How did Clop get its hands on the MOVEit zero day?

By Dina Temple-Raston

Published: 2023-08-30 · Archived: 2026-04-05 15:47:48 UTC

When the Russian-speaking cyber gang Clop began extorting companies en masse this summer, the headlines focused on impact: hundreds of companies breached, millions of peoples' personal data stolen, terabytes of identifying information uploaded to the dark web.

Clop exploited a bug in a widely used (but relatively unknown) file transfer software called MOVEit, gaining access to sensitive documents and exfiltrating data at scale for use in extortion campaigns. And even months after the initial breach, Clop continues to add to its list of victims every week.

What's raised eyebrows in the cybersecurity community is not just the scale of Clop's campaign, but the manner in which they compromised MOVEit in the first place. The group used a zero-day bug, an unknown vulnerability in the software that was either discovered by the gang or, more likely, purchased in a dark web forum. Dustin Childs, the head of threat awareness for Trend Micro's Zero Day Initiative, says criminals wielding zero-day bugs in extortion and ransomware campaigns is rare but not unheard of.

Childs would know. His team is constantly finding bugs and buying them from security researchers around the world. And in a conversation with the Click Here podcast, he talks about the zero-day market, Clop's remarkable strategy, and whether other ransomware gangs will follow their lead.

This conversation has been edited for length and clarity.

CLICK HERE: Let's start with your work with the Zero Day Initiative. You're constantly purchasing bugs in all kinds of software programs. How do you work out what a bug costs?

DUSTIN CHILDS: So depending on the type of bug, it could be worth $150. And depending on where it's sold, it could be worth up to $15 million. So we look at the bug, we look at how severe it is, we look at how widespread the product is. If it's a very niche product, it's not gonna be as much. If it's something like Microsoft Office or Google Chrome, it's obviously gonna be [worth] much more, since that's gonna be a greater impact to a lot more people. There's a wide range in value of these bugs. And we do look at each bug that is sent to us and sometimes we say, We're just not interested in this bug. It's just too niche. [Maybe] we offer a price and they either accept it or reject it, and then we take the bug and do our thing with it.

CH: And what do you do with the bug?

DC: So let's say it's a Microsoft bug. We purchase a Microsoft bug and then we take it and we build filters for [Trend Micro] products to protect our customers upfront. That's the big thing about the bug bounty marketplace is we're purchasing bugs with the end goal of getting the bugs fixed. And then we send the bug to Microsoft. They don't actually pay us.

CH: So how do you make money?

DC: That's the neat part. We don't make money at all. We make money by making our products better and selling more products.

CH: So give me an idea of what your shop is like. Is it a bunch of people in a room? Are they remote? What happens if one of your guys suddenly finds a zero day?

DC: We have a remote team. We're all over the world, and we've got about 12 to 15 researchers at any given time. They're doing their own research, reporting their own bugs. But different people have different specialties. So an Apple bug will go to one person or a Windows bug will go to another person and they look at it and they verify it. They make sure that it's real, and they'll make the suggestion whether or not we purchase it. Then we decide on a price.

CH: And if somebody finds a zero day, are they punching the air? Or is it a little more sedate than that?

DC: I guess it depends on the person. There are some people who definitely punch the air. There's people around the world where finding a zero day is life-changing for them, and we really do have people around the world. We have one researcher in Ethiopia, and he was punching the air because we essentially made him the richest man in his village. But then there are some people who might find 10 zero days, but they're all just gonna be worth $150. That's great, but you know, I'm not punching the air yet.

CH: I always thought of zero days as being something that only nation-states bought because they were so expensive.

DC: Right.

CH: So disabuse me of that.

DC: Well, there's two ways to think of zero days. There's zero-day *vulnerabilities* and there's zero-day *exploits.* Zero-day vulnerabilities are much more common than people think. They're out there everywhere, but they're not being exploited. I purchase zero-day vulnerabilities.

Zero-day exploits are relatively rare and they tend to be very expensive. Those are the ones people think of when we're talking about nation-state attacks and advanced persistent threats. And if you look at the world I live in, that's where the exploit brokers come in. They're purchasing zero-day exploits. They're paying a lot more for it, too. One of the biggest companies is offering, I think, $2.5 million for a zero-day exploit in Android phones. I'm holding a contest and offering $250,000. But they have a different business model as well. Whereas we get the bugs fixed, they resell the bugs to — most likely — nation-states. They don't disclose their customer list, of course, but when you're buying bugs for $2.5 million, who are you reselling them to? You're reselling them to the people who print the money. And that's gonna be the nation-states.

CH: Can you explain the difference between a zero-day vulnerability and an exploit?

DC: Finding a vulnerability in a software program is one level of expertise. But then finding a way to actually exploit that vulnerability is a second level of expertise. I can go out this afternoon and find bugs in programs, but I'm not an exploit writer. I will not figure out the way to actually exploit that bug. So that's the difference, really, between zero-day vulnerabilities and exploits. We're dealing with zero-day bugs that could potentially become

exploits one day. The exploits that are out there that are really expensive are already essentially weaponized by a threat actor to do actual damage to a target.

CH: So it's like opening the door versus actually knowing what you're going to do once you're inside.

DC: Right. It's the difference between having a key and using a key.

CH: So if we're talking about black hat hackers, are they the typical buyers for zero-day vulnerabilities?

DC: Not necessarily. There's certainly a criminal element that uses zero-day vulnerabilities, but most often they use what we call an "n-day," which is something that's been patched for a number of days. Those are much more common. The vendor says: *Here's a hole, here's a patch to plug the hole.* The problem is, people don't apply the patches faster than the bad guys can create the exploits for those holes. They do occasionally buy zero days on these underground forums. We've heard numbers up to $8 million for some of these sales. Of course, those are all rumors and speculations. They don't show receipts in underground forums, so I can't confirm that.

CH: The Clop criminal gang appears to be buying zero-day vulnerabilities. Have you seen gangs do that before?

DC: We have. It's very rare, though, for [criminals] to be purchasing zero days. But it's not unheard of.

CH: So where were you when you found out about the MOVEit hack?

DC: Interestingly enough, I was on vacation. That's always the case, isn't it? I was scrolling my phone on a beach next to a pool and, it's like, *Great. Why does it always happen on vacation?*

CH: And what was the first thing that went through your mind?

DC: The first thing that went through my mind is what is MOVEit? Because it was not a software that I was familiar with. But then the more I read about it, the second thing really was, *Oh, they actually used a zero day for this and not an n-day.* So that was really interesting. That's a little bit different.

CH: And did you immediately think it might be Clop given that they seem to focus on transfer programs?

DC: Doing attribution is very difficult, so I let other people do that for me. But since it's come out that it is Clop and they've taken credit for it, it does make sense. It does fit their M.O.

CH: And how do you think they got their hands on a zero day?

DC: There's multiple ways they could have acquired it. There are underground forums where there are auctions. So you'll have a forum and say, *Hey, I've got an exploit in this, and the bidding starts at $10,000.* Or they could have someone in their group who actually found the zero day. Or they could have purchased it from an initial access broker. Without any further details, I don't wanna speculate too much. But the most likely scenario is they purchased it off of a forum.

CH: So why do you buy a zero-day vulnerability when you can maybe just gain access to something without one?

DC: You buy it to increase your chances. It's all a matter of investment of resources, right? The longer it takes you to get in, the more likely you are to get caught. So if you can buy a shortcut, it's going to increase your chances as a ransomware crew to actually achieve your target.

CH: You mentioned the Android exploit, which would be really expensive. Do you have a sense of what an exploit for something as obscure as MOVEit would cost?

DC: It depends on the marketplace. We purchased a MOVEit bug not too long ago. I can't divulge what we paid for it, but it was not the most expensive bug that we purchased that day. I'll tell you that. *[Editor's note: The company said that vulnerability had been previously disclosed and patched.]* On the exploit broker marketplace, it would probably bring five figures, but not a high five-figure number. And I would think a little less on the criminal marketplace because when you buy from an exploit broker, they actually offer support contracts. So if you have problems using the exploits, they'll give you support. There's someone you can call, like, *Hey, I can't hack this guy.* And it's like, *OK, well here, let me walk you through it.* So that's why it's a little bit more on the exploit broker than a criminal forum.

CH: So if you're only paying, say, $10,000 or $20,000 for something and you get 5% of the people that you target to give you money, it's a pretty good return on investment.

DC: Exactly. They're doing this at scale because they expect a 1- to 5-percent return, and you just have to do it at scale enough. And certainly Clop has done it at scale. I'm a big sabermetric guy, a big baseball and statistics guy. I would love to see their statistics for how many people they targeted versus how many people they were able to compromise. So if anyone from Clop is listening and wants to tell me all of that, I'd love to hear it.

CH: When we typically think about ransomware groups, we think about them getting into a system, encrypting everything, maybe exfiltrating things as well, holding it hostage, and then waiting for money. But Clop doesn't encrypt stuff. Why?

DC: That's a very good question, and there's not a very clear answer as to why they don't encrypt stuff. One thing I think is happening is companies are less likely these days to actually pay out on ransomware. They're getting better at recovering from ransomware attacks and encryption attacks, so it's more valuable [for companies] to invest in backups and restoration procedures. So it could be possible that [Clop] said, *We're gonna have a better chance of getting paid if we just exfiltrate all this data and then extort them on releasing the data rather than just encrypting their files.*

CH: Does that also help them hide who they are?

DC: I think so. I think it helps to anonymize them a little bit, although there have been some reports that they're in Eastern Europe. Most ransomware gangs are located in Eastern Europe. But the lower footprint you leave on a target, the greater your chance of remaining anonymous. They seem to be a little bit more on the professional side. I don't like to use the word "professional" when it comes to ransomware because it is a criminal activity. But I would say they color with a different crayon. They're not as immature as, say, the Lapsus$ gang. They're not as bold as some of the other gangs that are in your face. They're a little bit more subtle. So it's a very interesting dynamic with Clop. They're just a little bit more mature and they know what works.

CH: This whole idea of not encrypting files and just exfiltrating things at scale — do you think that this is where ransomware is going? As you say, companies are increasingly doing decryption and backups on their own. So will exfiltration and extortion be a new trend?

DC: It's certainly interesting to see it happen, and I think it will be a trend for a while, if nothing else, because Clop has been incredibly successful. Like even today, they're coming out with new victims. It's a copycat sort of league, if you will. If one ransomware group is very successful, the other ransomware groups will see that success and try to imitate it. So I do think this will be a trend for a while because it has been so very successful.

CH: It also seems that Clop bit off more than it could chew — that they're not quite big enough to take advantage of everything they have. We're months out, and there's still a slow drip, drip, drip of what they have. Is that the right way to interpret this sort of long tail of the MOVEit hack?

DC: It seems that way. I don't know that anyone could have imagined this many companies being affected by this type of product. So I don't know that Clop had any idea the install numbers of MOVEit and what they were going to get out of it. That's another thing that's a little bit different about Clop. They don't seem to be in a rush. It's like, *We'll just take our time. We'll sit here on your data. We already have it, so we'll just get to you when we get to you.* They'll just keep [extorting] over and over again until they run out of resources or they're caught.

CH: I have the one last question that has to do with middleware. Do you feel like what Clop has done with MOVEit is any sort of inflection point when it comes to this because of the focus on middleware?

DC: I would actually back it up a little bit and say PaperCut was the inflection point. If you go back a few months, there's a piece of software called PaperCut, and this is one that I'd never heard of either. But it turns out that almost every university in North America uses this to manage their printers, and we saw active attacks in PaperCut very quickly.

We have been saying in [the Zero Day Initiative] that these middleware programs are a problem and that they are very susceptible because there hasn't been a lot of scrutiny. You take something like Microsoft Windows or macOS or Google Chrome, there's a lot of scrutiny that's put on those products. There's a lot of people finding bugs. And as a consequence, they're pretty secure. You take something [like middleware] — there's not been a lot of research into the security of these products, and consequently, they may have some very glaring holes that people can exploit once they really shine a spotlight on them. And once you find a bug in a product, a lot of people will start looking at that product as well. Because if there's one bug, that usually means there's a lot of bugs. That kind of shows that there's a viable path to destruction through this middleware. [For these client companies] the perimeter is very secure, the desktop is very secure. The stuff in the middle, it's kind of like the chocolatey nougat that you can get in there and really take advantage of.

[Dina Temple-Raston]

is the Host and Managing Editor of the Click Here podcast as well as a senior correspondent at Recorded Future News. She previously served on NPR's Investigations team focusing on breaking news stories and national security, technology, and social justice and hosted and created the award-winning Audible Podcast "What Were You Thinking."

Will Jarvis

is a podcast producer for the Click Here podcast. Before joining Recorded Future News, he produced podcasts and worked on national news magazines at National Public Radio, including Weekend Edition, All Things Considered, The National Conversation and Pop Culture Happy Hour. His work has also been published in The Chronicle of Higher Education, Ad Age and ESPN.
