М. Д. Кравцов

ATTACKERS USE MORSE CODE IN EVASIVE PHISHING CAMPAIGN

Cybercriminals try to change their schemes as fast as security and protection technologies do. In a targeted, invoice-themed XLS.HTML phishing campaign, attackers tend to change encryption and obfuscation mechanisms from time to time, showing high motivation and skill to constantly deceive detection and keep the credential theft operation working.

Such a campaign demonstrates the present-day email threat: sophisticated, evasive, and endlessly evolving. The HTML attachment is split into several segments, including the JavaScript files used to steal passwords, which are then encoded using various mechanisms. These attackers shifted from employing plaintext HTML code to using multiple encoding techniques, including old and unusual encryption methods like Morse code, to hide these attack segments. Some of these code segments do not even appear in the attachment itself. Instead, they are present in various open directories and are called by encoded scripts.

In effect, the attachment is comparable to a jigsaw puzzle: on their own, the individual segments of the HMTL file may appear harmless at the code level and may thus slip past conventional security solutions. Only when these segments are put together and properly decoded does the malicious intent show.

This campaign's primary goal is to steal usernames, passwords, and–in its more recent iteration–other information like IP address and location, which attackers use as the initial entry point for later infiltration attempts. As I previously noted, the campaign components include information about the targets, such as their email address and company logo. Such details enhance a campaign's social engineering lure and suggest that a prior reconnaissance of a target recipient occurs.

Morse code is an old and unusual method of encoding that uses dashes and dots to represent characters. This mechanism was observed by Microsoft in the February ("Organization report/invoice") and May 2021 ("Payroll") waves.

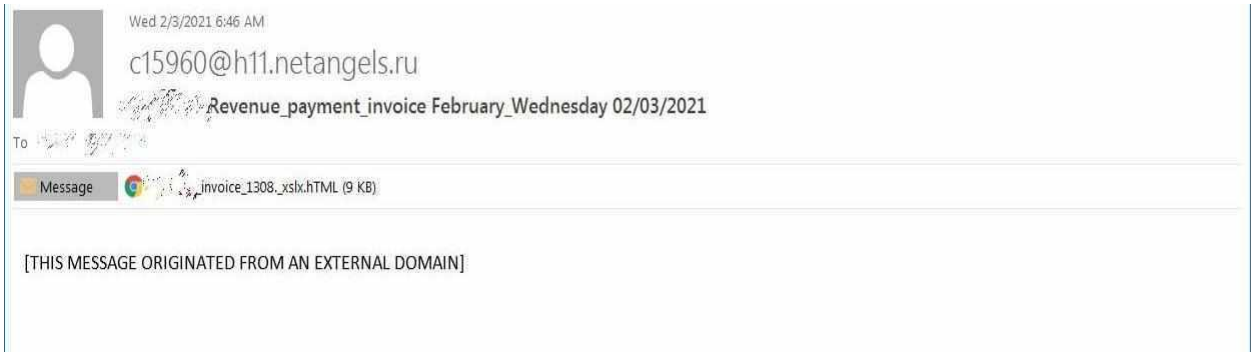
In the February iteration, links to the JavaScript files were encoded using ASCII then in Morse code. Meanwhile in May, the domain name of the phishing kit URL was encoded in Escape before the entire HTML code was encoded using Morse code.

Email-based attacks continue to make novel attempts to bypass email security solutions. In the case of this phishing campaign, these attempts include using multilayer obfuscation and encryption mechanisms for known existing file types, such as JavaScript. Multilayer obfuscation in HTML can likewise evade browser security solutions.

To defend organizations against this campaign and similar threats, Microsoft Defender for Office 365 uses multiple layers of dynamic protection technologies backed by security expert monitoring of email campaigns. Rich email threat data from Defender for Office 365 informs Microsoft 365 Defender, which provides coordinated defense against follow-on attacks that use credentials stolen through phishing. Microsoft 365 Defender does this by correlating threat data from email, endpoints, identities, and cloud apps to provide cross-domain defense.

A later targeted phishing campaign includes the novel obfuscation technique of using Morse code to hide malicious URLs in an email attachment. Here, each letter and number is encoded as a series of dots (short sound) and dashes (long sound).

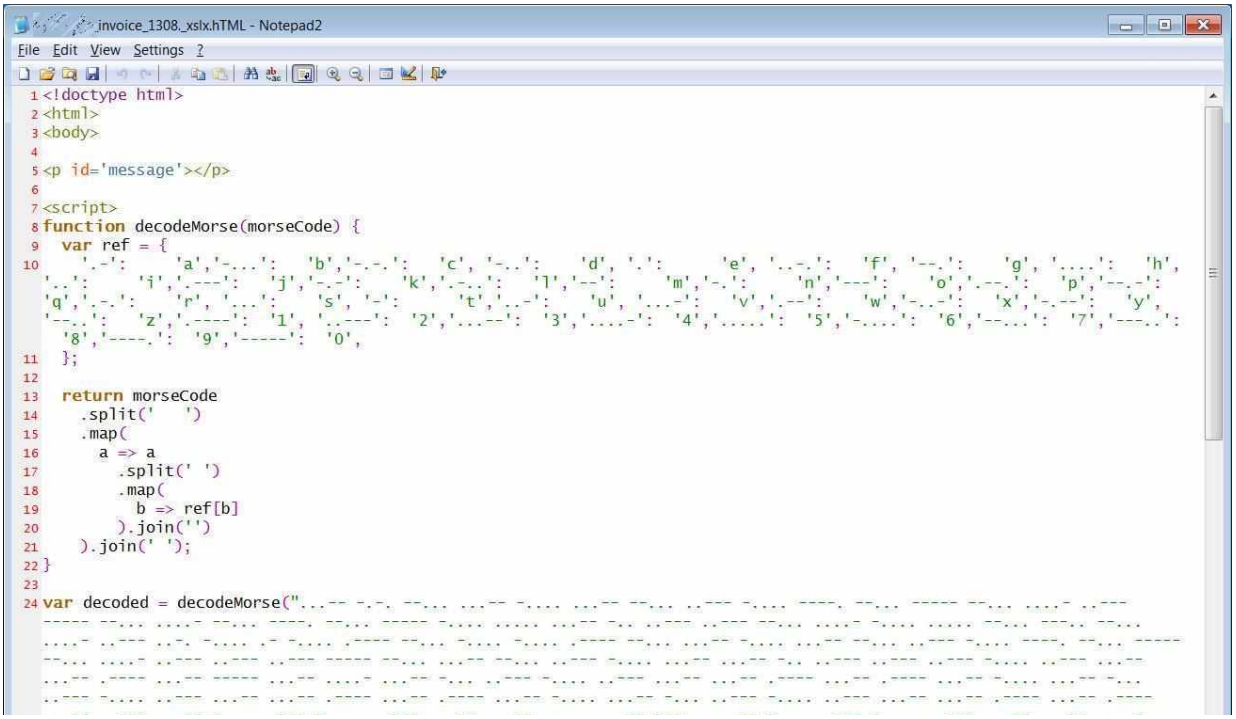
The phishing attack starts with an email pretending to be an invoice for the company with a mail subject like ‘Revenue_payment_invoice February_ Wednesday 02/03/2021.’ (picture 1)



Pic. 1. Phishing email

This email includes an HTML attachment named in such a way as to appear to be an Excel invoice for the company. These attachments are named in the format ‘[company_name]_invoice_[number]._xlsx.hTML.’

When viewing the attachment in a text editor, you can see that they include JavaScript that maps letters and numbers to Morse code. For example, the letter ‘**a**’ is mapped to ‘**.-**‘ and the letter ‘**b**’ is mapped to ‘**-...**’, as shown below. (picture 2)



Pic. 2. Source code HTML phishing attachment

The script then calls a decodeMorse() function to decode a Morse code string into a hexadecimal string. This hexadecimal string is further decoded into JavaScript tags that are injected into the HTML page.

These injected scripts combined with the HTML attachment contain the various resources necessary to render a fake Excel spreadsheet that states their sign-in timed out and prompts them to enter their password again.

Once a user enters their password, the form will submit the password to a remote site where the attackers can collect the login credentials.

This campaign is highly targeted, with the threat actor using the logo.clearbit.comservice to insert logos for the recipient's companies into the login form to make it more convincing. If a logo is not available, it uses the generic Office 365 logo, as shown in the image above.

Phishing scams are becoming more intricate every day as mail gateways become better at detecting malicious emails.

Due to this, everyone must pay close attention to URLs and attachment names before submitting any information. If something looks at all suspicious, recipients should contact their network administrators to investigate further.

As this phishing email uses attachments with double-extension (xlxs and HTML), it is important to make sure that Windows file extensions are enabled to make it easier to spot suspicious attachments.