US govt offers $10 million bounty for info on Clop ransomware

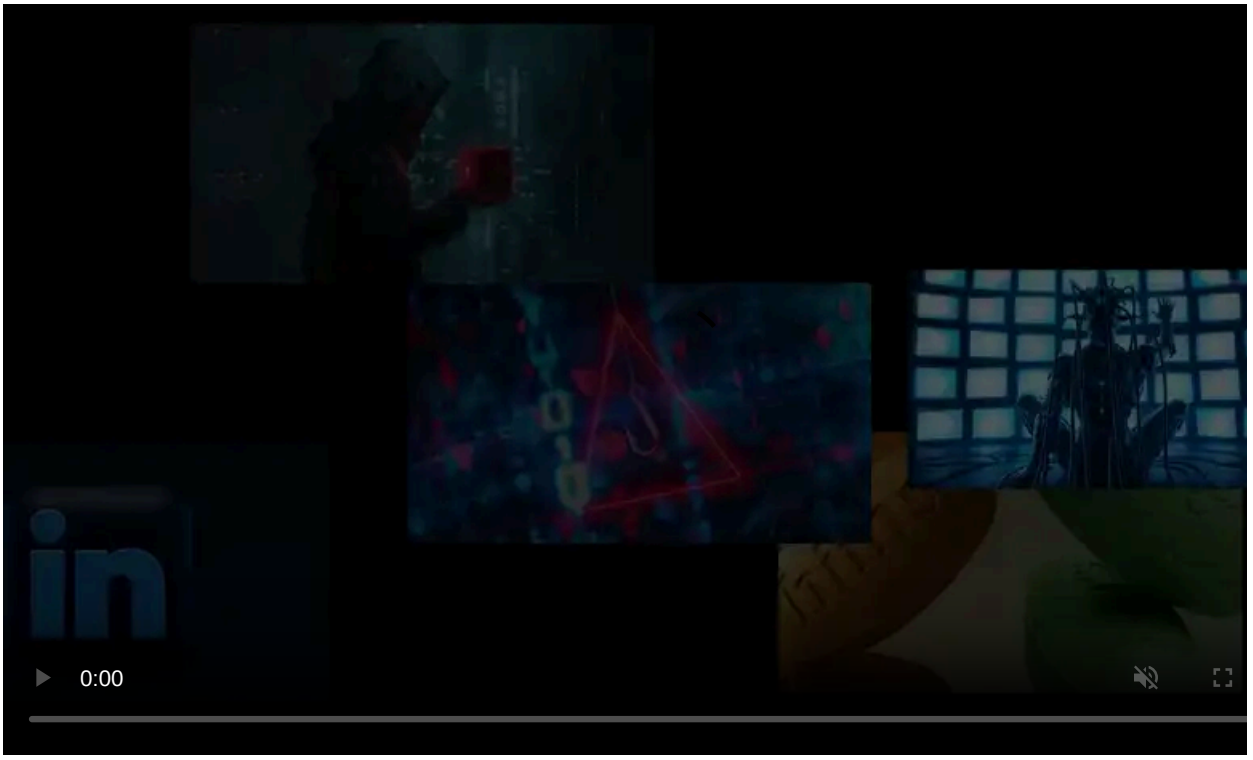
By Lawrence Abrams

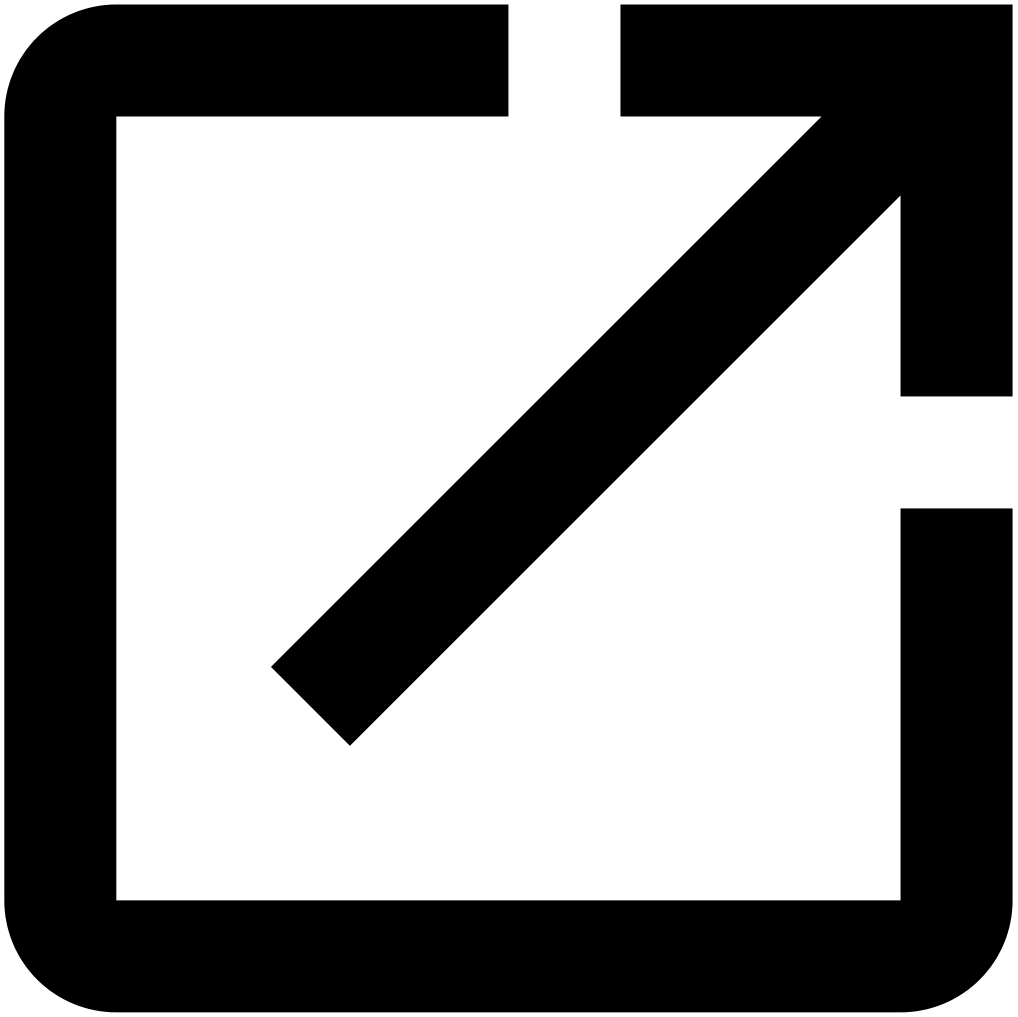
Published: 2023-06-17 · Archived: 2026-04-05 15:25:14 UTC

The U.S. State Department's Rewards for Justice program announced up to a $10 million bounty yesterday for information linking the Clop ransomware attacks to a foreign government.

"Do you have info linking CL0P Ransomware Gang or any other malicious cyber actors targeting U.S. critical infrastructure to a foreign government? Send us a tip. You could be eligible for a reward," tweeted the Rewards for Justice Twitter account.

Rewards of Justice (RFJ) is a U.S. Department of State program that offers monetary rewards for information on threat actors and attacks impacting the national security of the USA.


0:00



Initially launched to gather information on terrorists targeting U.S. interests, the program has since expanded to include information on cyber criminals, such as the Conti ransomware operation, Russian Sandworm hackers, REvil ransomware, and the Evil Corp hacking group.

Data breaches at U.S. federal agencies

This new RFJ bounty comes after the Clop ransomware conducted data-theft attacks on companies worldwide using a zero-day vulnerability in the MOVEit Transfer security file transfer platform.

The attacks started on May 27th, over the long U.S. Memorial Day holiday, with the Clop ransomware gang claiming to have stolen data from hundreds of companies.

This week, Clop began extorting companies by listing their names on a data leak site, promising to start leaking data if a ransom was not paid.

> ***DEAR COMPANIES.***
>
> CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.
>
> THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.
>
> WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.
>
> ***IMPORTANT!*** WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.
>
> ***STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.***
> ***STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM***
> ***STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR***
>
> WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE
>
> ***STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE***
> ***STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU***
> ***STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE***
> ***STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING***
> ***STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED***
> ***STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION***

Clop message on MOVEit Transfer attacks

At the same time, CNN first reported that numerous federal agencies, including The Department of Energy, were breached during these attacks, with data likely stolen.

The Clop threat actors told BleepingComputer earlier this month that any data stolen from governments was immediately deleted. They reiterated these claims this week in a message on their Tor data, saying they are only financially motivated and are not interested in politics.

"We got a lot of emails about government data, we don't have any government data and anything directly residing on exposed and bad protected not encrypted file transfer we still do the polite thing and delete all," reads a message on the Clop data leak site.

While the threat actors claim to be deleting any data stolen from governments, there is no way to determine if this actually takes place.

Therefore, federal agencies must make the assumption that stolen data could be abused or potentially acquired by foreign governments.

The Rewards for Justice program hopes to prevent future attacks by enticing people, including other threat actors who may have information about the Clop operation, to submit tips for a million-dollar reward.

To submit a tip, the State Department has set up a dedicated Tor SecureDrop server that can be used to submit information on Clop and other threat actors.

H/T vx-underground

Source: https://www.bleepingcomputer.com/news/security/us-govt-offers-10-million-bounty-for-info-on-clop-ransomware/