Resurgence of Voicemail-themed Phishing Attacks Targeting Key Industry Verticals in US

zscaler.com/blogs/security-research/resurgence-voicemail-themed-phishing-attacks-targeting-key-industry

Summary

Since May 2022, ThreatLabz has been closely monitoring the activities of a threat actor which targets users in various US-based organizations with malicious voicemail-notification-themed emails in an attempt to steal their Office365 and Outlook credentials. The tactics, techniques, and procedures (TTPs) of this threat actor have a high overlap with a previous voicemail campaign that ThreatLabz analyzed in July 2020.

In this new instance of the campaign, the threat actor has targeted users in US-based organizations in specific verticals including software security, US military, security solution providers, healthcare / pharmaceutical, and the manufacturing supply chain.

As Zscaler was one of the targeted organizations, it gave us a good insight into the full attack chain and motives of this threat actor.

Key points

- Voicemail-themed phishing campaigns continue to be a successful social engineering theme used by this threat actor to lure victims in opening a malicious attachment.
- Multiple key industry verticals in the US such as military, software security vendors, healthcare, pharmaceuticals, and the manufacturing supply chain were targeted by this threat actor.

- The goal of the threat actor is to steal credentials of Office365 and Outlook accounts, both of which are widely used in large enterprises.
- A CAPTCHA is used by the threat actor to guard the final credential phishing page from automated URL analysis algorithms.
- Each URL is specifically crafted for the targeted individual and the targeted organization.
- The campaign is active at the time of publishing this report.

Attack chain

The attack flow involves a voicemail-themed notification email sent to the victim. The email contains an HTML attachment which, when opened, will redirect the user to a credential phishing site. The goal of the threat actor is to harvest Office 365 credentials of the victim.

We will describe each component of the attack-chain in more detail in this report.

Attack chain [Technical analysis]

Email analysis

The email theme is focused on a voicemail notification that tells the victim they have a missed voicemail, promting the user to open the HTML attachment. This social engineering technique has worked successfully for the threat actor in previous campaigns.

Figure 1 shows an example of the email sent to the victim. The "From" field of the email was crafted specifically to align with the targeted organization's name.

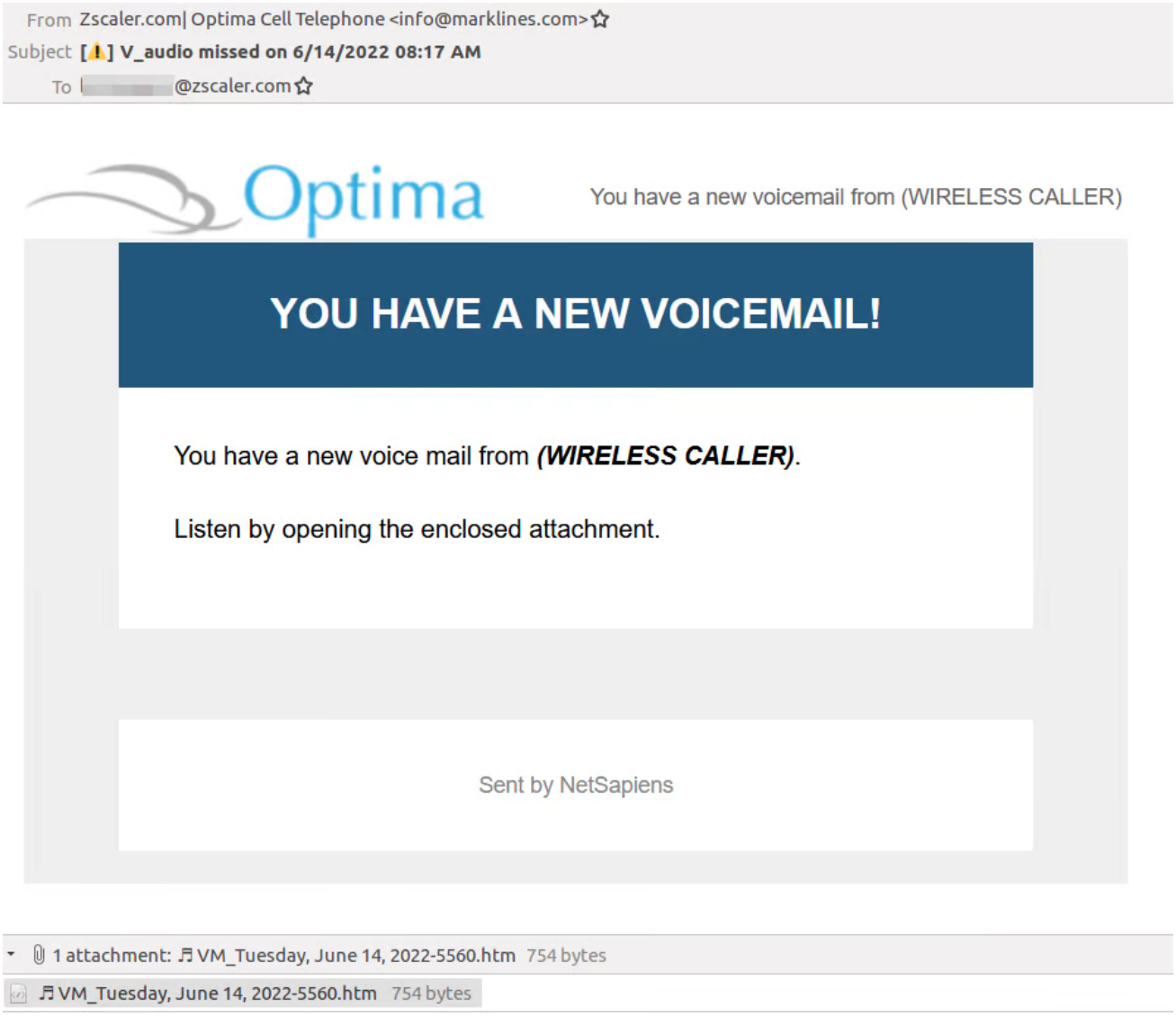

Figure 1: Voicemail-themed email sent to a user at Zscaler

Analysis of the email headers shows that the threat actor leveraged email servers located in Japan. Figure 2 shows the headers for one of the emails.

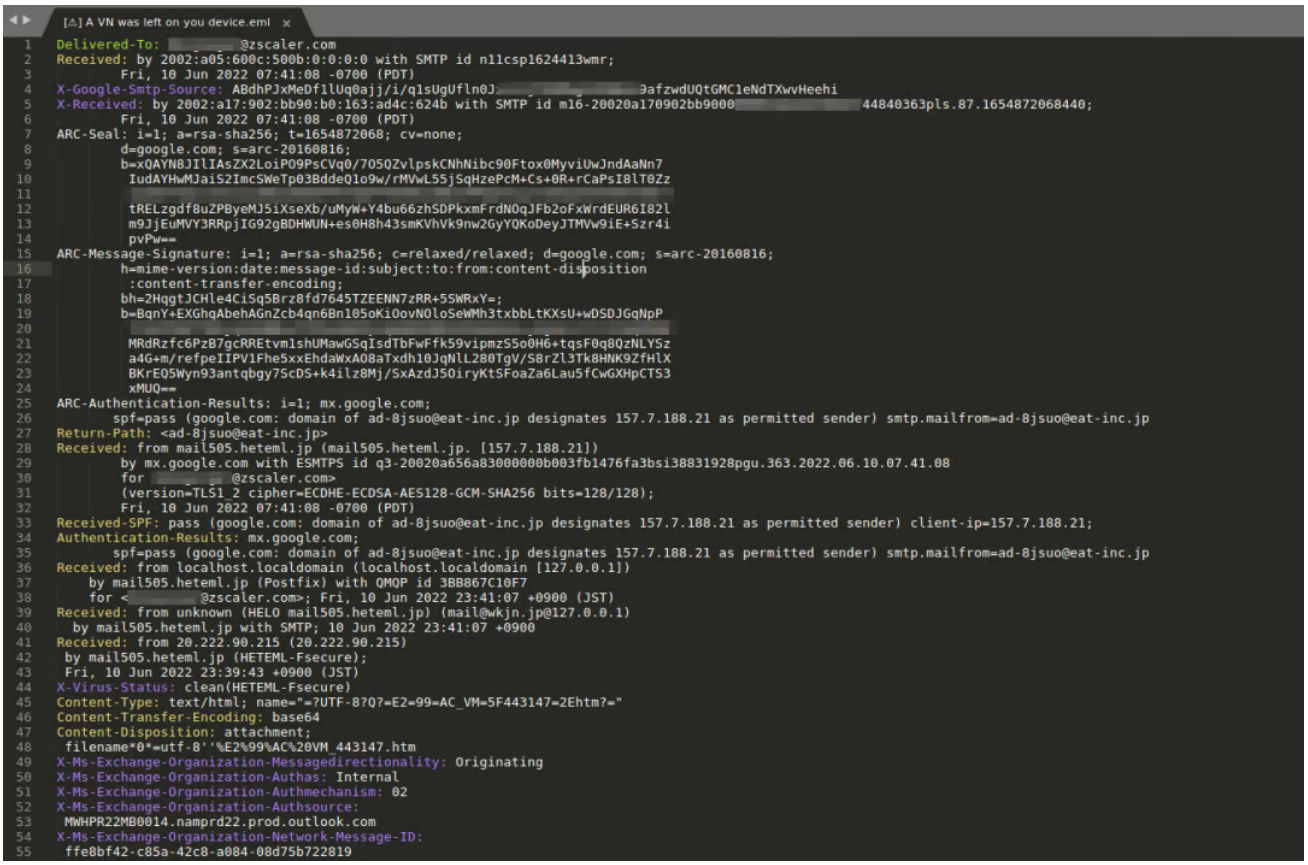

Figure 2: Email header

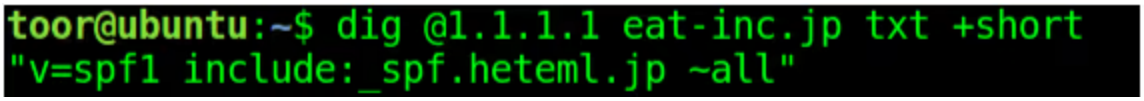

Figure 3: Mail server details

HTML attachment analysis

For the purpose of analysis, we will consider the HTML attachment with the MD5 hash: dd0ddbc951de5cad9c8ace516c514693

Figure 4 shows the HTML attachment sent in the email which contains encoded JavaScript.

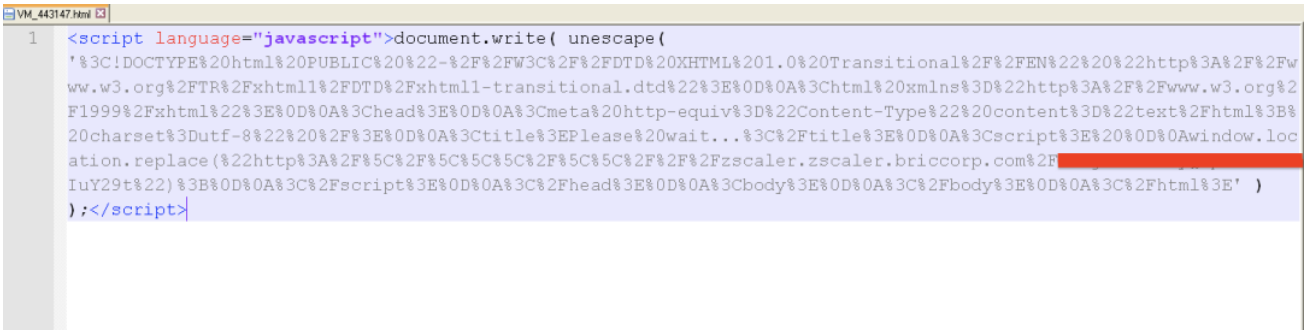

Figure 4: HTML attachment

Figure 5 shows the resulting code after deobfuscation.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "
http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Please wait...</title>
<script>
window.location.replace("http:/\/\\\/\\\///zscaler.zscaler.briccorp.com/[redacted]");
</script>
</head>
<body>
</body>
</html>
```

Figure 5: Decoded JavaScript from the HTML attachment

This code redirects the user to an attacker-controlled URL using window.location.replace()

URL analysis

[Stage-1 URL] - Redirector

The URL inside the HTML attachment is a redirector URL which redirects the user to the final credential phishing page.

In each instance of the attack, the URL followed a consistent format which included the name of the targeted organization as well as the email address of the targeted individual. Figure 6 below highlights the format.

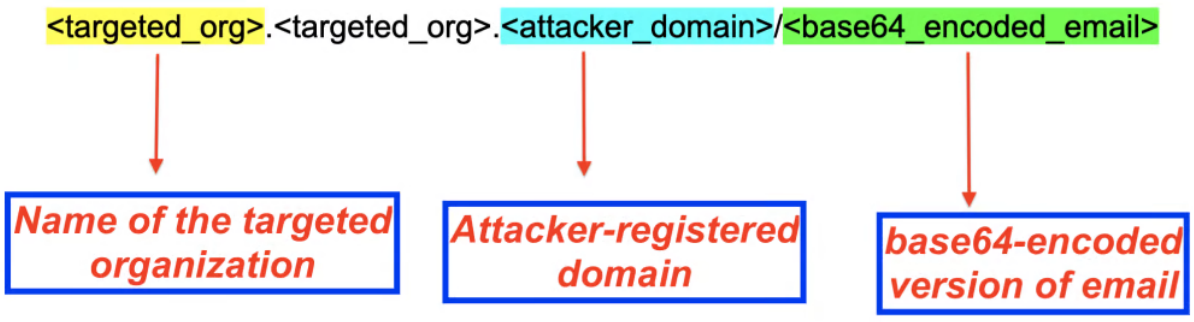

Figure 6: Stage-1 URL format

For instance, when an individual in Zscaler was targeted, the URL used the following format:

zscaler.zscaler.briccorp[.]com/<base64_encoded_email>

Since the format of the URL gives away critical information about the target, we used that information from our collected telemetry to enumerate the list of targeted organizations and individuals.

Based on analysis of this telemetry, we can conclude with a high confidence level that the targets chosen by the threat actor are organizations in the US military, security software developers, security service providers, healthcare / pharmaceutical and supply-chain organizations in manufacturing and shipping.

It is important to note that if the URL does not contain the base64-encoded email at the end; it instead redirects the user to the Wikipedia page of MS Office or to office.com.

[Stage 2 URL] CAPTCHA check

The Stage 1 URL in the HTML attachment will redirect the user to the Stage 2 URL which requires the user to solve a Captcha before presenting the actual Office credential phishing page.

For Captcha, it uses the Google reCAPTCHA technique. This helps the threat actor evade automated URL analysis tools. A similar technique was used in the July 2020 instance of a voicemail-themed campaign.

Figure 7 and 8 show 2 examples of captcha displayed by the Stage 2 URLs.

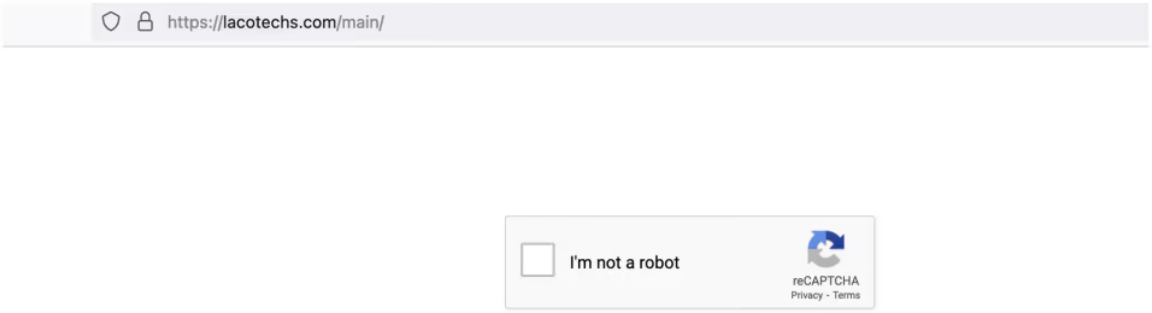

Figure 7: Captcha displayed by the phishing page

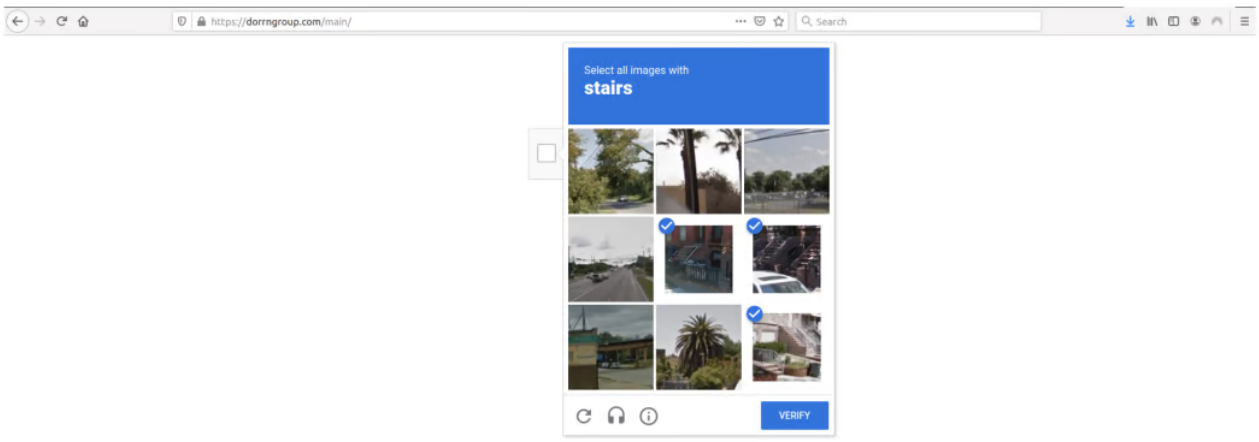

Figure 8: Captcha displayed by the phishing page

[Stage 3 URL] - Credential phishing page

Once the user solves the Captcha successfully, they will be redirected to the final credential phishing page which attempts to steal the Office 365 credentials of the user as shown in Figure 9.

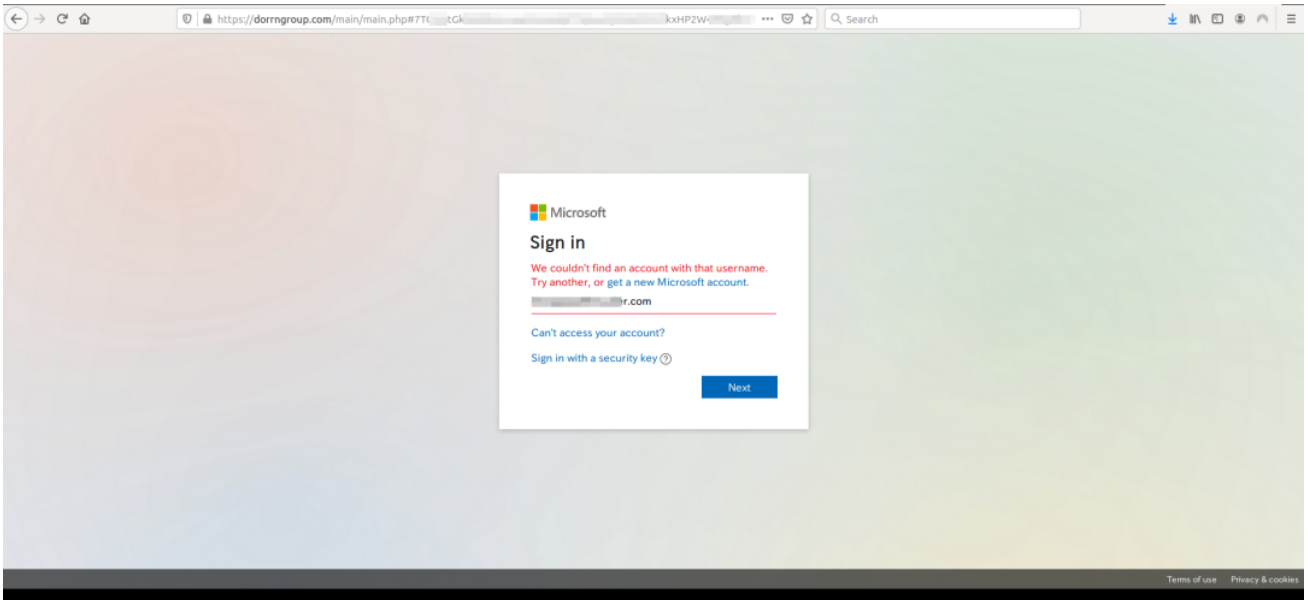

Figure 9: Actual credential phishing page of Office 365

Zscaler's detection status

Zscaler's multilayered cloud security platform detects indicators at various levels, as seen here:

HTML.Phish.Microsoft
HTML.Phish.Office365
HTML.Phish.Zscaler

Figure 10 shows the detection status of Zscaler's credential phishing detection system.

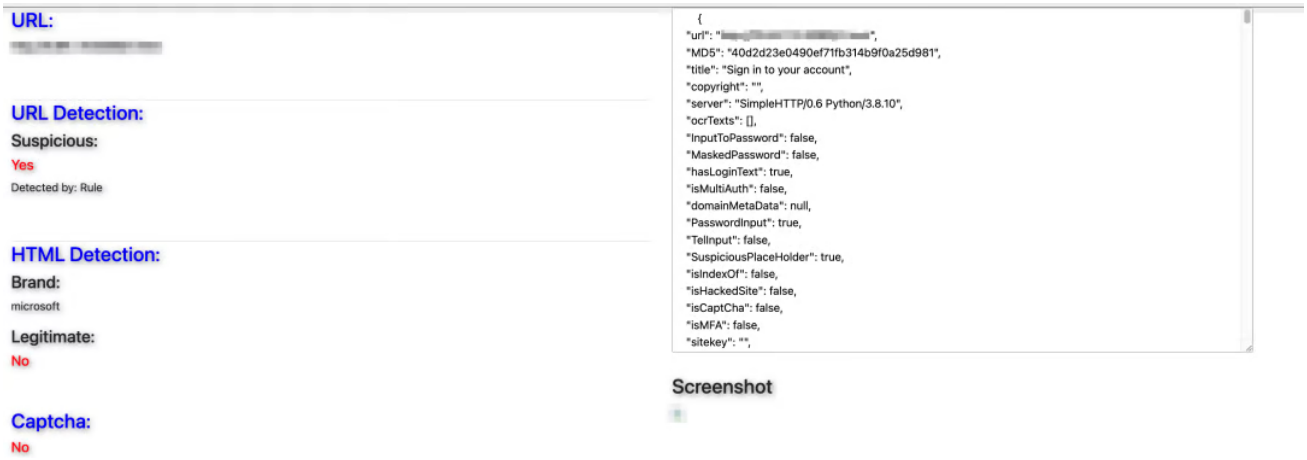

Figure 10: URL detection by Zscaler's credential phishing detection system

Conclusion

Voicemail-themed phishing campaigns continue to be a successful social engineering technique for attackers since they are able to lure the victims to open the email attachments. This combined with the usage of evasion tactics to bypass automated URL analysis solutions helps the threat actor achieve better success in stealing the users' credentials.

As an extra precaution, users should not open attachments in emails sent from untrusted or unknown sources. As a best practice, in general, users should verify the URL in the address bar of the browser before entering any credentials.

The Zscaler ThreatLabz team will continue to monitor this campaign, as well as others, to help keep our customers safe.

Indicators of compromise (IOCs)

attacker-registered domains

briccorp[.]com
bajafulfillrnent[.]com
bpirninerals[.]com

lovitafood-tw[.]com
dorrngroup[.]com
lacotechs[.]com
brenthavenhg[.]com
spasfetech[.]com
mordematx[.]com
antarnex[.]com