FTX erstattet Opfern von 3Commas-Phishing-Angriffen 6 Mio. USD

Mindestens drei FTX-Benutzer stellten fest, dass aufgrund eines Phishing-Angriffs Millionen von ihren Konten fehlten Der API-Anbieter 3Commas entdeckte, dass mehrere gefälschte Websites zum Phishing seiner Benutzer verwendet wurden Sam Bankman-Fried, CEO von FTX, sagte, die Kryptowährungsbörse werde 6 Millionen US-Dollar ausgeben, um die Opfer eines Phishing-Betrugs zu entschädigen, der auf ihre Benutzer abzielt ج aber nie wieder. Seit letzter Woche wurden mindestens drei FTX-Benutzer von dem Betrug betroffen, der es Hackern ermöglichte, Millionen von Dollar mit nicht autorisierten Trades von ihren Konten abzuschöpfen. Die Angreifer verschafften sich Zugriff, indem sie die Schlüssel der 3Commas Application Programming Interface (API) ausnutzten, die …

- Mindestens drei FTX-Benutzer stellten fest, dass aufgrund eines Phishing-Angriffs Millionen von ihren Konten fehlten
- Der API-Anbieter 3Commas entdeckte, dass mehrere gefälschte Websites zum Phishing seiner Benutzer verwendet wurden

Sam Bankman-Fried, CEO von FTX, sagte, die Kryptowährungsbörse werde 6 Millionen US-Dollar ausgeben, um die Opfer eines Phishing-Betrugs zu entschädigen, der auf ihre Benutzer abzielt ح aber nie wieder.

Seit letzter Woche wurden mindestens drei FTX-Benutzer von dem Betrug betroffen, der es Hackern ermöglichte, Millionen von Dollar mit nicht autorisierten Trades von ihren Konten abzuschöpfen. Die Angreifer verschafften sich Zugriff, indem sie die Schlüssel der 3Commas Application Programming Interface (API) ausnutzten, die von den betroffenen FTX-Benutzern verwendet wurden.

3Commas ist ein automatisierter Krypto-Trading-Bot-Anbieter, der den automatisierten Kauf und Verkauf von Krypto an großen Börsen wie FTX ermöglicht. Es wird als Effizienztool angesehen, das es Benutzern ermöglicht, Hunderte von Trades einfach zu platzieren, was manuell anspruchsvoll ist.

Die Angriffe wurden bei einem FTX-Benutzer aufgedeckt angeblich stellte fest, dass sein Konto am 19. Oktober mehr als 5.000 Mal mit DMG-Token gehandelt hatte, was zu einer Extraktion von fast 1,6 Millionen Dollar in Bitcoin, FTX-Token, Ether und anderen Kryptowährungen (damaliger Wert) führte.

Ein zweiter Benutzer offengelegt am 22. Oktober, dass er Opfer des FTX-Angriffs wurde und behauptete, er habe infolge des Vorfalls etwa 104 Bitcoin (2 Millionen US-Dollar, aktuelle Preise) verloren. Er behauptete auch, er habe sein 3Commas-Konto nie verwendet, um einen Bot einzurichten.

FTX-Phishing möglicherweise durch Malware ausgelöst

DMG, das Token, das von den Hackern in ihrem Schema genutzt wird, ist das Governance-Token des nicht mehr existierenden dezentralisierten Finanzprojekts DeFi Money Market (DMM), das Betrieb eingestellt am 5. Februar nach erkundigeniches von der SEK.

Der Preis von DMG ist seit der Schließung um fast 60 % eingebrochen, erholte sich aber bis Montag auf 0,02 $ ₾ laut Angaben ungefähr auf dem gleichen Niveau wie bei der Schließung von DMM CoinGecko Daten.

3Kommas Bestätigt dass eine Reihe von Partnerbörsen-API-Schlüsseln verwendet wurden, um nicht autorisierte Geschäfte für DMG-Krypto-Handelspaare auf Börsenkonten durchzuführen. Auch Trader, die 3Commas nie genutzt hätten, seien von der Phishing-Attacke betroffen, hieß es.

Bei weiteren Untersuchungen fand das Team mehrere gefälschte 3Commas-Websites, die zum Phishing ihrer Benutzer verwendet wurden. Hacker hatten das Design der Benutzeroberfläche der Website repliziert, um API-Schlüssel von Benutzern zu erbeuten, die fälschlicherweise die gefälschte Website verwendet hatten, um ihre Exchange-Konten zu verbinden.

3Commas sagte, es gehe außerdem davon aus, dass API-Schlüssel von Benutzern über Malware und Browsererweiterungen von Drittanbietern gestohlen wurden. Es lehnte die Verantwortung ab und sagte, es sei höchst

unwahrscheinlich, dass der Sicherheitsvorfall von den Diensten von 3Commas ausging. Blockworks hat FTX und 3Commas um einen Kommentar gebeten.

Bankman-Fried legte ein Twitter-Thread Frustration über den Vorfall zum Ausdruck bringen. ȝDies war nicht nur kein Phishing von FTX, es war nicht einmal eine FTX-Site. Und im Allgemeinen können wir nicht kompensieren, dass Benutzer von gefälschten Versionen anderer Unternehmen in diesem Bereich gephishing werden!ȝ

ȝEs ist nicht FTX und wir haben im Grunde keine Kontrolle darüberȝ, sagte Bankman-Fried.

> 8) Wie auch immer, kürzlich ist etwas Frustrierendes passiert.
>
> Wir haben hauptsächlich Websites ausgemerzt, die versuchen, Benutzer zu phishen, indem sie sich als FTX tarnen. Aber wir können keine gefälschten Websites reparieren, die sich als *andere* Dienste ausgeben.
>
> Einige Benutzer haben sich versehentlich auf gefälschten anderen Websites registriert, darunter 3 Kommas.
>
> ҉ SBF (@SBF_FTX) 23. Oktober 2022

Bankman-Fried fügte hinzu, dass FTX Phishing-Sites, die sich als die Börse selbst ausgeben, größtenteils eliminiert hat, aber nicht dasselbe für Sites tun kann, die sich als andere Dienste ausgeben.

ȝUm es klar zu sagen, Phishing ist fast immer ein Fall, bei dem der Benutzer freiwillig (aber unwissentlich) seine Kontodaten an

einen Betrüger weitergibt, indem er eine schlechte Website oder ähnliches aufruft ج aber trotzdem nehmen wir unsere Pflicht zum Schutz der Kunden ernst. sogar von sich selbstɔ, twitterte er.

In diesem Fall hat Bankman-Fried versucht, die von der 3Commas-Phishing-Kampagne betroffenen Benutzer zu entschädigen, aber er warnte in allen Großbuchstaben, dass ɔdies eine einmalige Sache ist und wir dies in Zukunft nicht mehr tun werdenɔ.

. .

Der Beitrag FTX to Reimburse $6M to 3Commas Phishing Attack Victims ist keine finanzielle Beratung.

Details