MANDIANT ADVANTAGE

News Analysis

March 25, 2022 07:28:15 PM, 22-00007972

# Morgan Stanley Client Accounts Breached in Social Engineering Attacks

**FROM THE MEDIA:**

New York, N.Y.-based financial services firm Morgan Stanley has revealed that, on Feb. 11, 2022, its wealth and asset management division was hit by "vishing" attacks that exposed account information belonging to some of its customers. According to reports, as part of the vishing attacks, attackers impersonated Morgan Stanley in voice calls designed to convince targeted individuals to provide sensitive information that included login and banking credentials. According to an alert sent to customers by Morgan Stanley, "As you are aware, on or around Feb. 11, 2022, you were contacted by a bad actor claiming to be with Morgan Stanley. The bad actor was able to obtain information relating to your Morgan Stanley Online account, subsequently accessing this account and initiating unauthorized Zelle payments." A spokesperson for Morgan Stanley also informed *Bleeping Computer* that "there was no data breach or information leak from Morgan Stanley. This compromise was not a result of any action of Morgan Stanley Wealth Management and our systems remain secure. Your Morgan Stanley Wealth Management account has been flagged to our Customer Call Center so that any callers into the Call Center will be prompted with additional verification. Your previous Morgan Stanley Online account was also disabled."

**READ THE STORY:** Bleeping Computer

**NEWS ANALYSIS RATING:** MEDIA ON-TARGET

**ANALYST COMMENT:**

Mandiant Threat Intelligence assesses with high confidence that investment services face a constant high-intensity threat from financially motivated cyber threat actors, which range from highly sophisticated threat groups to unsophisticated, opportunistic individuals. Threat actors have long relied on social engineering to bypass robust security controls and exploit user behavior to compromise accounts, launch malware, steal proprietary information, or collect data for future criminal/espionage activity. Humans often are the weakest link in a robust security environment, as they are vulnerable to compromise via social engineering. Threat actors have used social engineering to carry out criminal and espionage activity against a wide variety of industries, and human weaknesses are industry-agnostic. Education, training, testing, and constant vigilance are the primary risk mitigations to protect users from nefarious operations using social engineering. Media on-target.

## Related Intelligence Report(s):

Threats to Investment Services and Exchanges | 21-00021147

SUBSCRIPTION REQUIRED

27

Industry Profile: Financial Services (2021) | 21-00004164
SUBSCRIPTION REQUIRED

Industry Snapshot: Financial Services (Q4 2021) | 22-00001284
SUBSCRIPTION REQUIRED

## About this Product

The expert analysts at FireEye Intelligence highlight and provide context to current media trends each day as they analyze and encapsulate the events in cyber security. Topics selected cover a broad array of cyber threats and are intended to aid readers in framing key publically discussed threats. FireEye does not specifically endorse any third-party claims made in this material or related links, and the opinions expressed by third parties are theirs alone. The enclosed FireEye Intelligence comments and accuracy rankings are based on information available at the time of publication, and FireEye reserves the right to hone its analytical perspectives as the threats evolve and as further intelligence is made available.

**MEDIA ON-TARGET**

This ranking denotes a media trend in which the information reported is generally verifiable and can be correlated with our additional intelligence sources.

**PLAUSIBLE**

This ranking refers to a story possessing key information that, although plausible based off our past observations of similar events, we have not been able to validate in the short time available.

**JUDGMENT WITHHELD**

This ranking refers to a story which is complex enough that we cannot validate it in a short time.

**MEDIA OFF-TARGET**

This ranking refers to a story in which key elements are unsubstantiated or inaccurate. A story can have a key element which is inaccurate, and the rest accurate, and still receive the ranking Off Target.

The accuracy rating is applied through analysis of the data behind each trend based on FireEye closed sources of information. The reason for this rating is so that our readers can quickly be alerted to trends, which are not yet substantiated or are based on information in conflict with FireEye findings. This document is developed and provided by FireEye Intelligence for direct distribution to your organization. Re-distribution or publication outside of your organization is not permitted without the expressed written permission of FireEye.

MANDIANT ADVANTAGE

5950 Berkshire Lane, Suite 1600 Dallas, TX 75225



27