TLP:CLEAR

CENTRE FOR CYBERSECURITY BELGIUM

FLASH REPORT

GOVERNMENT-THEMED PHISHING WITH RDP ATTACHMENTS

CYBER THREAT INTELLIGENCE REPORT

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date: 23 October 2024
Version: 1.0 EN
Author: The Centre for Cybersecurity Belgium

Target audience:
Recipients of the RDP phishing emails.
The campaign targeted governmental entities at the time of writing.

Permitted distribution of TLP:CLEAR:
Recipients can spread this to the world, there is no limit on disclosure.
More information: https://www.first.org/tlp/

Table of Contents

EXECUTIVE SUMMARY

The Centre for Cybersecurity Belgium (CCB) received multiple notifications of a spear phishing campaign targeting national CSIRTs and governmental organisations in Europe.

The attacker poses as the national CSIRTs and uses phishing mails to serve an RDP file as an attachment.

The goal is to acquire access to the victim's local drives. This allows the attacker to manipulate local folders and files of that victim.

When the local drives are exposed using the RDP malware, exfiltration is highly likely and there is an increased risk of serving additional malicious code and achieving persistence

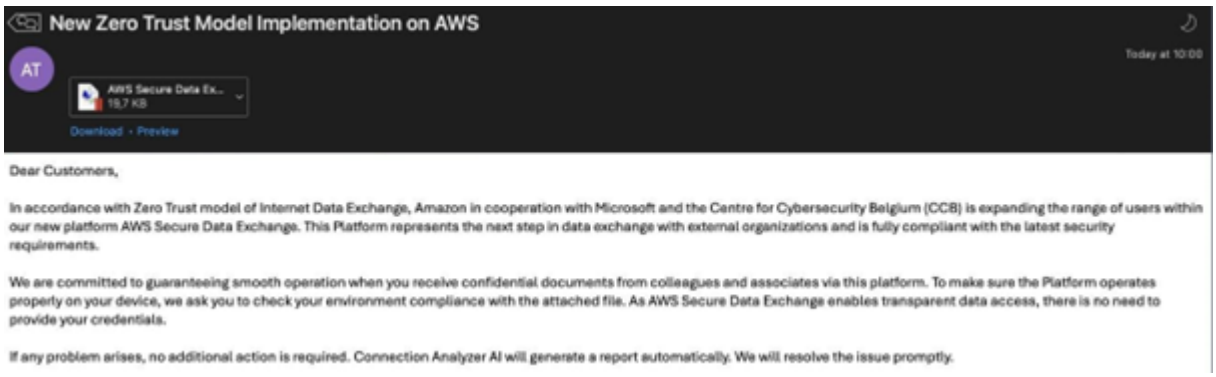

Figure 1: Example phishing email abusing the CCB's name to gain trust.

Modus operandi

Based on multiple notifications:

- The attackers impersonate the national CSIRTs of the targeted organisation, e.g. the CCB for a Belgian organisation.
- The attacker lures the victim with the pretext of a "Cloud Collaboration" effort.
- The phishing email serves a malicious RDP file.
- If the victim opens the RDP file, the local drives will be exposed to the attacker's infrastructure.

Note that these specifics are based on details of a limited dataset.

RECOMMENDATIONS

Spread awareness

The CCB recommends to educate your employees to recognize phishing emails and to always double check the email addresses used by the sender. More information can be found on https://safeonweb.be/en/learn-identify-fake-e-mails.

Monitor or block emails with RDP files attached

The CCB recommends to block incoming emails that contain an RDP file as attachment. If your organisation has seen such emails, review your logs for outgoing RDP connections to suspicious domains.

Consider also blocking other binary files (e.g., exe, com, bat, …).

RDP recommendations

RDP can be used for legitimate purposes. However, administrators need to implement additional protection measures to use RDP securely.

You can find more information on the risks of RDP, as well as on how to secure this protocol, on the website of Safeonweb@work: https://atwork.safeonweb.be/RDP.

Report incidents and threat information

If you encounter a similar incident (or encountered such incident in the past), please notify us by using our reporting form (https://ccb.belgium.be/en/cert/report-incident) or by e-mail (incident@ccb.belgium.be). For urgent cases, you can also reach us by phone on +32 (0)2 501 05 60.

If you have questions or any other information, you can contact us on info@ccb.belgium.be.

REFERENCES

CERT-UA: https://cert.gov.ua/article/6281076

ABOUT THE CCB

The **Centre for Cybersecurity Belgium (CCB)** is the national authority for cybersecurity in Belgium. The CCB supervises, coordinates and monitors the application of the Belgian cyber security strategy. Through optimal information exchange, companies, the government, providers of essential services and the population can protect themselves appropriately.

The Centre for Cybersecurity Belgium (CCB) was established by Royal Decree of 10 October 2014 and operates under the authority of the Prime Minister.

The **CyTRIS (Cyber Threat Research and Intelligence Sharing)** Department of the Centre for Cybersecurity Belgium monitors cyber threats and publishes regular reports. The Team collects, analyses and distributes information on threats, vulnerabilities and attacks on the information and communication systems of Belgium's vital sectors (critical infrastructure, government systems, critical data).

CyTRIS is also responsible for the Early Warning System (EWS). The EWS includes the information exchange platforms of the Belgian CSIRT. CyTRIS is responsible for the operational communication and information exchange with other national CSIRT. CyTRIS also provides the "Spear Warning" procedure. A "Spear Warning" is an individual warning about an infection or vulnerability sent to organisations.

The CCB Connect & Share events, such as the Quarterly Cyber Threat Report (QCTR) events organised by CyTRIS, bring together different stakeholders and consultation platforms at least once a quarter and inform all participants as well as the Organisations of Vital Interest about the active cyber threats. At the QCTR event, the operation of the Early Warning System (EWS) is also discussed. Through this platform, the CyTRIS Team sends pertinent and analysed threat information to national security agencies, Vital Interest Organisations, their sectoral authorities and other partners.

The QCTR is also offered as a webinar and is open to anyone, worldwide (https://app.livestorm.co/ccb?lang=en).