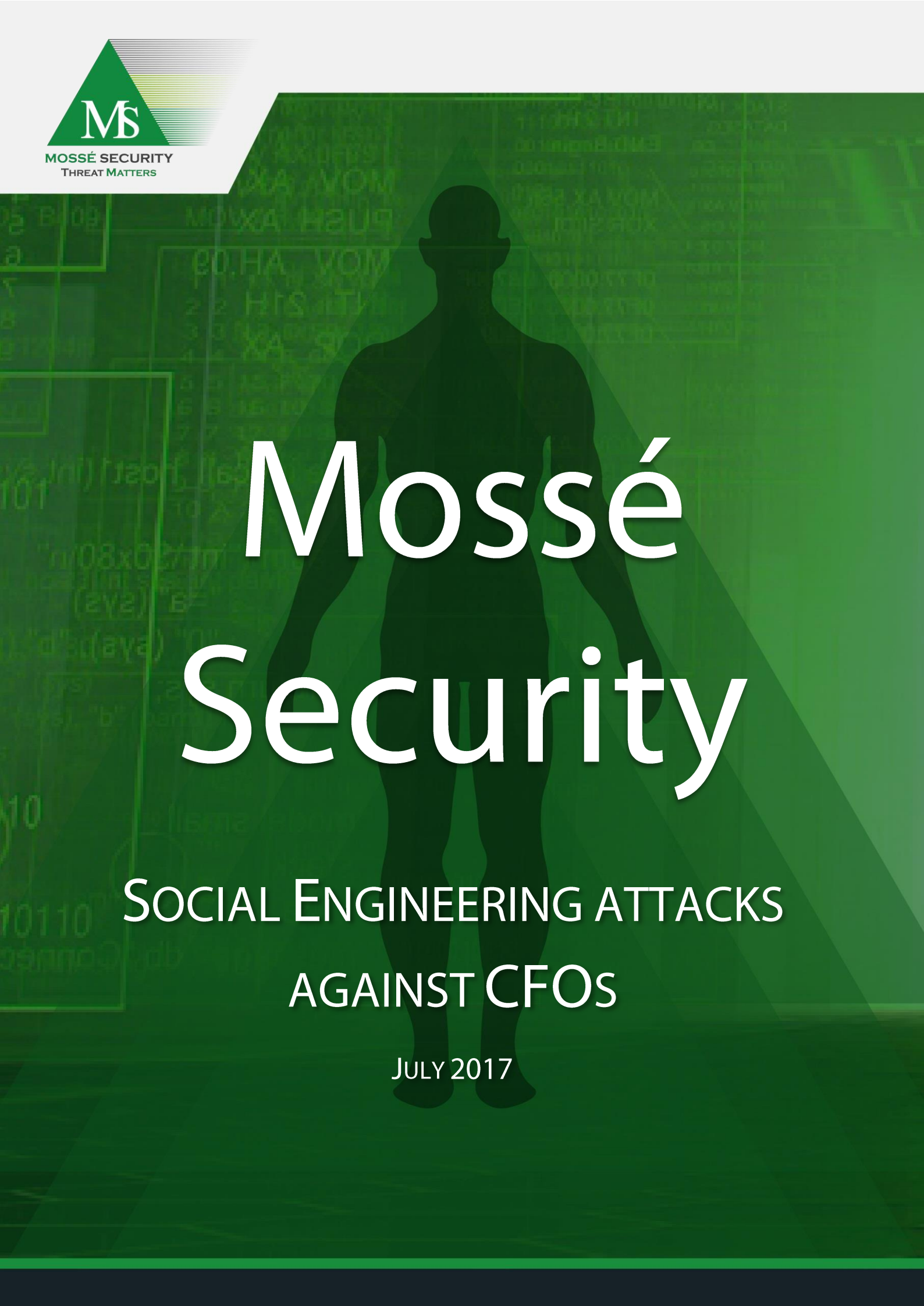
MOSSÉ SECURITY
THREAT MATTERS
Mossé
Security
SOCIAL ENGINEERING ATTACKS
AGAINST CFOS
JULY 2017

TABLE OF CONTENTS

Tables:

Figures

THREAT REPORT

Business executives of small and medium sized firms all over Australia are being targeted by sophisticated social engineers that attempt to defraud them with fake invoices. In this report, we present an advanced attacker group that successfully defrauded numerous small businesses in Melbourne, Sydney and Brisbane in Australia.

We have labelled this group "FRAUDSTERS-1", and this report presents their attack techniques and offers recommendations that companies can implement to protect themselves.

FRAUD OPERATION OVERVIEW

FRAUDSTERS-1 compromises the email servers of business advisory companies located outside of Australia and uses their domain names to send emails to Chief Financial Officers (CFOs) pretending to be the Chief Executive Officer (CEO).

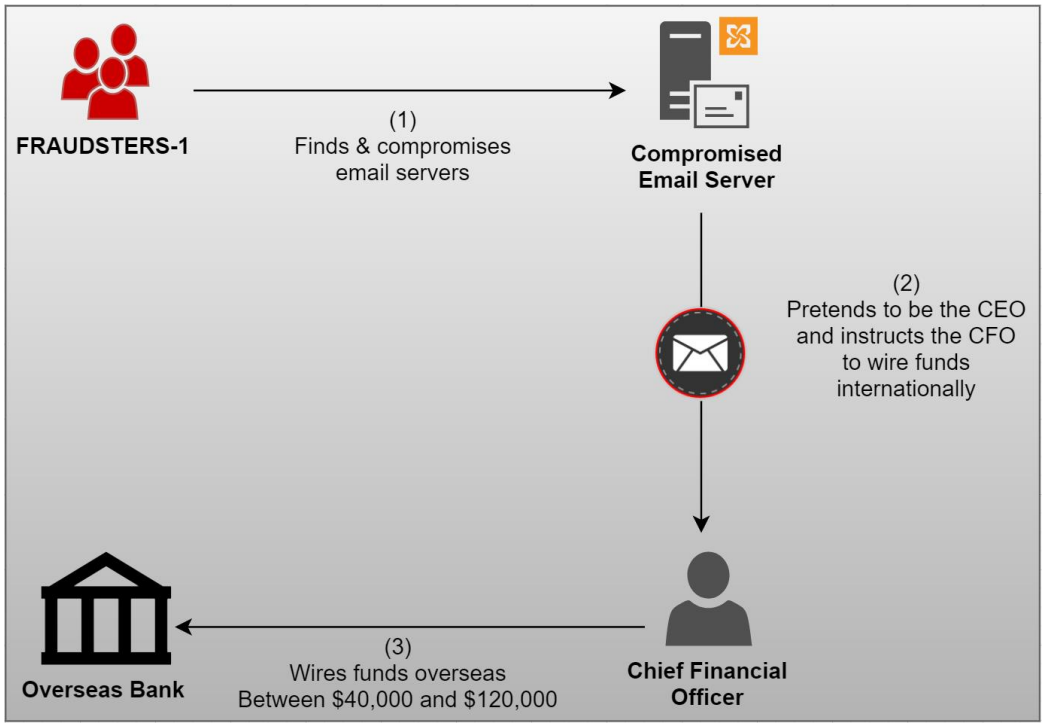

Figure 1 – Overview of FRAUDSTERS-1 Operation

The English language and grammar in their emails is flawless, and they employ numerous social engineering techniques such as calibrated questions, "no" questions, labels, and pretexting. Any successful attack results in deceiving the CFO into wiring funds to money-mules located in South East Asian countries such as Malaysia, Hong Kong and Vietnam.

TAKING ADVANTAGE OF EMAIL INTERFACES

Some email clients only display the sender's first and last names. Their interfaces hide the full email of the sender. Email applications on mobile and tablets were found to be affected by this issue more often than thick-clients. See the image to the right for an example.

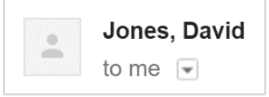

Figure 2 – Email Interface

FRAUDSTERS-1 uses this interface vulnerability to help them hide that they are issuing emails from incorrect email addresses.

ATTACK EXAMPLE

For confidentiality reasons, all client specific information has been removed from the following email samples and the real names of the people have been changed. All other details are authentic.

Email 1: Leading with a "no" question

From:	"David Jones" <david.jones@businessadvisoryfirm.com>
To:	"Kate Myers" <kate.myers@victim.com.au>

Kate,

Is there any reason why we couldn't wire funds to Hong Kong if we chose to work with a supplier located there?

Thank you, David.

Chief Executive Officer

Unsophisticated social engineers would have emailed the CFO, Kate Myers, with a fake invoice and gone straight to asking for payment. However, FRAUDSTERS-1 chooses to start interacting with its victims using a "no" question meant to confirm that international wire transfers are possible and uncovering any roadblocks that could prevent payments.

Email 2: Following with a calibrated "how" or "what" question

From:	"David Jones" <david.jones@businessadvisoryfirm.com>
To:	"Kate Myers" <kate.myers@victim.com.au>

Kate,

Thank you for confirming that international payments are possible.

What information do you need to onboard international suppliers and how fast can we move on a payment once they are onboarded?

Thank you, David.

Chief Executive Officer

On their second or third email communication, FRAUDSTERS-1 uses a calibrated "how" or "what" question to start leading the CFO into making an international wire payment to a fictitious supplier. What is particularly powerful with this approach is that the attackers are at no point asking for permission (yes or no) or attempting to use force against the CFO to get the funds wired. Instead, they are gently manipulating the CFO in a way that is almost undetectable to an untrained person.

Email 3: Going for the kill using deadlines

From:	"David Jones" <david.jones@businessadvisoryfirm.com>
To:	"Kate Myers" <kate.myers@victim.com.au>

Kate,

Thank you.

Below are the suppliers' details:

Account Beneficiary: XXXXXXXXXXX

Beneficiary Address: YYYYYYYYYYY

IBAN: AA11 2233 4455 6677 8899

SWIFT: XXXXXX

Is there any reason why we couldn't wire $49,895.65 to them today? Our company is responding to an emergency and we have signed an agreement to engage this supplier to help us.

Thank you, David.

Chief Executive Officer

Once again, FRAUDSTERS-1 uses a "no" question to identify any roadblocks that the victim may have to processing the payment. They also make use of deadlines to try and instil a sense of emergency in their target. Using deadlines is particularly effective against people who want to be helpful and work for companies that do not have proper procurement procedures to onboard and validate external vendors.

Email 4: Coming back for more

If the first wire was successful, FRAUDSTERS-1 re-initiates contacts with the victim and attempts to defraud them some more:

From:	"David Jones" <david.jones@businessadvisoryfirm.com>
To:	"Kate Myers" <kate.myers@victim.com.au>

Kate,

We are going to engage this company for additional services.

Could we wire an additional $135,652.12 to them today?

Thank you, David.

Chief Executive Officer

Of all of the email chains that we have reviewed, FRAUDSTERS-1 only makes blatant social engineering mistakes when it attempts to steal more funds from its victims. The most obvious of those mistakes is that the attackers were always seen to ask far too much more money the second time.

SOCIAL ENGINEERING TECHNIQUES EMPLOYED

The following table presents the main social engineering techniques FRAUDSTERS-1 employs:

Technique	Description	Example
Calibrated Question	A question that starts with "how" or "what" that gently and covertly leads the victim towards the target's goals. This technique is also extremely effective at identifying potential roadblocks ahead of time and diffusing them.	If we were to send money overseas, how would we do it?
Leading with "no" Question	A closed-ended question that elicits the victim to answer "no". This is much more effective than asking for "yes".	Is there any reason why we couldn't wire funds overseas?
Deadline	A technique to instil a sense of emergency into the victim and appealing to their desire to help.	How fast can you move on the payment? This is an emergency for us.
Pre-texting	A lie to coerce people into breaching security protocols or obtain unauthorised access to sensitive information.	Pretending to be someone they are not and inventing a bogus story about having to pay a supplier.
Complex Dollar Numbers	Instead of asking for a round dollar figure like $50,000.00, FRAUDSTERS-1 uses complex dollar figures like $49,895.65. Victims have reported to us that those complex figures made the fraudulent emails look and feel more trustworthy.	Using $49,895.65 instead of $50,000.00.

Table 1 – Social Engineering Techniques Employed

LAW ENFORCEMENT

All the clients that contacted us to help them deal with FRAUDSTERS-1 also contacted Australian law enforcement authorities. In all cases, they were told that nothing could be done to recuperate their lost funds.

RECOMMENDATIONS

Traditional security awareness training proved insufficient to defeat sophisticated social engineers. In this case, FRAUDSTERS-1 has mastered the art of influencing their victims via emails and on the phone. Thus, even employee capable of detecting traditional phishing emails were not been able to detect them until it was too late.

Recommendation 1: Implement proper procurement processes

Payment of invoices should only be allowed after the finance team has received an agreement with wet-signatures. Also, onboarding of new vendors and emergency same-day payments should require an authorisation in-person from the appropriate officer. In small companies, that may be the Chief Executive Officer.

Recommendation 2: Run tabletop social engineering exercises

Reading about social engineering attacks, or conducting basic security awareness is insufficient when facing sophisticated social engineers. Companies should hire expert anti-social-engineer trainers to run tabletop attack simulations in front of small classes. Employees should take turn at playing the social engineers and attempting to defeat them.

CONCLUSION

FRAUDSTERS-1 is one of the most sophisticated groups of social-engineers Mossé Security has responded to in Australia. Traditional security awareness and regular spear phishing tests that impart a culture of "not clicking on things" proved ineffective against this threat actor.

FRAUDSTERS-1's techniques worked against senior executives that are used to identifying deception in business. CFOs are the guardians of a company's money and are not easily manipulated into wiring funds to untrusted parties.

Every targeted cyberattack we have witnessed since 2015 had social engineering components to them. Attackers have elevated their level of deception and companies must invest in more advanced anti-social-engineering training for all their staff members.