International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 5, May 2020||

Modernized Homoglyph URL Attack by Hackers to Steal User Credentials

Urvesh Thakkar

Cyber Security Researcher, Cyber Crime Investigator, Founder, and President at Anti Cyber Crime Society, Pune, India

ABSTRACT: With an increase in digital communication and sharing, there is also a rapid increase in social engineering attacks such as Phishing. Bad actors are coming up with new attack surfaces at a rapid rate. These attacks are so sophisticated that any person can be easily targeted and exploited. These days, awareness is increased regarding URLs for websites. With this, a greater number of users are now cautious and alert about fake-looking URLs that can steal personal information and credentials. Above all, hackers are now using a new attack strategy for targeting online users for stealing credentials. In a Homoglyph URL attack, a normal letter associated with an ASCII value is replaced by a Cyrillic alphabet.

KEYWORDS: Phishing attacks, Social Engineering, Homoglyph Attack

I. INTRODUCTION

Similar words are often called as synonyms. Similarly, characters i.e. numbers are letters that are look-alike are called homoglyphs. Consider the example, 'a' and 'а' looks the same, but 'а' belongs to the latter to Cyrillic. For the naked eye, while it is extremely difficult to determine the difference between the two, in the case of computers it gets interpreted in an entirely different meaning. Homographs are two words, that look the same but are entirely different.

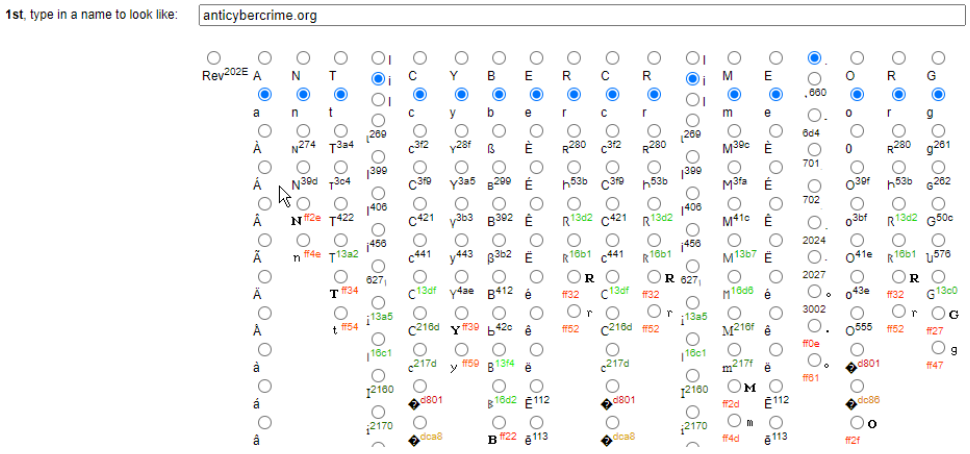
For example, consider the word “wave” is and written the same but resembles completely different meanings depending upon the context used. It can mean a hand wave we generally do as a form of action; on the other hand, it also resembles a water wave. Here is a real-time example, consider these two URLs ‘ijircce.com’ and ‘ijircce.com’. At first glance, both URLs look the same but the former URL is a homoglyph URL that lands nowhere. All the attacker needs are a homoglyph URL generator and some credits for purchasing the homoglyph domain.

Homoglyph URL attacks are so unique that even if a user is aware of cyber-attacks still, he/she can be exploited easily.

II. REQUIREMENTS AND FUNCTIONING

Executing a homoglyph attack is no rocket science. Any bad actor having basic knowledge and familiarity with homoglyph attacks can easily perform it and target a large number of users. There are various methodologies in which homoglyph URLs can be used to target legitimate sites and acquire sensitive information. The most common method in which the attack is carried is using an online homoglyph generator. The following are the steps:

Step 1: We used the following online homoglyph generator: http://www.irongeek.com/homoglyph-attack-generator.php
Step 2: Enter your target URL in the box and choose from a range of ways to represent every letter in the output URL.



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 5, May 2020||

In the above example, we just replaced ‘a’ in our URL. Bad actors make small changes to make the URL look legitimate and better.
Step 4: After making the changes, click on submit and boom, you just created a homoglyph URL.

As mentioned above, a homoglyph attack is the easiest to generate but sadly, it is less known to the digital users and there is a lack of awareness. Now the attacker will use the above URL to host a phishing page or any website that forces you to install the malware in your systems. With an increase in the number of websites, domain registration has become much cheaper. Any bad actor can easily use this homoglyph attack and register a malicious homoglyph URL with a budget of less than 15$.
Not only online tools, that need a manual selection of characters to replace, but various tools can also automate the process and generate a homoglyph URL for any website that we choose. In the example below, we will look at how Evil-URL tool can be used to automatically generate homoglyphs. The tool can run easily on Linux systems and can also run on other OS, with just minimum prerequisites to install.

Step 1: We need to clone the Evil-URL tool repository from GitHub.
The following is the official tool repo: https://github.com/UndeadSec/EvilURL

Step 2: Once everything is set, this tool requires python as a prerequisite for usage. Once done, the tool can be used and as shown in the below image, it asks for entering a URL for which we need a homoglyph.

Step 3: Once the target website is entered, it will then ask to select the domain level such as .com, .net, etc.

Step 4: The tool will automatically replace characters in the URL and will generate a homoglyph domain.
The image below represents the homoglyph URLs generated. Moreover, it not only just generates a homoglyph but also specifies the character replaced and gives more than two to three homoglyph URL possibilities.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 5, May 2020||

```
[*] Char replaced: w
[*] Using Unicode: Cyrillic Small Letter We
[*] Unicode number: w
[*] Evil url: http://www.ijircce.com
------------------------------


[   MORE EXTENSIVE EVIL URL:   ]

[*] Char replaced: c, e, o, p, w.
[*] Using Unicode: Greek Lunate Sigma Symbol, Cyrillic Small Letter Ie, Cyrillic Small Letter O, Cyril
lic Small Letter Er, Cyrillic Small Letter We.
[*] Unicode number: c, e, o, p, w.
[*] Evil url: http://www.ijircce.com
------------------------------
```

Now this generated homoglyph can be registered as a domain and can be hosted as a phishing site or any malicious website.

III. CASE STUDIES AND INDUSTRIAL IMPACTS

It is quite often that these kinds of sophisticated attacks are so simple to generate that already many famous websites are already targeted in the past.

JET AIRWAYS CASE STUDY:

Jet Airways, a well-known airline was impacted by the homoglyph URL attack. Users were receiving messages on their WhatsApp claiming that "Jet airways Airline is giving 2 free tickets to everyone, to celebrate their 25th Anniversary, click here to get yours: http://jetairways.com/tickets"

There is a strong chance, that users won't be able to notice the homoglyph change. The letter 'i' is replaced. The result of this message was that Jet Airways had to release an official disclaimer stating regarding such links. The number of users that were affected is still a mystery. Also, when this attack increased at a higher rate, the airline had to file a complaint to terminate the link. Attackers often lure users in these kinds of special prizes and claim to steal confidential information.

DMART PHISHING

This is one of the most recent phishing scams. DMART is renowned and well famous in India, having more than 200 stores across India. During the recent lockdown period, DMART was providing food and grocery supply to the residents at their doorsteps. As a result of which, the popularity was increased in a tremendous amount. Bad actors took advantage of this opportunity and targeted many users via phishing.

This scam also had the same intent, to lure users in the name of offers, etc.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 5, May 2020||

The viral message stated "D-Mart is giving FREE INR 2,500 shopping voucher to celebrate its 17th anniversary, click here to get yours: http://www.dmart?ndia.com/voucher Enjoy" Again in this case, the character 'i' was replaced and using this homoglyph URL the attack was carried out.

IV. MITIGATION AND CONCLUSION

Using these kinds of tricks, users often tend to lose their sensitive information and security. The point is, can these kinds of attacks be prevented? There are certain ways in which users can prevent being a trap of homoglyph attack. Out of all the prevention steps, one the major preventive measure is self-awareness. Users should be aware of these kinds of attacks and URLs. Some of the awareness points include:

- Never believe on any link, claiming to provide you free offers. These kinds of luring sites are forwarded on social media such as WhatsApp and at times also in Emails.
- Carefully observe the URL of the website and then proceed. Evil-URL tool, as mentioned above, can not only generate homoglyphs but there is also an option to detect them. So, if you feel something is wrong, you can also cross-check using the tool.
- Even if you mistakenly visited such a malicious website, that potentially attacked your credentials, immediately change your password and enable two-factor authentication.
- There are various SSL server test websites such as www.ssllabs.com/ssltest - these sites assign grades to the webservers by analysis. If on any site, the grade is less than "A", do not click on the URL.
- Stay alert when you see a shortened URL, bad actors use this trick to make the attack look more legitimate.

Homoglyphs are nothing but a unique way to confuse the users and play mind tricks. These kinds of attacks resulting in manipulation of the human mindset are called Social Engineering attacks. A Homoglyph attack is one of them. The most common way to stay away from these threats is to be aware and stay alert. Safe browsing, only sharing emails to legit sites, etc. Thankfully, defence systems are rapidly improvising themselves to detect these kinds of attacks at a certain level, users also play an important role if they are aware.

REFERENCES

1. https://blog.blazeinfosec.com/what-you-see-is-not-what-you-get-when-homographs-attack/
2. https://www.esds.co.in/blog/jet-airways-phishing-attack/
3. https://www.anticybercrime.org
4. https://www.esds.co.in/blog/d-mart-phishing-attack/#sthash.tCX4KyVk.dpbs
5. https://blog.malwarebytes.com/101/2017/10/out-of-character-homograph-attacks-explained/

BIOGRAPHY

Urvesh Devendra Thakkaris a Security Researcher and cybercrime investigator. He holds an experience of more than 4 years in the cybersecurity industry. He is president at the Anti Cyber Crime Society. His areas of research are Social Engineering, Windows Exploitation, Android Exploitation, OSINT, and digital forensics. He was also awarded with Global Cyber Crime Helpline Award – as Fortune Hunter of Digital India. He also has keen interest in study of Cyber Psychology.