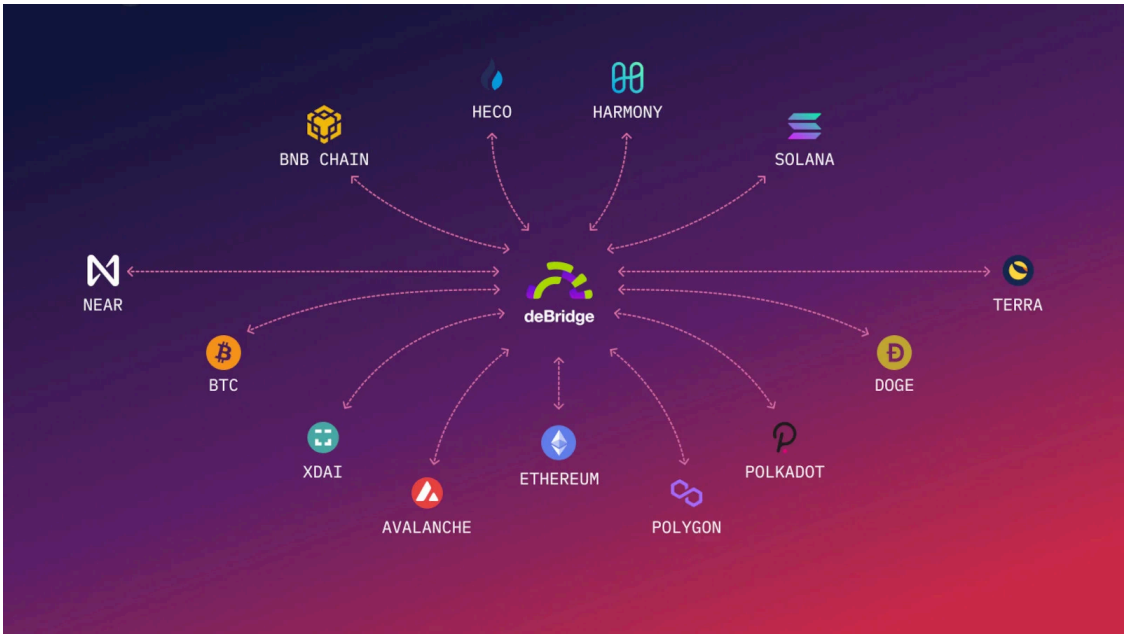
deBridge Finance crypto platform targeted by Lazarus hackers

By Ionut Ilascu

Published: 2022-08-08 · Archived: 2026-04-05 13:27:30 UTC



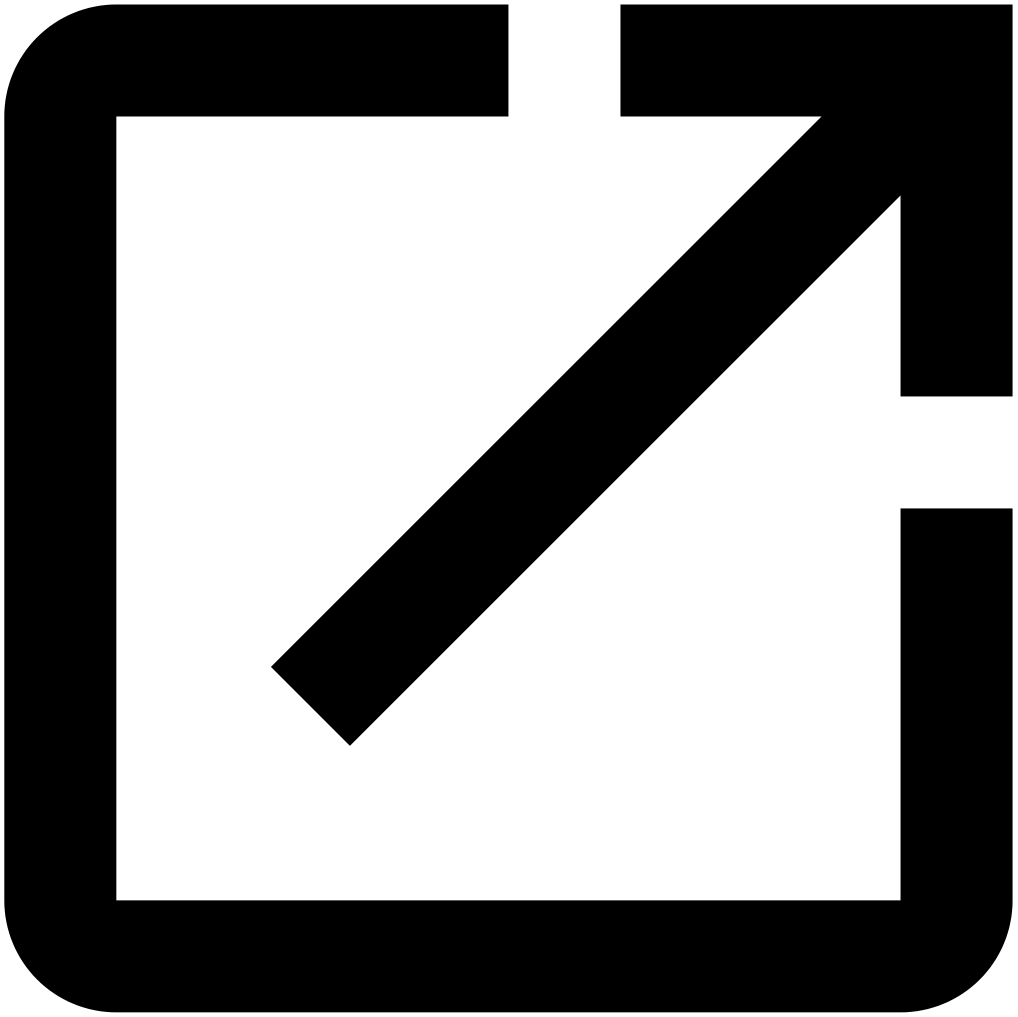
Hackers suspected to be from the North Korean Lazarus group tried their luck at stealing cryptocurrency from deBridge Finance, a cross-chain protocol that enables the decentralized transfer of assets between various blockchains.

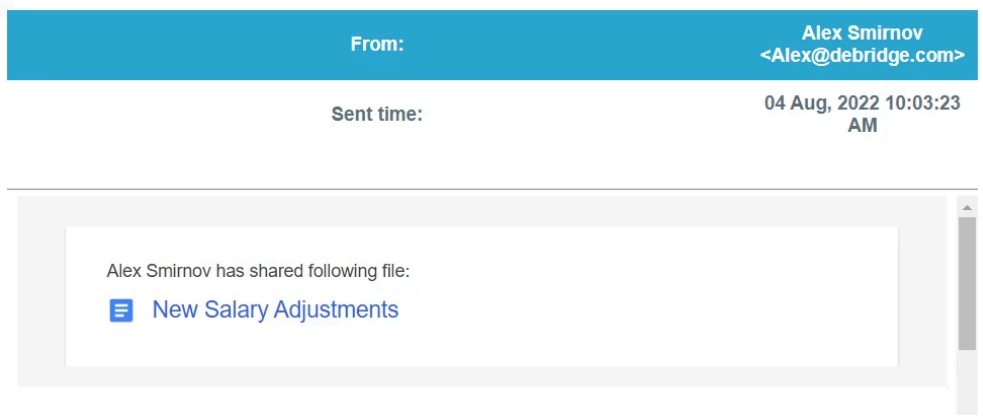
The threat actor used a phishing email to trick company employees into launching malware that collected various information from Windows systems and allowed the delivery of additional malicious code for subsequent stages of the attack.

Fake PDF and text files

The hackers targeted deBridge Finance employees on Thursday with an email purporting to be from the company co-founder, Alex Smirnov, allegedly sharing new information about salary changes.


DIE LINKE.
0:00

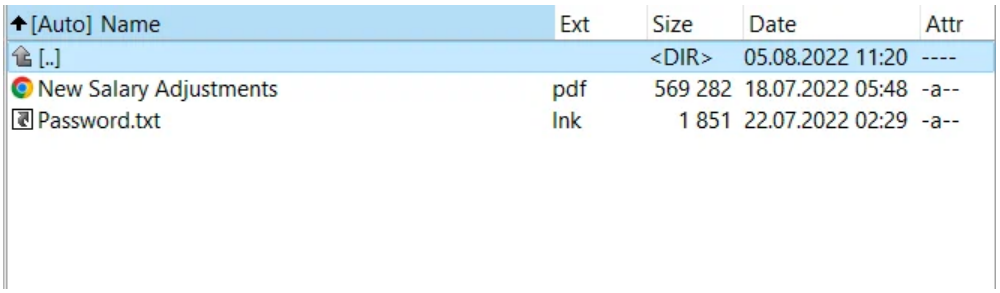




Email targeting targeting deBridge employees

source: Alex Smirnov

The email reached multiple employees and included an HTML file named 'New Salary Adjustments' that pretended to be a PDF file along with a Windows shortcut file (.LNK) that poses as a plain text file containing a password.



Fake PDF and text files used for targeting deBridge employees

source: Alex Smirnov

Clicking the fake PDF opened a cloud storage location claiming to provide a password-protected archive containing the PDF, thus bringing the target to launching the fake text file to obtain the password.

In a thread on Twitter, Smirnov explains that the LNK file executes the Command Prompt with the following command that retrieves a payload from a remote location:

The script was created to show a Notepad with the "pdf password: salary2022" and to check if the compromised system is protected by a security solution from ESET, Tencent, or Bitdefender.

Smirnov says that if the processes for the abovementioned security products are not present, the generated malicious file was saved in the startup folder, to ensure persistence.

This allowed the malware to achieve persistence and send out requests to the attacker's command and control server for further instructions.

At this stage, the threat actor collected details about the infected system like username, operating system, CPU, network adapters, and running processes.

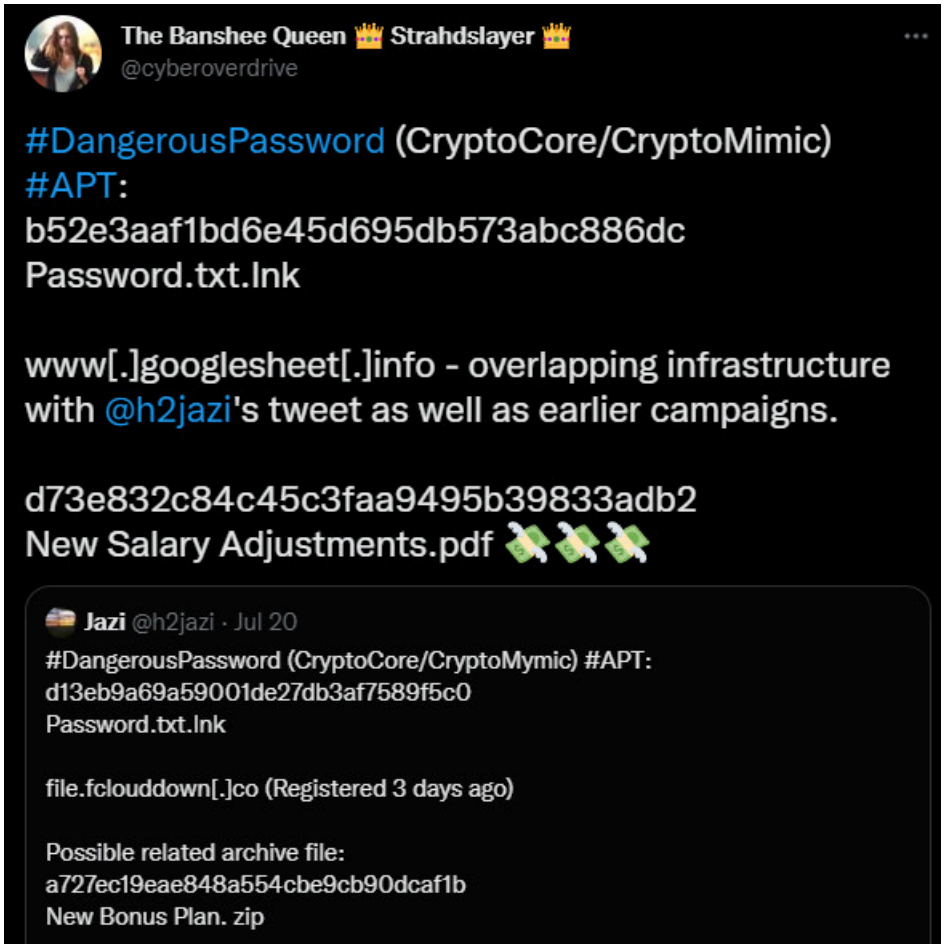
Smirnov says that the malware used in the attack was flagged by a small number of antivirus solutions.

The email was sent to multiple deBridge employees but most of them reported it as suspicious. However, one of them took the bait and downloaded and opened the document, which allowed Smirnov to analyze the attack.

Tied to North Korean Lazarus hackers

The connection to the North Korean hackers in the Lazarus group was possible due the overlap in file names and infrastructure used in a previous attack attributed to the threat actor.

Back in July, security researchers from PwC U.K. and Malwarebytes reported another campaign from the Lazarus hacker group - also referred to as CryptoCore and CryptoMimic - that used either the same same filenames or similar ones.

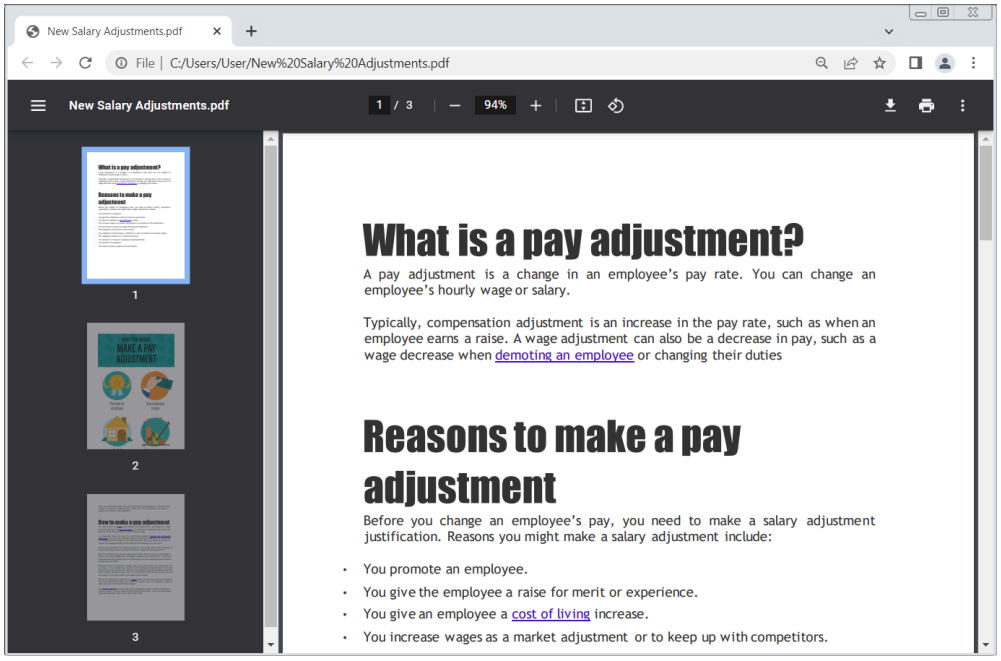


Malwarebytes and PwC researchers report similar Lazarus campaigns

BleepingComputer has learned that the same campaign has targeting cryptocurrency firms even earlier, in March, when the hackers targeted the crypto trading platform Woo Network with a document pretending to be a job offer from Coinbase cryptocurrency exchange platform.

While the file names are different, the attacker used the same fake PDF trick mask the malicious file and to get the victim to execute it.

In both attacks on deBridge and Woo Network, the hackers used malware for Windows systems. If a macOS system was detected, the victim would get a ZIP archive with a real PDF file.



Real PDF delivered to non-Windows machines

source: BleepingComputer

North Korea's Lazarus group has been focusing on hitting companies that rely in their business on blockchain technology and dececentralization concepts.

The threat actor uses social engineering tricks to establish a foothold on the victim computer and then tries to find a way to syphon cryptocurrency funds and assets.

One of the largest cryptocurrency heists attributed to this group is the theft of $620 million in Ethereum from Axie Infinity's Ronin network bridge.

Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
