible.

c. Solution's control servers use self-signed digital certificates

d. Cynet 360 clients on end computers did not check the validity of digital certificates at all

Response to c & d:
We can 100% confirm, that there is no security vulnerability in the communication between Cynet Endpoints to the Cynet SaaS infrastructure. Cynet agents are set to validate the digital certificates they see as part of their communication with the Cynet infrastructure and the digital certificates used by Cynet for communications with the Cynet infrastructure are not self-signed.
By default, all on-premise deployments of Cynet use a technique called “SSL Pinning” to make sure that no man in the middle activity can be achieved, the same goes for our SaaS deployments. However, the reason why the “attack” described in the blog you identified was successful, was because the deployment that they tested in had SSL Pinning disabled due to the customers' tests and the writer of the blog took advantage of this situation.
We reiterate that in the live environment there’s no vulnerability.

e. Cynet 360 application was compiled into binary code on a rather outdated operating system.
Response: The Cynet 360 application is compiled on new, updated, and patched operating system.

Cynet takes pride in providing best in class security to its customers. It also works in co-ordination with other security vendors to keep the cyberspace secure.

In light ofthe above, Cynet requests that you add those clarification to the article no later than January 24, 2023.

Sincerely,

Eran Argov

Legal Counsel