Tackling CFO Fraud

Christopher Boyd – Lead Malware Analyst

Malwarebytes

Introductions

- Chris Boyd – Blogger / Researcher @ Malwarebytes
- 7 time Microsoft MVP in Consumer Security
- Malwarebytes – founded in 2008
- 400 employees, focused on infection landscape

The CFO Fraud Problem

- Fake CEOs, confused CFOs
- Businesses losing millions of dollars a year
- Simple threat, devastating consequences – no Malware required
- No second chances

CFO Fraud: Damage done

$750
million

7,000 US companies, 2013/15

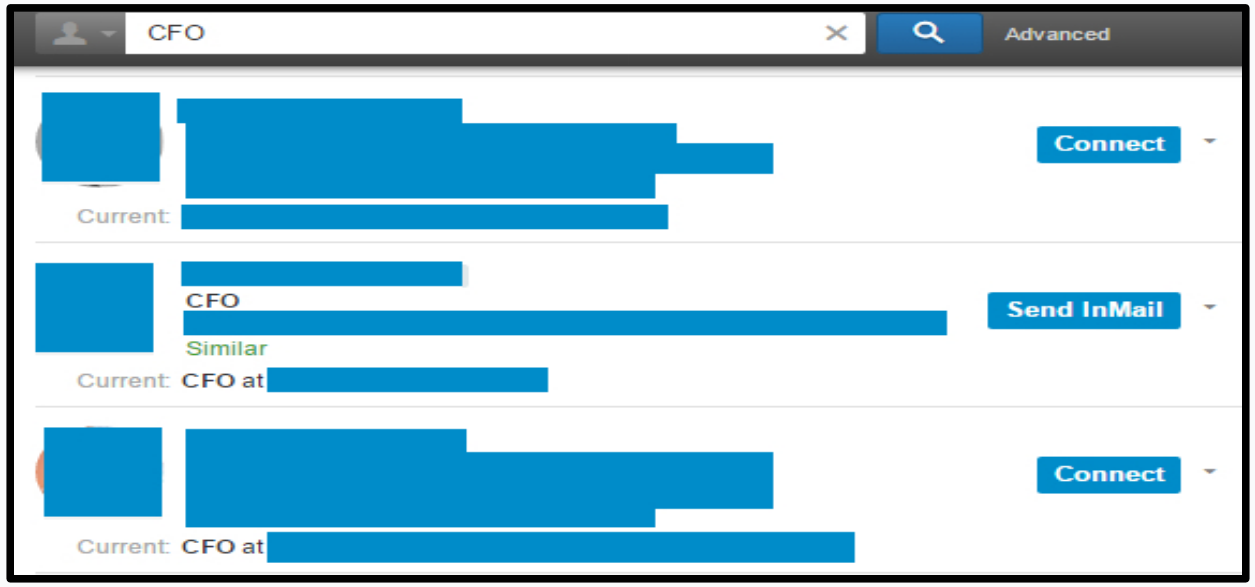
$1.2
billion

Internationally

270%
increase

In identified victims/losses

1) Linkedin: 374,836 results for CFO



2) Typosquat a URL

3) CFO mail sent from domain

From: Marcin Kleczynski [mailto:marcin@malwerabytes.com]
Sent: Wednesday, July 15, 2015 8:13 AM
To: Mark Harris
Subject: Fw:Wire Instruction

Mark,

Process the wiring instruction attached.Code this to professional services as a prepaid expense, and email me the confirmation when completed. I'll forward support later on. I am currently busy and I'll appreciate swift email correspondence.

$52,140.60

Keeping up the pressure: would you say no to your boss?

From: Marcin Kleczynski [mailto:marcin@malwerabytes.com]
Sent: Wednesday, July 15, 2015 9:19 AM
To: Mark Harris
Subject: RE: Fw:Wire Instruction

They are new Global Art vendors Proceed with wire transfer, and get back to me with the confirmation receipt. I will send supporting documentation and additional details later in the day. Email me ASAP.

From: Marcin Kleczynski [mailto:marcin@malwerabytes.com]
Sent: Wednesday, July 15, 2015 9:43 AM
To: Mark Harris
Subject: RE: Fw:Wire Instruction

Email me with confirmation receipt when completed.

"GLOBAL ART INC"
PNC BANK
BANK WIRE TRANSFER INSTRUCTIONS:

BANK: PNC BANK
ADDRESS: 11 PENN PLAZA, NY
NEW YORK, 10001 USA

ABA ROUTING NUMBER: 031207607
ACCOUNT NUMBER: 8110122742

AMOUNT: USD 52,140.60

CREDIT TO: GLOBAL ART INC.
4802 25TH AVE, ASTORIA
NEW YORK, 11103 USA

Action Items

Create a two-step system for authorising wires

Use a phone – but count the cost

Reduce social media/related HR footprint, and search for lost traces

More info: https://blog.malwarebytes.com/

Thank you!

Christopher Boyd

Malwarebytes