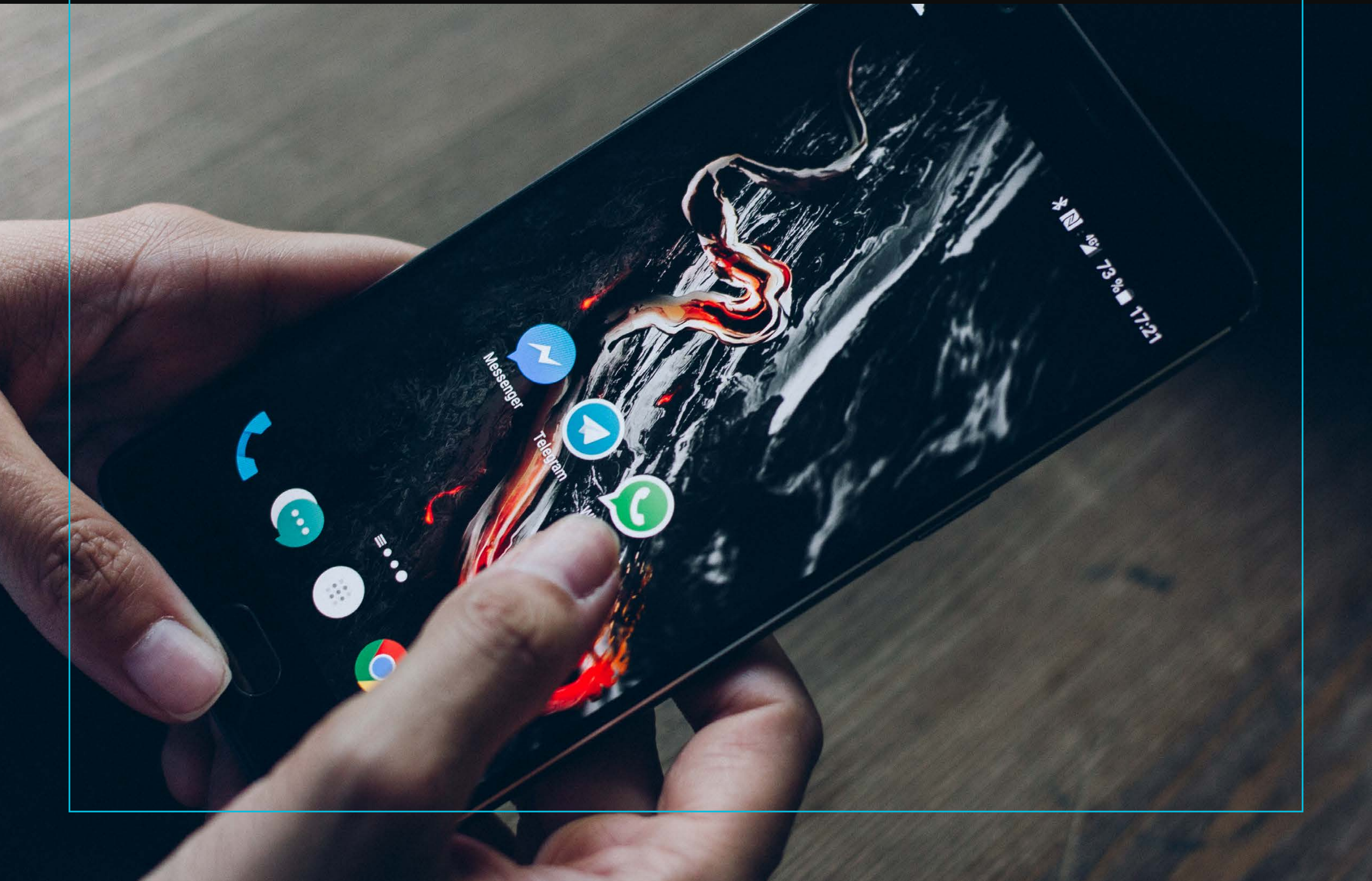
SAFEGUARD CYBER

Telegram Impersonation Targets Crytpocurrency Firm Employees with Malware

Malware Report

DIVISION SEVEN



Executive Summary

An institutional cryptocurrency customer wanted to understand if its traders had been targeted by crypto-stealing malware highlighted in Microsoft threat research released on December 6, 2022. With SafeGuard Cyber's lookback capabilities for Telegram, our Division Seven (D7) threat intelligence team was able to confirm traders had been targeted months ago, in July 2022. In contrast to the longer trust-building TTPs detailed by Microsoft, our forensic analysis was able to identify the threat actor impersonating a trusted individual to more efficiently carry out the social engineering attack.

Background

SafeGuard Cyber has several large cryptocurrency investment firms as customers. One such customer deploys our platform for content capture and archiving for Telegram, on behalf of its traders, to satisfy SEC recordkeeping requirements. However, in early December 2022, Microsoft published research on a threat actor the company tracks as DEV-0139. In its report, Microsoft noted the threat actor "joined Telegram groups used to facilitate communication between VIP clients and cryptocurrency exchange platforms and identified their target from among the members. The threat actor posed as representatives of another cryptocurrency investment company, and in October 2022 invited the target to a different chat group and pretended to ask for feedback on the fee structure used by cryptocurrency exchange platforms." DEV-0139 sends a weaponized Excel file with the name OKX Binance & Huobi VIP fee comparision.xls armed with malicious macros.

Event Analysis

Our customer wanted to understand if its traders had been targeted by this threat actor. Using SafeGuard Cyber's lookback capabilities and detection engine, the D7 team was able to locate and confirm an instance when traders were targeted with this malicious file in July 2022. Moreover, in this timeframe, we detected that the threat actor adopted the tactic of impersonating a known employee from our customer organization to deliver the payload.

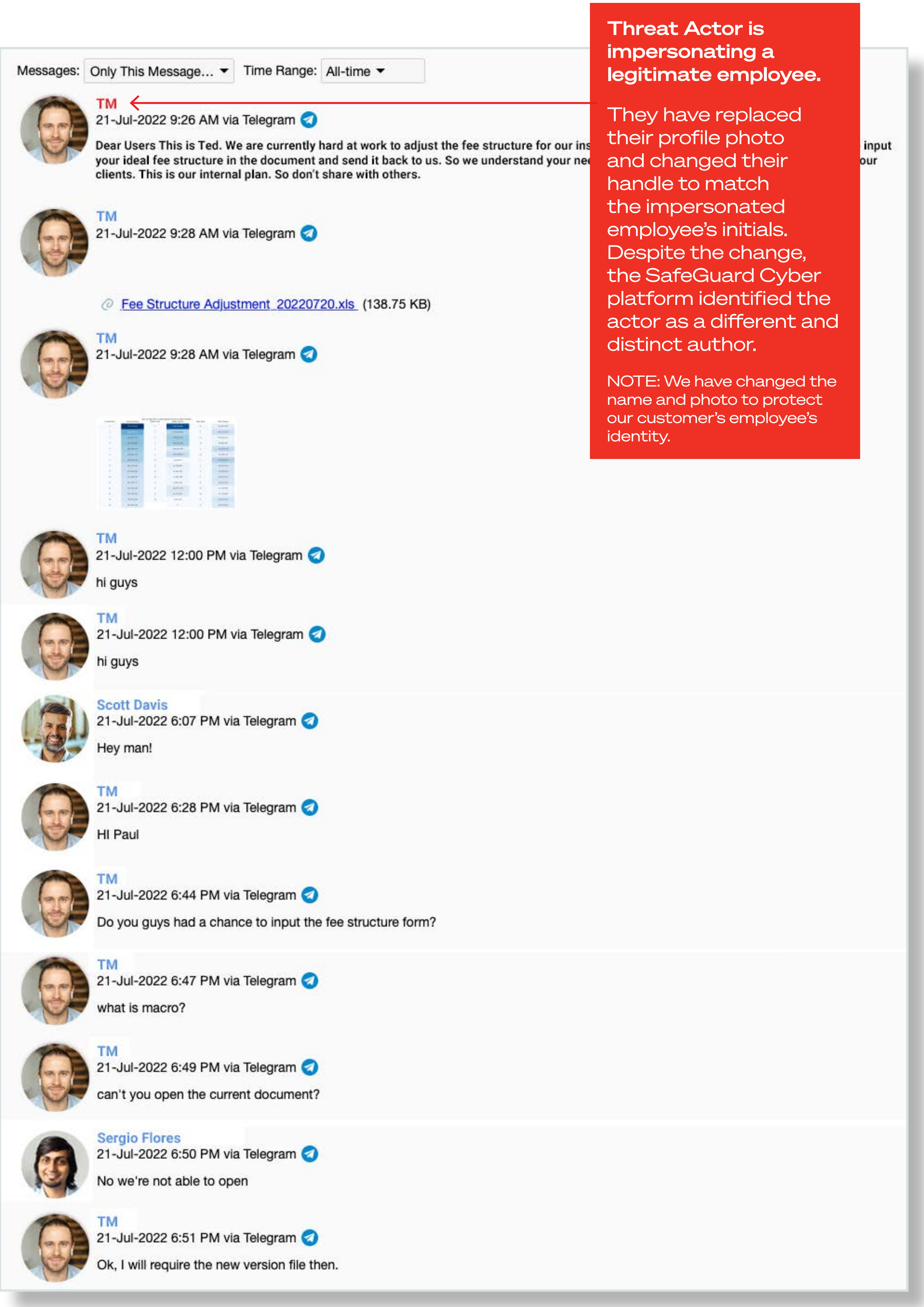
We detected this impersonation because we track communications against "authors," as defined by user metadata. The threat actor attempted the impersonation through use of the legitimate user's initials. The impersonation, however, was detected because they're recorded and flagged as a different unique author. The D7 team believes that DEV-0139's use of detailed trust building, as reported by Microsoft, was likely an adaptation to less successful, albeit easier, impersonation tactics.

The result of this analysis is a compliance customer has enabled deeper security detections for monitored Telegram users. This move is part of a larger trend we have observed over the course of 2022, a greater convergence of security and compliance in financial services to address overall business communication risks.

Threat Actor is impersonating a legitimate employee.

They have replaced their profile photo and changed their handle to match the impersonated employee's initials. Despite the change, the SafeGuard Cyber platform identified the actor as a different and distinct author.

NOTE: We have changed the name and photo to protect our customer's employee's identity.



Messages: Only This Message… ▾ Time Range: All-time ▾

TM
21-Jul-2022 9:26 AM via Telegram

Dear Users This is Ted. We are currently hard at work to adjust the fee structure for our ins input
your ideal fee structure in the document and send it back to us. So we understand your nee our
clients. This is our internal plan. So don't share with others.

TM
21-Jul-2022 9:28 AM via Telegram

Fee Structure Adjustment_20220720.xls (138.75 KB)

TM
21-Jul-2022 9:28 AM via Telegram

TM
21-Jul-2022 12:00 PM via Telegram
hi guys

TM
21-Jul-2022 12:00 PM via Telegram
hi guys

Scott Davis
21-Jul-2022 6:07 PM via Telegram
Hey man!

TM
21-Jul-2022 6:28 PM via Telegram
HI Paul

TM
21-Jul-2022 6:44 PM via Telegram
Do you guys had a chance to input the fee structure form?

TM
21-Jul-2022 6:47 PM via Telegram
what is macro?

TM
21-Jul-2022 6:49 PM via Telegram
can't you open the current document?

Sergio Flores
21-Jul-2022 6:50 PM via Telegram
No we're not able to open

TM
21-Jul-2022 6:51 PM via Telegram
Ok, I will require the new version file then.

AMERICAS
977 Seminole Trail #373
Charlottesville, VA
22901 USA
+1 (800) 974-3515
sales@safeguardcyber.com

SAFEGUARD CYBER