Cybecs Security Solutions
Tampa, Florida

info@cybecs.com
www.cybecs.com
1-844-949-1911

REDROK
Powered by Cybecs

2023

REDROK

USE CASE

”

There are only **two different types** of companies in the world:

those that **have been breached** and know it and those that **have been breached and don’t know it**.

Ted Schlein

ABOUT REDROK

RedRok deploys a strategic solution that explores the structural nature of the organization that taps into the cyclical flow of the evolving nature of risk management, technology, privacy and security.

REDROK

We offer the highest out of the box threat intelligence solution to enable and support business operation.

CUSTOMER USE CASE

Customer use case that highlights the successful implementation of our cyber security tools, Red and Exsight. This case study outlines how Red was used to identify and respond to potential threats, providing valuable insights into the evolving threat landscape.

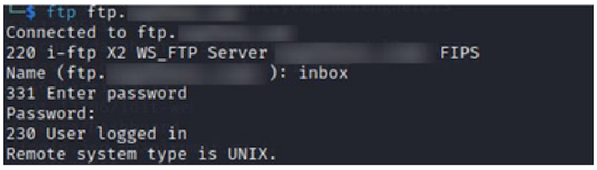
It is important to note that all customer data used in this case study has been anonymized to protect their privacy and confidentiality. Additionally, the information shared in this case study has been limited to what is necessary for the purpose of illustrating the use of Red in detecting and responding to cyber threats.

We hope that this customer use case will provide valuable insights for organizations looking to enhance their cybersecurity posture and stay ahead of the ever-evolving threat landscape.

USE CASE 23.02.2023

We are pleased to share a recent customer use case that highlights the effectiveness of Red, our cutting-edge cyber technologies. In this case, Red was instrumental in detecting a potential cyber threat and helping the organization respond quickly and effectively.

On Saturday, during routine monitoring, our cyber intelligence Red identified leaked FTP credentials along with several high privileged users that belong to one of our customers that had been posted on a dark web forum. The credentials were associated with a client subdomain.

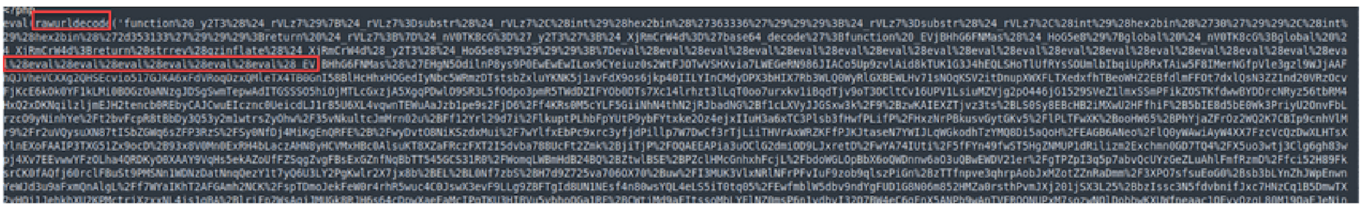


To verify whether the credentials were legitimate, Red used Exsight, our external reconnaissance tool. Exsight used the leaked credential, conducted an in-depth scan of the FTP content, and confirmed that the credentials were indeed valid and associated with the client. Once validated Red immediately alerted the security team to investigate the potential breach.

Further investigation revealed that an unauthorized user had accessed the client's FTP server and had uploaded a malicious file.

The security team was able to quickly remove the file from the FTP server, changed the password to all the leaked accounts and take other necessary actions (which we cannot disclose) to prevent any further damage.

We analyzed the file:



Based on the code we provided earlier, it appears to be a variant of the PHP Shell Trojan. This type of malware allows an attacker to execute arbitrary commands on the compromised server, potentially leading to a complete takeover of the system. After decoding some of the code.

```
se;"><span>Read file:</span><br><input class='toolsInp' type=text name=f><input
type=submit value='>>'></form></td>
        </tr><tr>
                <td><form onsubmit="g('FilesMan',null,'mkdir',this.d.value);retu
rn false;"><span>Make dir:</span> <font color='green'>(Writeable)</font><br><inp
ut class='toolsInp' type=text name=d><input type=submit value='>>'></form></td>
                <td><form onsubmit="g('FilesTools',null,this.f.value,'mkfile');r
eturn false;"><span>Make file:</span> <font color='green'>(Writeable)</font><br>
<input class='toolsInp' type=text name=f><input type=submit value='>>'></form></
td>
        </tr><tr>
                <td><form onsubmit="g('Console',null,this.c.value);return false;
"><span>Execute:</span><br><input class='toolsInp' type=text name=c value=''><in
put type=submit value='>>'></form></td>
                <td><form method='post' ENCTYPE='multipart/form-data'>
                <input type=hidden name=a value='FilesMAn'>
                <input type=hidden name=c value='/Users/user1/'>
                <input type=hidden name=p1 value='uploadFile'>
                <input type=hidden name=charset value='Windows-1251'>
                <span>Upload file:</span> <font color='green'>(Writeable)</font>
<br><input class='toolsInp' type=file name=f><input type=submit value='>>'></for
m><br  ></td>
        </tr></table></div></body></html>logout
```

This file characteristics simulate to Trojan.PHP.Shell.AM which is a type of Trojan horse, a malicious software program that is designed to perform unauthorized and potentially harmful actions on a computer system. In the case of Trojan.PHP.Shell.AM, it is specifically designed to provide remote access to the compromised system by opening a backdoor that allows attackers to execute arbitrary commands and perform various types of malicious activities.
This particular Trojan is designed to run on web servers and targets PHP files. It is typically spread through various means such as phishing attacks, email attachments, and drive-by downloads. Once it infects a system, it can allow attackers to steal sensitive data, such as login credentials and financial information, as well as execute commands on the compromised system.

Additionally, the Trojan may be used to launch attacks against other systems, send spam emails, or perform other malicious activities as directed by the attackers. As such, it is important to take appropriate measures to prevent the spread of such malware, including keeping anti-virus and anti-malware software up to date, using strong passwords and other security measures, and avoiding suspicious email attachments and downloads.

Thanks to the quick detection and response enabled by Red and Exsight, the organization was able to prevent a potentially serious cyber-attack and protect its clients' sensitive information. In summary, this customer use case demonstrates how Red and Exsight can work together to detect and respond to potential cyber threats in real-time. With Red's advanced threat intelligence capabilities and Exsight's external reconnaissance tools, organizations can stay ahead of the evolving cyber threat landscape and protect their valuable data from potential attacks.

REDROK

AI-Powered Threat Management

2023

Powered by Cybecs

Tampa, Florida

Telephone +1-844-949-1911

E-mail: info@cybecs.com