IMAGE: KLAYSWAP, THE RECORD

Catalin Cimpanu | February 14, 2022

KlaySwap crypto users lose funds after BGP hijack

Cybercrime News Technology

Hackers have stolen roughly $1.9 million from South Korean cryptocurrency platform KLAYswap after they pulled off a rare and clever BGP hijack against the server infrastructure of one of the platform's providers.

The BGP hijack—which is the equivalent of hackers hijacking internet routes to bring users on malicious sites instead of legitimate ones—hit KakaoTalk, an instant messaging platform popular in South Korea.

The attack took place earlier this month, on February 3, lasted only for two hours, and KLAYswap has confirmed the incident last week and is currently issuing compensation for affected users.

How the hack took place

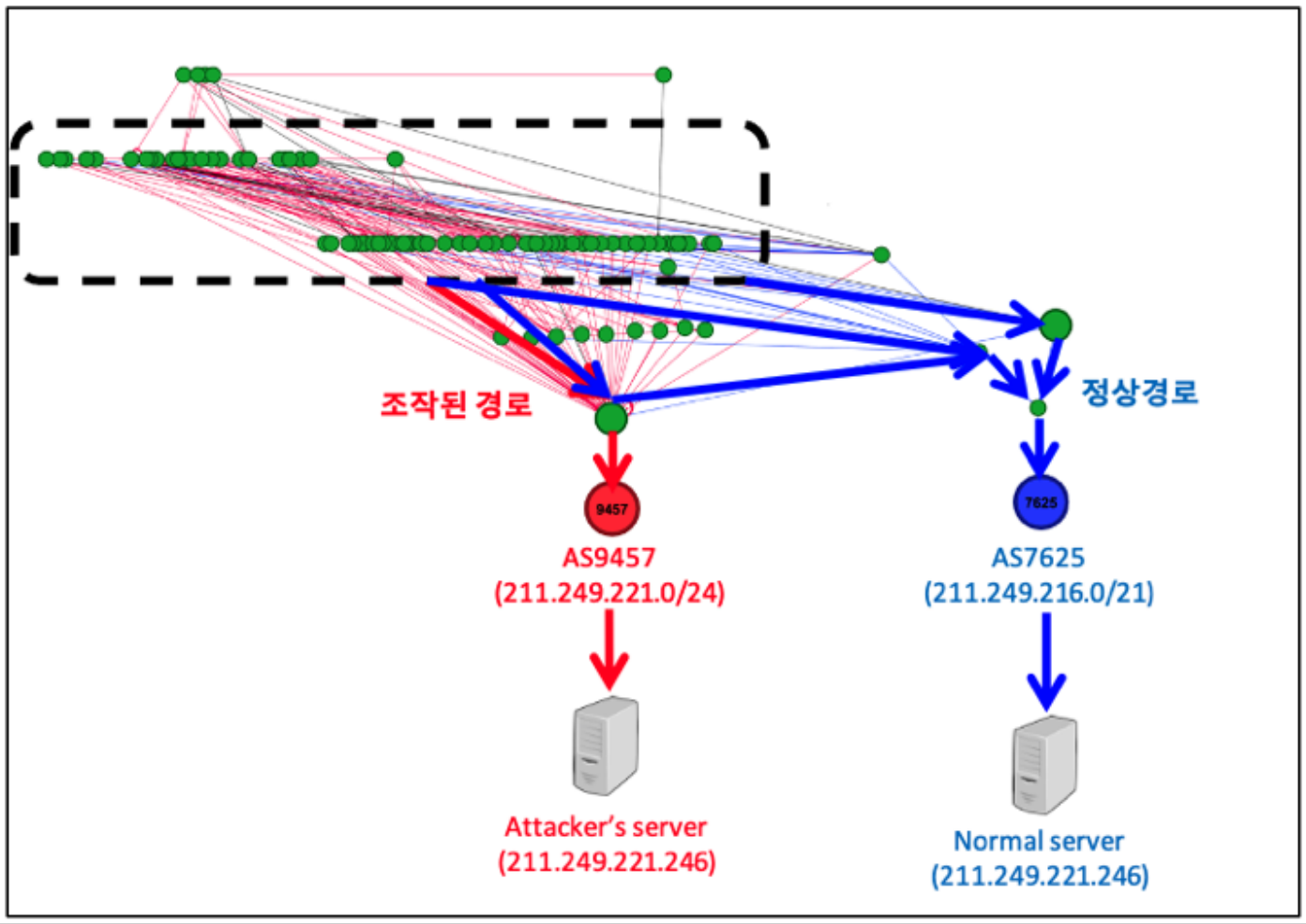
But the incident itself is very different from how most cryptocurrency platforms are getting hacked. Most cryptocurrency heists these days happen after attackers compromise the account of an employee or compromise the platform's code to steal funds from victim accounts.

The KLAYswap attack is different because it didn't target KLAYswap itself, but the server infrastructure of KakaoTalk, a service the platform was using for marketing and as a way of communicating with users during tech support operations.

Planned months in advance, the attackers used an autonomous system (AS), which is a "fictitious" internet entity used by companies who own their own IP address spaces, such as telecoms, data centers, hosting providers, or software companies.

The purpose of an AS is to "advertise" internet routes to tell other AS-es what IP address spaces they own and what domains can be found hosted on their property. At a technical level, this is done via BGP (Border Gateway Protocol) routes, which ASes constantly send to each other.

Using a rogue AS known as **AS9457**, on February 3, the attackers began advertising that they owned the IP addresses that served **developers.kakao.com**, which was part of KakaoTalk's developer infrastructure and where the company hosted its official Kakao SDK (software development kit), which third-party apps would use to integrate with its services.



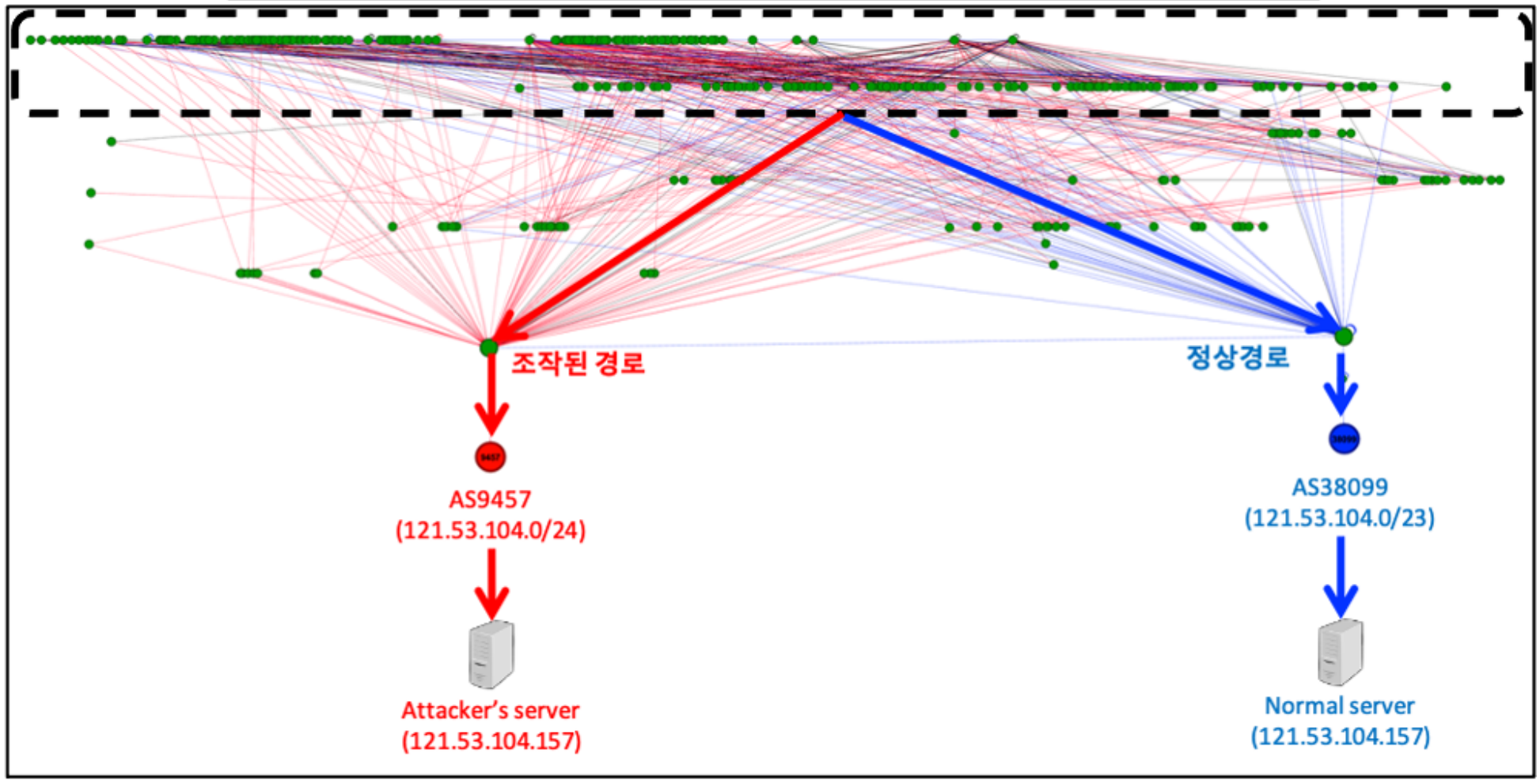


IMAGE: S2W

In a report published last week, South Korean cybersecurity firm S2W said that the attackers used a BGP hijack as a way to serve a malicious version of KakaoTalk's JavaScript SDK file, namely:

https://developers.kakao.com/sdk/js/kakao.min.js

Users who wanted to load this file from the official Kakao developer site received a version from the attacker's servers.

But S2W said this file was modified to include additional code at the end of the file that, once loaded inside a user's browser, would wait for them to initiate a transaction on the KLAYswap website, such as an asset deposit, swap, or withdrawal.

Once an operation was detected, the code would hijack the funds and send the user's assets to an attacker-controlled wallet, from where the funds would be immediately laundered through OrbitBridge and FixedFloat, two cross-blockchain conversion services.

KLAYswap said that during a period of two hours—from 11:30 to 1:30, on February 3—the attacker stole the equivalent of 2.2 billion of Korean won (~$1.9 million) worth of various cryptocurrency assets.

"At the time of the issue, it is understood that 407 abnormal transactions occurred in a total of 325 [customer] wallets," KLAYswap said last week.

Malicious code was delivered to KLAYswap users only

S2W said the attackers stopped the BGP hijack on their own as own, and to avoid triggering warnings with other sites where the Kakao SDK JavaScript file was used, they added a filtering system that delivered the malicious version only for users of the KLAYswap service.

Since it's unclear what level of access the attackers may have to customer accounts, KLAYswap is currently advising users to deauthorize its service's access to customer wallets, move funds to new wallet addresses, and re-sync with the service after that operation is completed.

The company is also advising users to reset their browser cache, just in case their browsers may serve a locally-stored version of the Kakao SDK that still contains the malicious code.

The incident also marks the third time that a BGP hijack has been used to go after a cryptocurrency service.

The first incident of this kind took place in 2014 when a threat actor hijacked the BGP routes for various cryptocurrency mining services, while the second incident took place in 2018 when a threat actor hijacked the website of crypto-wallet service MyEtherWallet.

BGP attacks are rare because they are hard to pull off at a technical level, requiring a deep understanding of the relations between different AS-es, and are typically detected right away when services start announcing new BGP routes they haven't announced before.

Tags BGP · BGP hijack · cryptocurrency · cryptocurrency heist · DeFi · KakaoTalk · KLAYswap · South Korea

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

Previous article

Next article

BRIEFS

Panasonic: February ransomware attack only affected Canada branch | April 12, 2022

F5 investigating reports of NGINX zero day | April 11, 2022

BlackCat ransomware group claims attack on Florida International University | April 11, 2022

WonderHero game disabled after hackers steal $320,000 in cryptocurrency | April 7, 2022

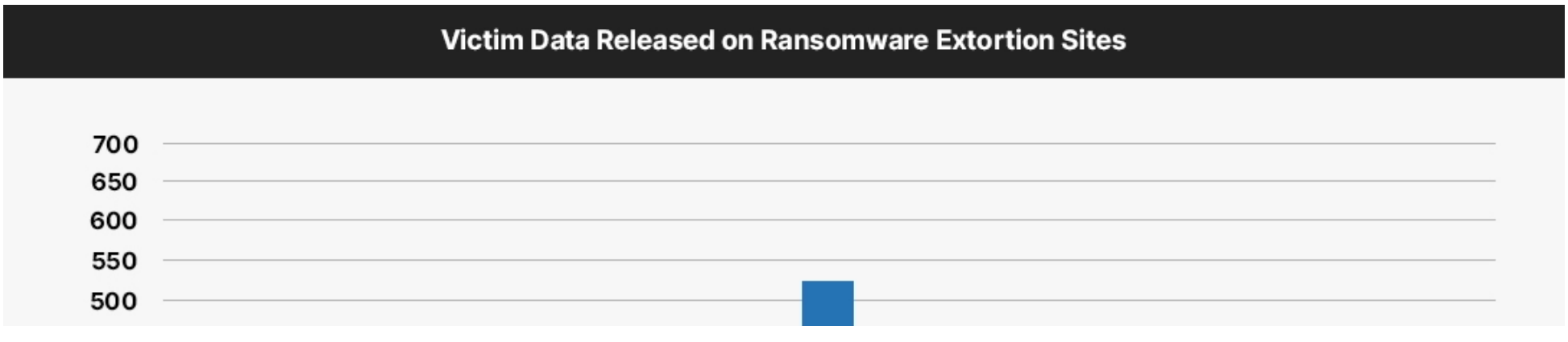
Researcher finds cryptomining malware targeting AWS Lambda | April 6, 2022

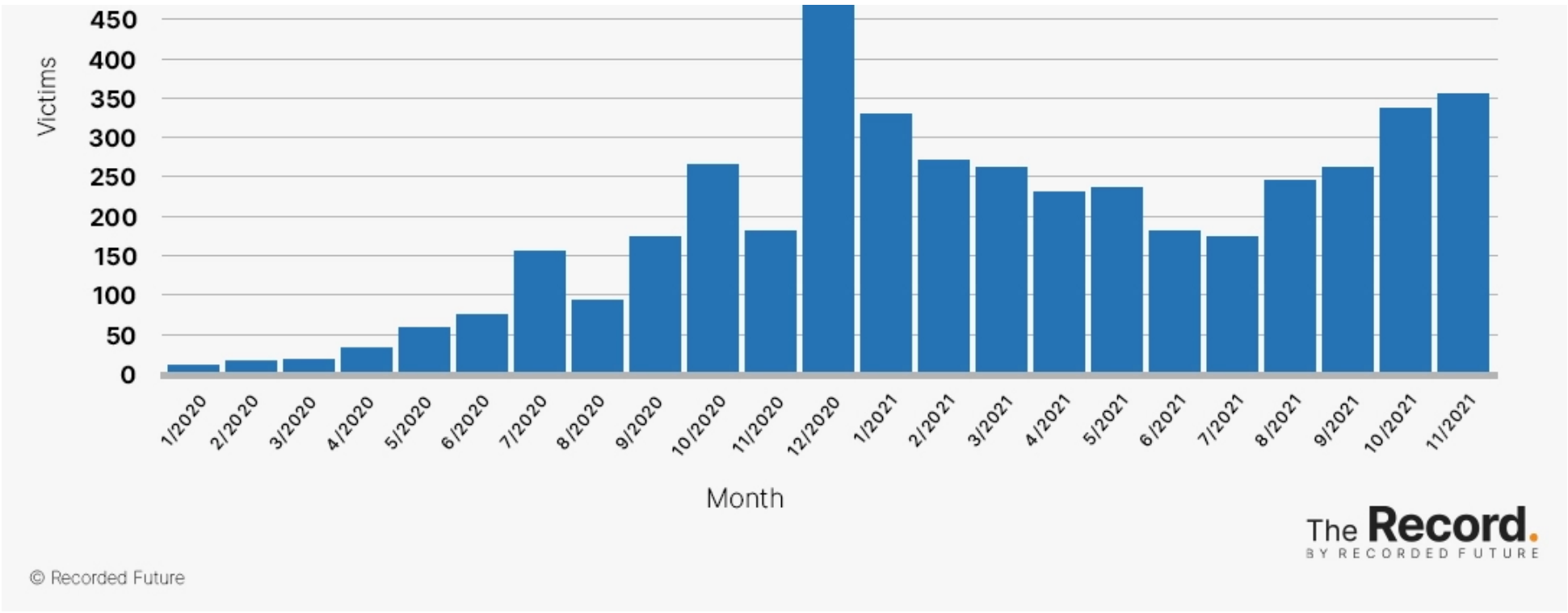
Block says former Cash App employee accessed data from US customer accounts | April 6, 2022

Ukrainian CERT details Russia-linked phishing attacks targeting government officials | April 5, 2022

German wind turbine maker shut down after cyberattack | April 4, 2022

RANSOMWARE TRACKER: THE LATEST FIGURES [MARCH 2022]





RANSOMWARE TRACKER: THE LATEST FIGURES [MARCH 2022]