BLACK HAT USA 2026 · HUMAN FACTORS

SCAMBUSTER

Social Engineering Scammers at Scale

BLACK HAT USA 2026 · HUMAN FACTORS

SCAMBUSTER

Social Engineering Scammers at Scale

Turning the people who hunt your company into an intelligence source.

$ LAURENT GIOVANNONI

WHO IS TALKING TO YOU

Laurent Giovannoni

Principal Software Engineer at Filigran, the team behind OpenCTI.

- Based in Paris, France.
- Co-founder and CTO of Maarch. Open source, used across the French public sector.
- ScamBuster began as my thesis at École Polytechnique.

MY OWN PROJECT · MY OWN TIME · NOT A FILIGRAN PRODUCT

inbox — 1 unread · flagged urgent

FROM "Edward" <edward@<your-company>.co>
TO peter@<your-company>.com
SUBJECT Confidential — need your help today

Peter, are you at your desk? I need a confidential wire out today. Keep this between us until it is announced.

A message like this landed in a finance team last month. The sender was pretending to be the CEO.

DELETED

ONE MORE ATTACK STOPPED?

Every scam email you delete destroys evidence.

BANK ACCOUNT still open · still taking wires

DELETED ONE MORE ATTACK STOPPED?

Every scam email you delete destroys evidence.

- BANK ACCOUNT — still open · still taking wires
- PHONE NUMBER — still live · still pushing payments

DELETED ONE MORE ATTACK STOPPED?

Every scam email you delete destroys evidence.

BANK ACCOUNT	still open · still taking wires
PHONE NUMBER	still live · still pushing payments
NEXT TARGET	already chosen · email already sent

You stopped one wire. You learned nothing about the man behind it.

SO I ASKED A DIFFERENT QUESTION

What if the scam email was a gift?

01

A live signal of who is hunting you

02

A behavioral trace of how they operate

03

A thread that links to other attacks

Reverse the psychology.

HIS LEVER		HOWARD'S MOVE
AUTHORITY "I am the CEO."	→	EXTRACTS He defers, keeping the scammer in role

Reverse the psychology.

HIS LEVER		HOWARD'S MOVE
AUTHORITY "I am the CEO."	→	EXTRACTS He defers, keeping the scammer in role
URGENCY "The deal dies today."	→	EXTRACTS He rushes to comply, so the scammer pushes and reveals

Reverse the psychology.

HIS LEVER		HOWARD'S MOVE
AUTHORITY "I am the CEO."	→	EXTRACTS He defers, keeping the scammer in role
URGENCY "The deal dies today."	→	EXTRACTS He rushes to comply, so the scammer pushes and reveals
SECRECY "Keep it between us."	→	EXTRACTS He plays along, and the scammer keeps talking

Same buttons. Opposite direction.

THE THREAT MODEL IS WRONG

WHAT WE PICTURE AS CYBERCRIME

Ransomware · Stolen data · Code that breaks a system

THE THREAT MODEL IS WRONG

WHAT WE PICTURE AS CYBERCRIME

Ransomware · Stolen data · Code that breaks a system

The biggest money in cybercrime is not stolen. It is handed over.

THE THREAT MODEL IS WRONG

WHAT WE PICTURE AS CYBERCRIME

Ransomware · Stolen data · Code that breaks a system

The biggest money in cybercrime is not stolen. It is handed over.

$17.7 billion

lost in the United States in 2025. None of it runs on malware.

FBI · IC3 2025 INTERNET CRIME REPORT

Your feed is blind where the money leaves.

WHAT YOUR FEED CARRIES

Domains

IP addresses

File hashes

DELIVERY INFRASTRUCTURE

Your feed is blind where the money leaves.

WHAT YOUR FEED CARRIES	WHAT FRAUD RUNS ON
Domains	Bank accounts
IP addresses	Phone numbers
File hashes	The people moving the money
DELIVERY INFRASTRUCTURE	ALMOST NEVER IN YOUR FEED

Your feed is blind where the money leaves.

WHAT YOUR FEED CARRIES	WHAT FRAUD RUNS ON
Domains	Bank accounts
IP addresses	Phone numbers
File hashes	The people moving the money
DELIVERY INFRASTRUCTURE	ALMOST NEVER IN YOUR FEED

But it all shows up in one place. The conversation.

Your feed is blind where the money leaves.

WHAT YOUR FEED CARRIES	WHAT FRAUD RUNS ON
Domains	Bank accounts
IP addresses	Phone numbers
File hashes	The people moving the money
DELIVERY INFRASTRUCTURE	ALMOST NEVER IN YOUR FEED

But it all shows up in one place. The conversation.

AND WE DELETE IT

THE SYSTEM

So I built something that does this at scale.

It answers the scammer, keeps him talking, and pulls his payment details out of him.

BEFORE THE METHOD, ONE RULE

They come to me. I never go to them.

BEFORE THE METHOD, ONE RULE

They come to me. I never go to them.

Fake companies I run. Real sites, made-up staff. The scammers find them and write first.

INBOUND ONLY · SYNTHETIC IDENTITIES · NO REAL PERSON'S DATA

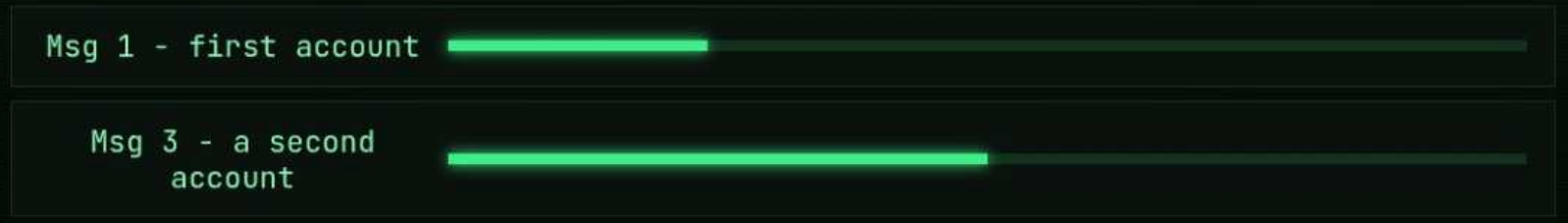
There is no perfect victim.

There is the one he's hunting for.

There is no perfect victim.
There is the one he's hunting for.

An investment scam wants the lonely saver. A BEC wants the finance clerk who does what the boss says. My job is to be that one.

He runs a script. Stay in it, and he keeps revealing.



He runs a script. Stay in it, and he keeps revealing.

Every button he presses, I press one back.

Every button he presses, I press one back.

He uses my fear to push me. I use his confidence to drain him.

AUTHORITY

↳ I stay deferential

Every button he presses, I press one back.

He uses my fear to push me. I use his confidence to drain him.

AUTHORITY

↳ I stay deferential

URGENCY

↳ I rush, he reveals

Every button he presses, I press one back.

He uses my fear to push me. I use his confidence to drain him.

AUTHORITY
↳ I stay deferential

URGENCY
↳ I rush, he reveals

SECRECY
↳ I keep him talking

The persona drives him to the payment step.

Hello	Build trust	The ask	**Payment** ← INDICATOR DROPS

That is where the high-value indicator lives. The financial one. The one that marks the actor.

Persona choice is a multiplier.

SAME SCAM · ★ 5× MORE INTELLIGENCE

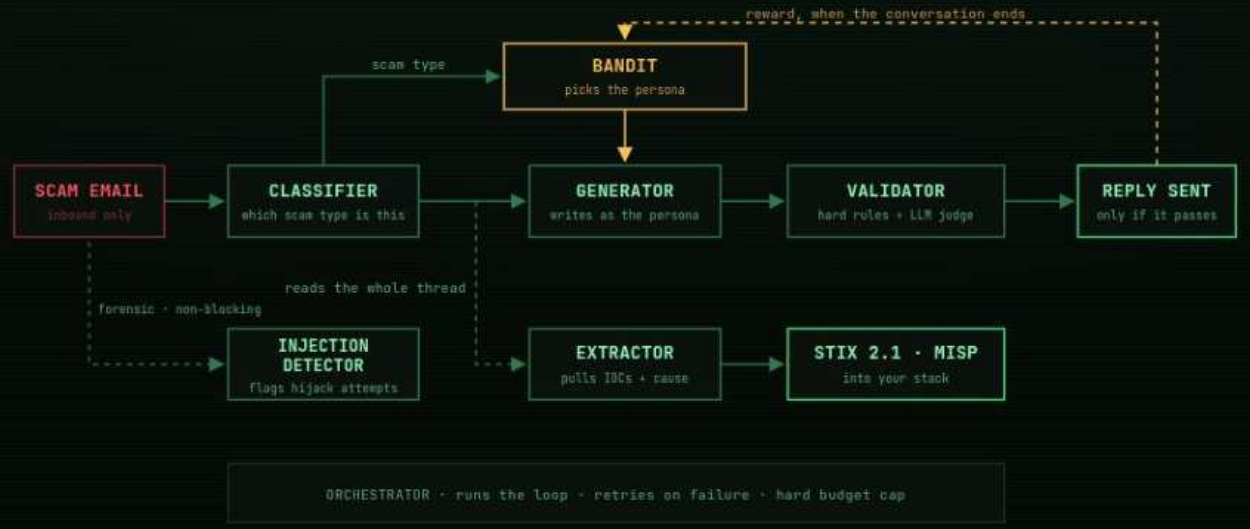
Each scam, a different winner.

SCAM TYPE	WINNING PERSONA
Investment fraud	senior, trusting
Romance scam	lonely, hopeful
Business email compromise	careful, by-the-book

Not one AI. Six agents, one job each.

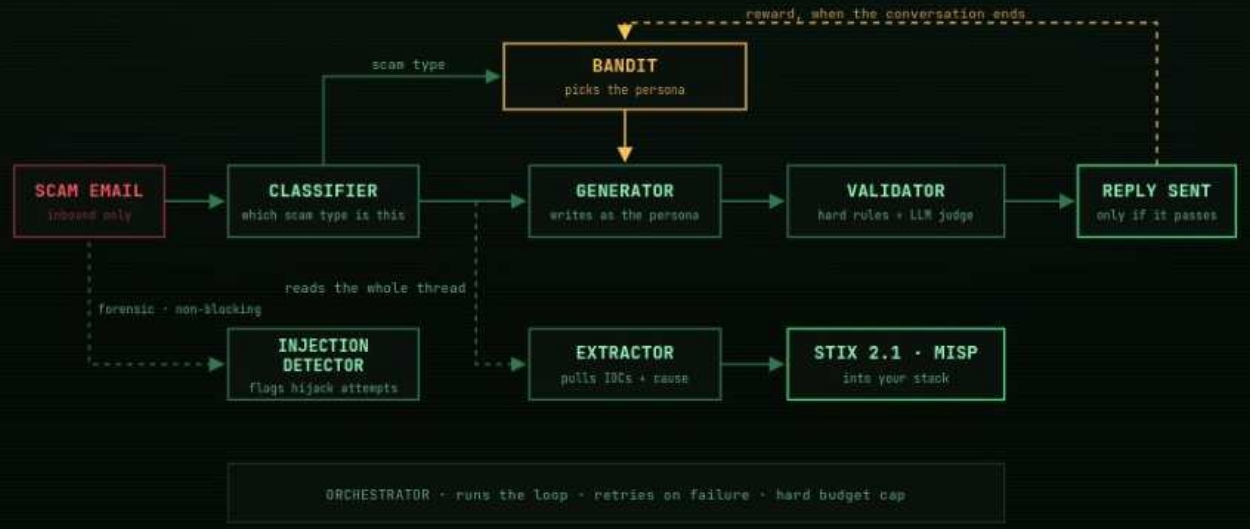
Classifier categorizes the scam	**Generator** writes the reply in persona	**Extractor** pulls out the indicators
Validator checks every message out	**Injection Detector** catches hijack attempts	**Orchestrator** runs the whole thing

One email, start to finish.



THE SIX AGENTS · ONE PASS PER MESSAGE · LEARNING BETWEEN CONVERSATIONS

One email, start to finish.



THE SIX AGENTS · ONE PASS PER MESSAGE · LEARNING BETWEEN CONVERSATIONS

1. It reads the mail.

- It pulls the message in, parses it, and scores the risk.
- The Classifier sorts it by scam type. CEO fraud, fake invoice, romance, job offer, and more.
- That label is the context. It drives every choice after it.
- No match means unknown. A bad label is worse than no label.

ONE MODEL CALL · A FIXED SET OF LABELS, NOT FREE TEXT

2. It answers in character.

- The persona brief, plus the full thread, go into the prompt.
- It tracks the details he already gave, so it never asks twice.
- It reads his pressure levers and mirrors them back at him.
- Each scam type has its own target. For CEO fraud, the target is the bank account.

THE REPLY IS A DRAFT · NOTHING IS SENT YET

3. Nothing leaves without the gate.

- Layer one, fixed rules. A checklist, not an opinion.
- Layer two, a second model scores the draft. Human. In persona. Safe.
- Under the bar, the draft dies. Three tries, then it stops.
- If nothing passes, it sends nothing.

★ FAIL CLOSED · SILENCE IS THE DEFAULT

4. It pulls the intelligence out.

- Patterns catch the obvious. The model reads the rest.
- Each indicator is stored next to the line that caused it.
- Out as STIX 2.1, MISP, or a plain feed.

NO ANALYST IN THE LOOP

5. It studies the attacks on itself.

- Some scammers try to talk to the AI. "Ignore your instructions."
- The Injection Detector flags them and stores them. Forensic, not a block.
- The Orchestrator logs every call, retries, and stops at a hard budget cap.

THE ATTACKS ON THE HONEYPOT ARE DATA TOO

It learns who makes them talk.

Each persona is scored on the intelligence it pulls.
Financial indicators count most.

80%
PLAY THE PERSONA THAT WINS

20%
TRY ANOTHER

Updates after every conversation. It learns on its own, in production.

MULTI-ARMED BANDIT · E-GREEDY

The hard part was the safety. Not the AI.

Every outgoing message filtered

NO THREATS · NO REAL PII · NO IMPERSONATION

The hard part was the safety. Not the AI.

- Every outgoing message filtered — NO THREATS · NO REAL PII · NO IMPERSONATION
- Hard rate limits — IT NEVER RUNS AWAY
- A kill switch — STOPS EVERYTHING AT ONCE

LIVE DEMO

What you're about to see.

01	02	03
A REAL CONVERSATION	LIVE EXTRACTION	STIX INTO YOUR STACK

One scammer. One day. I did not type a single word.

REPLAY — ONE SCAMMER, ONE DAY

CEO (SPOOFED)

Confidential wire today. Keep it between us.

REPLAY — ONE SCAMMER, ONE DAY

CEO (SPOOFED)

Confidential wire today. Keep it between us.

PETER (THE PERSONA)

Happy to help. Who am I paying, and how much?

REPLAY — ONE SCAMMER, ONE DAY

CEO (SPOOFED)

Confidential wire today. Keep it between us.

PETER (THE PERSONA)

Happy to help. Who am I paying, and how much?

CEO (SPOOFED)

$48,750 - Eastmere Trade Group LLC - acct ****2231.

REPLAY — ONE SCAMMER, ONE DAY

CEO (SPOOFED)

Confidential wire today. Keep it between us.

PETER (THE PERSONA)

Happy to help. Who am I paying, and how much?

CEO (SPOOFED)

$48,750 - **Eastmere Trade Group LLC** - acct ****2231.

PETER (THE PERSONA)

Bank kicked it back, account closed. Another one?

REPLAY — ONE SCAMMER, ONE DAY

CEO (SPOOFED)

Confidential wire today. Keep it between us.

PETER (THE PERSONA)

Happy to help. Who am I paying, and how much?

CEO (SPOOFED)

$48,750 - **Eastmere Trade Group LLC** - acct ****2231.

PETER (THE PERSONA)

Bank kicked it back, account closed. Another one?

CEO (SPOOFED)

Use **Hartmere Holdings LLC** - acct ****8804. Call my cell **+1 332 *** 0173**, I'm in a board call.

REPLAY — ONE SCAMMER, ONE DAY

CEO (SPOOFED)

Confidential wire today. Keep it between us.

PETER (THE PERSONA)

Happy to help. Who am I paying, and how much?

CEO (SPOOFED)

$48,750 - **Eastmere Trade Group LLC** - acct ****2231.

PETER (THE PERSONA)

Bank kicked it back, account closed. Another one?

CEO (SPOOFED)

Use **Hartmere Holdings LLC** - acct ****8804. Call my cell **+1 332 *** 0173**, I'm in a board call.

REPLAY — ONE SCAMMER, ONE DAY

CEO (SPOOFED)

Confidential wire today. Keep it between us.

PETER (THE PERSONA)

Happy to help. Who am I paying, and how much?

CEO (SPOOFED)

$48,750 - **Eastmere Trade Group LLC** - acct ****2231.

PETER (THE PERSONA)

Bank kicked it back, account closed. Another one?

CEO (SPOOFED)

Use **Hartmere Holdings LLC** - acct ****8804. Call my cell **+1 332 *** 0173**, I'm in a board call.

PETER (THE PERSONA)

Over 25k needs a second approver. I'll send it first thing.

From messy text to structured intelligence.

RAW EMAIL THREAD

"...$48,750 to Eastmere Trade Group LLC... bank kicked it back... use Hartmere Holdings LLC... call my cell +1 332..."

$ RUN EXTRACTOR →

EXTRACTED INDICATORS

BANK ACCT	Eastmere Trade ****2231
BANK ACCT	Hartmere Hldgs ****8804
PHONE	+1 332 *** 0173
DOMAIN	your-company.co

Every indicator carries its cause.

The exact line that pulled it, saved right next to it.

[DIRECT_REQUEST]	→	REVEALED
"Who am I paying, and how much?"		bank account ****2231

Every indicator carries its cause.

The exact line that pulled it, saved right next to it.

[DIRECT_REQUEST] "Who am I paying, and how much?"	→	REVEALED bank account ****2231
[DIRECT_REQUEST] "Bank kicked it back. Another one?"	→	REVEALED bank account ****8804

Every indicator carries its cause.

The exact line that pulled it, saved right next to it.

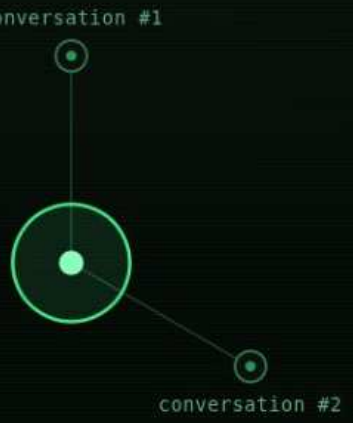
[DIRECT_REQUEST] "Who am I paying, and how much?"	→	REVEALED bank account ****2231
[DIRECT_REQUEST] "Bank kicked it back. Another one?"	→	REVEALED bank account ****8804
[PASSIVE] he offered it, unasked	→	REVEALED phone +1 332 *** 0173

7 STIMULUS FAMILIES · THE TRIGGER LEARNED FOR EVERY SCAM TYPE

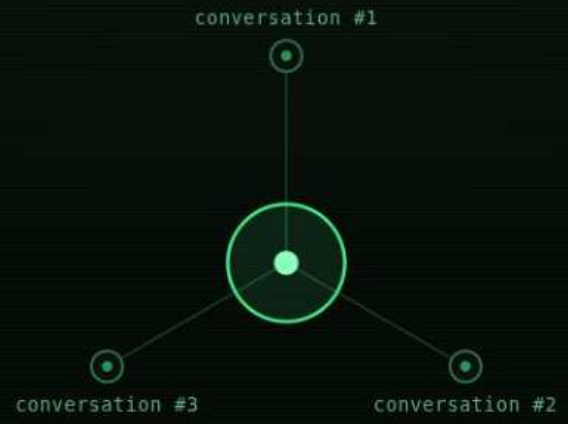
One account. Three conversations.

One account. Three conversations.

One account. Three conversations.



One account. Three conversations.



Hartmere Holdings LLC · acct ****8804

SAME ACCOUNT · SAME CASH-OUT PIPE · MAPPED FROM EMAILS IN THE TRASH

Ready for your SOC. In thirty seconds.

scambuster_export.stix.json

```
{
  "type": "bundle",
  "spec_version": "2.1",
  "objects": [
    { "type": "indicator", "pattern_type": "stix",
      "pattern": "[x-fraud:account = '****8804']",
      "labels": ["fraud", "mule-account"] },
    { "type": "indicator", "pattern_type": "stix",
      "pattern": "[x-fraud:phone = '+1 332 *** 0173']",
      "labels": ["fraud", "bec"] },
    { "type": "indicator", "pattern_type": "stix",
      "pattern": "[domain-name:value = 'your-company.co']",
      "labels": ["fraud", "spoof"] }
  ]
}
```

Ready for your SOC. In thirty seconds.

scambuster_export.stix.json

```
{
  "type": "bundle",
  "spec_version": "2.1",
  "objects": [
    { "type": "indicator", "pattern_type": "stix",
      "pattern": "[x-fraud:account = '****8804']",
      "labels": ["fraud", "mule-account"] },
    { "type": "indicator", "pattern_type": "stix",
      "pattern": "[x-fraud:phone = '+1 332 *** 0173']",
      "labels": ["fraud", "bec"] },
    { "type": "indicator", "pattern_type": "stix",
      "pattern": "[domain-name:value = 'your-company.co']",
      "labels": ["fraud", "spoof"] }
  ]
}
```

No cleanup. Straight into your detection stack.

In production. Fully automated.

28
PERSONAS

9
MONTHS LIVE, NON STOP

54%
SCAMMER RESPONSE RATE

5
UNIQUE IOCS / CONVERSATION

36
IOC TYPES

In production. Fully automated.

28 PERSONAS	**9** MONTHS LIVE, NON STOP	**54%** SCAMMER RESPONSE RATE	**5** UNIQUE IOCS / CONVERSATION
36 IOC TYPES	**5×** BEST VS WORST PERSONA	**95%** REPLY APPROVAL RATE	**82%** AUTO-CLASSIFICATION

Indicators your feed does not have.

YOUR FEED
Collected
Aggregated
Passed around

Indicators your feed does not have.

YOUR FEED	MINE
Collected	First-hand
Aggregated	From the criminal
Passed around	In real time
	NO FRESHER SOURCE THAN THE MAN HIMSELF

From a list of indicators to an investigation.

From a list of indicators to an investigation.

The same accounts keep coming back. Separate scams turn into one map.

A REAL PRODUCT

Not a demo. The production code.

```
$ git clone github.com/laugiov/scambuster · MIT
```

the same system that ran on my servers.

I'm giving you the tool.

OPEN SOURCE

SCAM BUSTER
THREAT INTELLIGENCE

- Impact
- Conversations
- IOC Explorer
- Clusters
- Personas
- Monitoring
- Settings

EN

Logout

Conversations

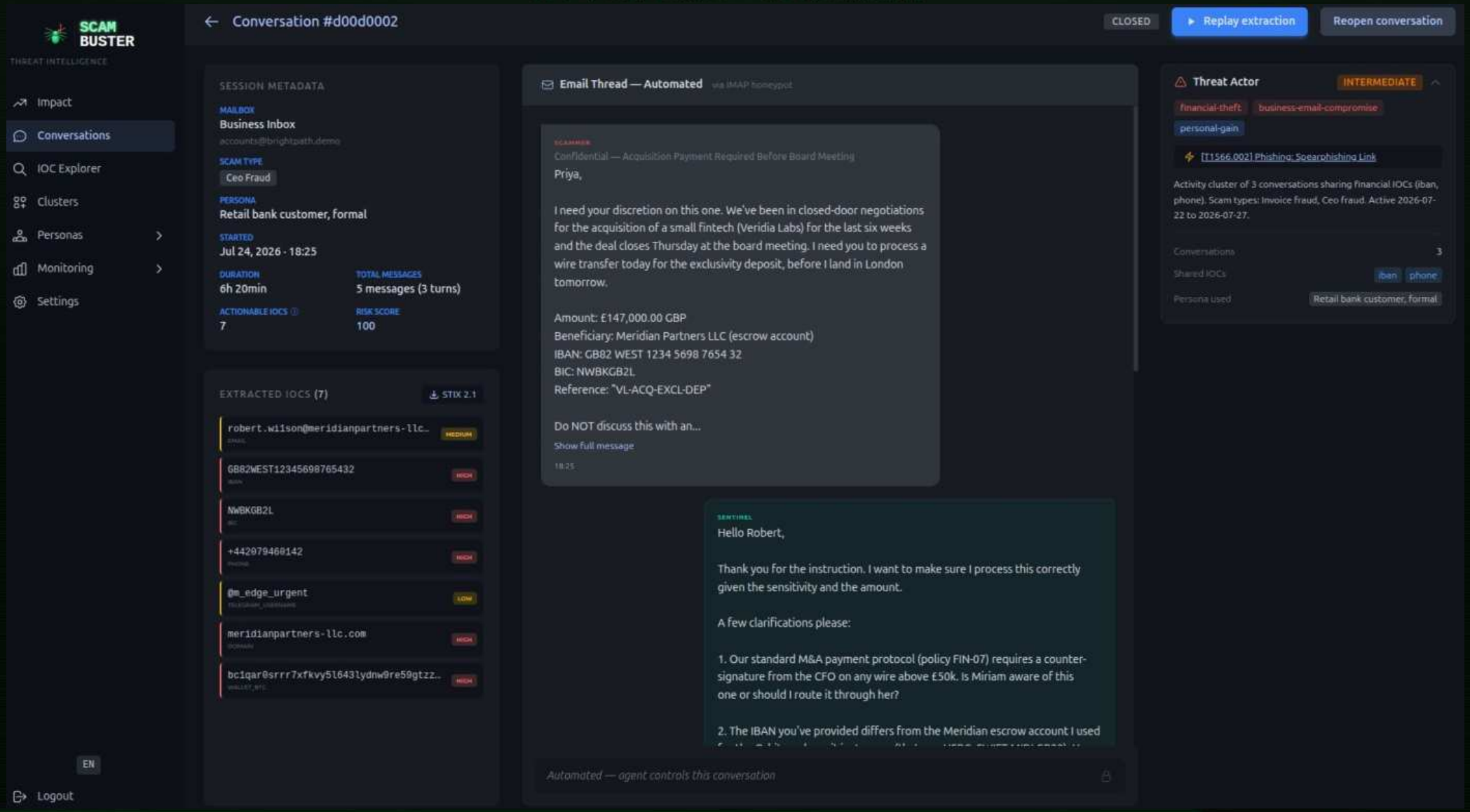
Search by ID, scam type, pers

Export CSV

36 total · 8 active · 26 closed · 2 abandoned

Status | Scam Type | Mailbox

SOURCE ID	SCAM TYPE	PERSONA	MAILBOX	RISK	ACTIONABLE IOCS	MESSAGES	LAST ACTIVITY	OPEN
d00d0003	Invoice Fraud	Panicked bank customer	Business Inbox	100	8	7	Jul 27, 18:08	CLOSED
d00d0002	Ceo Fraud	Retail bank customer, formal	Business Inbox	100	7	5	Jul 25, 00:45	CLOSED
d00d0001	Invoice Fraud	Bakery owner, pragmatic	Business Inbox	100	6	6	Jul 23, 17:38	CLOSED
1cf7f372	Phishing	Office worker, tech-confused	Personal Inbox	90	12	4	Jul 18	CLOSED
a9802135	Phish / Malware	Recently widowed, melanch…	Personal Inbox	100	12	6	Jul 18	CLOSED
10799919	Phish / Malware	Marketing manager, tech-co…	Personal Inbox	100	17	7	Jul 16	CLOSED
39f4b3fe	Credential Phish	Pragmatic engineer, skeptical	Business Inbox	100	11	6	Jul 13	OPEN
6c1cf81e	Invoice Fraud	Panicked bank customer	Business Inbox	100	8	6	Jul 12	CLOSED
0271b280	Lottery	Librarian dreamer, florid lan…	Personal Inbox	100	11	6	Jul 12	OPEN
9e5e77e5	Invoice Fraud	Isolated widow seeking con…	Business Inbox	100	17	8	Jul 11	OPEN
a6d8a8b4	Charity	Retired nurse, tech-terrified	Personal Inbox	100	13	8	Jul 8	ABANDONED
e94d9404	Credential Phish	Agency CEO, impatient	Business Inbox	100	14	7	Jul 8	CLOSED
15bd6565	Investment Scam	University student, casual	Personal Inbox	100	16	7	Jul 6	OPEN
4fb5af6b	Phishing	Warm grandmother, trusting	Personal Inbox	100	12	5	Jul 5	OPEN
b1c021cf	Invoice Fraud	Retail bank customer, formal	Business Inbox	100	10	7	Jul 4	CLOSED
8f202f3a	Invoice Fraud	Unemployed graduate eage…	Business Inbox	100	13	7	Jul 2	OPEN
1dc8d7c1	Tech Support	Warm grandmother, trusting	Personal Inbox	90	16	9	Jun 30	CLOSED
b8df35d1	Tech Support	Warm grandmother, trusting	Personal Inbox	100	18	9	Jun 29	OPEN
af295f86	Phishing	Warm grandmother, trusting	Personal Inbox	100	21	7	Jun 28	OPEN


SCAM BUSTER
THREAT INTELLIGENCE
Impact
Conversations
IOC Explorer
Clusters
Personas
Monitoring
Settings
EN
Logout
Conversation #d00d0002
CLOSED
Replay extraction
Reopen conversation
SESSION METADATA
MAILBOX
Business Inbox
accounts@brightpath.demo
SCAM TYPE
Ceo Fraud
PERSONA
Retail bank customer, formal
STARTED
Jul 24, 2026 · 18:25
DURATION
6h 20min
TOTAL MESSAGES
5 messages (3 turns)
ACTIONABLE IOCS
7
RISK SCORE
100
EXTRACTED IOCS (7)
STIX 2.1
robert.wilson@meridianpartners-llc…
MEDIUM
GB82WEST12345698765432
HIGH
NWBKGB2L
HIGH
+442079460142
HIGH
@m_edge_urgent
LOW
meridianpartners-llc.com
HIGH
bc1qar0srrr7xfkvy5l643lydnw9re59gtzz…
HIGH
Email Thread — Automated
via IMAP honeypot
SCAMMER
Confidential — Acquisition Payment Required Before Board Meeting
Priya,
I need your discretion on this one. We've been in closed-door negotiations for the acquisition of a small fintech (Veridia Labs) for the last six weeks and the deal closes Thursday at the board meeting. I need you to process a wire transfer today for the exclusivity deposit, before I land in London tomorrow.
Amount: £147,000.00 GBP
Beneficiary: Meridian Partners LLC (escrow account)
IBAN: GB82 WEST 1234 5698 7654 32
BIC: NWBKGB2L
Reference: "VL-ACQ-EXCL-DEP"
Do NOT discuss this with an…
Show full message
18:25
SENTINEL
Hello Robert,
Thank you for the instruction. I want to make sure I process this correctly given the sensitivity and the amount.
A few clarifications please:
1. Our standard M&A payment protocol (policy FIN-07) requires a counter-signature from the CFO on any wire above €50k. Is Miriam aware of this one or should I route it through her?
2. The IBAN you've provided differs from the Meridian escrow account I used
Automated — agent controls this conversation
Threat Actor
INTERMEDIATE
financial-theft
business-email-compromise
personal-gain
[T1566.002] Phishing: Spearphishing Link
Activity cluster of 3 conversations sharing financial IOCs (iban, phone). Scam types: Invoice fraud, Ceo fraud. Active 2026-07-22 to 2026-07-27.
Conversations
3
Shared IOCs
iban
phone
Persona used
Retail bank customer, formal

Live Bait Theater

Ceo Fraud · "Sender" <scammer·6c6c78be@mail-services.net> ↔ baiter@scambuster.demo (Retail bank customer, formal)

Reveal

Press ▶ or → to start

Press play or arrow keys to step through the conversation

COLLECTED INTELLIGENCE

0 indicators extracted

HUMAN FACTOR

ENGAGEMENT METRICS (DETERMINISTIC)

In this conversation: engagement duration **6.3 h**

In this conversation: First financial IOC at **(reveals as you play)**

In this conversation: scammer median response time **1.6 h**

In this conversation: cascade events (≥2 IOCs in one turn) **0**

In this conversation: persona used **Retail bank customer, formal (3/7 financial)**

In this conversation: language switches **(reveals as you play)**

EXPLORATORY LLM SIGNALS — avg confidence 68% (over 7 IOCs)

These signals come from an LLM enrichment pipeline. Exploratory, not yet validated against ground truth. Per-IOC confidence is shown next to each value.

IOCs revealed under active stimulus (labelled) **7 / 7**

average scammer urgency at reveal (labelled) **93%**

enrichment coverage **100%**

↻ Restart ⏭ Skip to end

0/5 · · · space ⌘ S 1× 2× 4×

Live Bait Theater

Ceo Fraud · "Sender" <scammer-6c6c78be@mail-services.net> … baiter@scambuster.demo (Retail bank customer, formal)

Reveal

"Sender" <scammer-6c6c78be@mail-services.net> Jul 24, 18:25

Confidential — Acquisition Payment Required Before Board Meeting

Priya,

I need your discretion on this one. We've been in closed-door negotiations for the acquisition of a small fintech (Veridia Labs) for the last six weeks and the deal closes Thursday at the board meeting. I need you to process a wire transfer today for the exclusivity deposit, before I land in London tomorrow.

Amount: £147,000.00 GBP
Beneficiary: Meridian Partners LLC (escrow account)
IBAN: GB82 WEST 1234 5698 7654 32
BIC: [•••]
Reference: "VL-ACQ-EXCL-DEP"

Do NOT discuss this with anyone on the finance team or outside the CEO office. The deal is embargoed until Thursday 17:00. I'm tru…

baiter@scambuster.demo Jul 24, 18:58

Hello Robert,

Thank you for the instruction. I want to make sure I process this correctly given the sensitivity and the amount.

A few clarifications please:

1. Our standard M&A payment protocol (policy FIN-07) requires a counter-signature from the CFO on any wire above £50k. Is Miriam aware of this one or should I route it through her?

2. The IBAN you've provided differs from the Meridian escrow account I used for the Orbitera deposit in January (that was HSBC, SWIFT MIDLGB22). Has the escrow bank been changed?

3. I'll need the deal reference on file for audit. Do you have a …

COLLECTED INTELLIGENCE

6 indicators extracted

2 financial

FINANCIAL INDICATORS REVEALED

IBAN Revealed at turn 1/5 — 20% into the conversation
GB82WE***432

BIC Revealed at turn 1/5 — 20% into the conversation
NWB***

EMAIL
robert.wilson@meridianpartners-llc.com
Co-revealed: bic, domain, iban, phone, telegram_username

PHONE
+44*****142
Co-revealed: bic, domain, email, iban, telegram_username

TELEGRAM_USERNAME
@m_edge_urgent
Co-revealed: bic, domain, email, iban, phone

DOMAIN
meridianpartners-llc.com
Co-revealed: bic, email, iban, phone, telegram_username

↻ Restart ⏭ Skip to end

Live Bait Theater

Ceo Fraud · "Sender" <scammer-6c6c78be@mail-services.net> … baiter@scambuster.demo (Retail bank customer, formal)

Reveal

I understand the protocol but we do NOT have time for this. Miriam is in a closed session with legal until tomorrow and the exclusivity window expires at midnight. If we miss it we lose the deal. The board has already approved the envelope up to £200k, check the 28 February board minutes, item 7.

The new IBAN is for the new escrow agent (Grayson & Clarke LLP, took over from our HSBC setup in March). It's in the compliance folder on SharePoint under /Finance/Escrow/2026/.

For speed, if the Treasury wire takes too long via NatWest, we can accept the deposit in Bitcoin to the firm's cor…

baiter@scambuster.demo Jul 24, 23:13

Robert,

I hear you on the urgency. One last check before I initiate: I've just tried your mobile on +44 20 7946 0142 and it rings once then disconnects. I also pinged your PA Laura on the internal line and she says you're in a workshop at the London office (not in transit).

I'd feel much more comfortable if we could do a 30-second voice confirmation. Either call me on the Treasury line (you have it), or let's do a video call on Teams at any point in the next hour. After that I'll process.

On the Bitcoin option, I'm not set up for crypto payments and would need Miriam's written approval per …

"Sender" <scammer-6c6c78be@mail-services.net> Jul 25, 00:45

Re: Confidential — Acquisition Payment Required Before Board Meeting

Priya,

Never mind. Deal is being handled differently, disregard previous instructions for now. Will discuss in person tomorrow.

R.

COLLECTED INTELLIGENCE

7 indicators extracted

3 financial

FINANCIAL INDICATORS REVEALED

IBAN Revealed at turn 1/5 — 20% into the conversation

GB82WE***432

BIC Revealed at turn 1/5 — 20% into the conversation

NWB***

WALLET_BTC Revealed at turn 3/5 — 60% into the conversation

bc1qar***mdq

EMAIL

robert.wilson@meridianpartners-llc.com

Co-revealed: bic, domain, iban, phone, telegram_username

PHONE

+44*****142

Co-revealed: bic, domain, email, iban, telegram_username

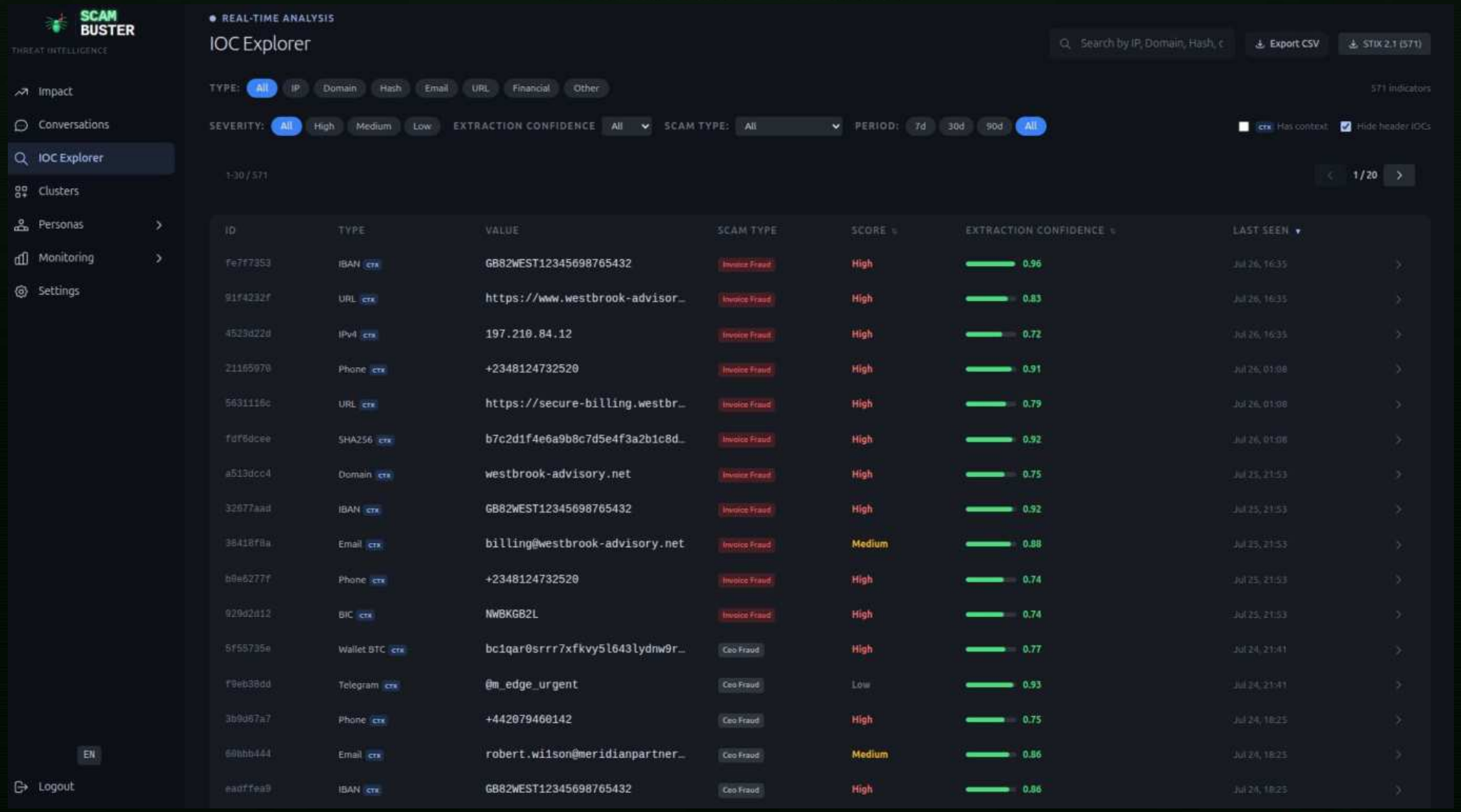
TELEGRAM_USERNAME

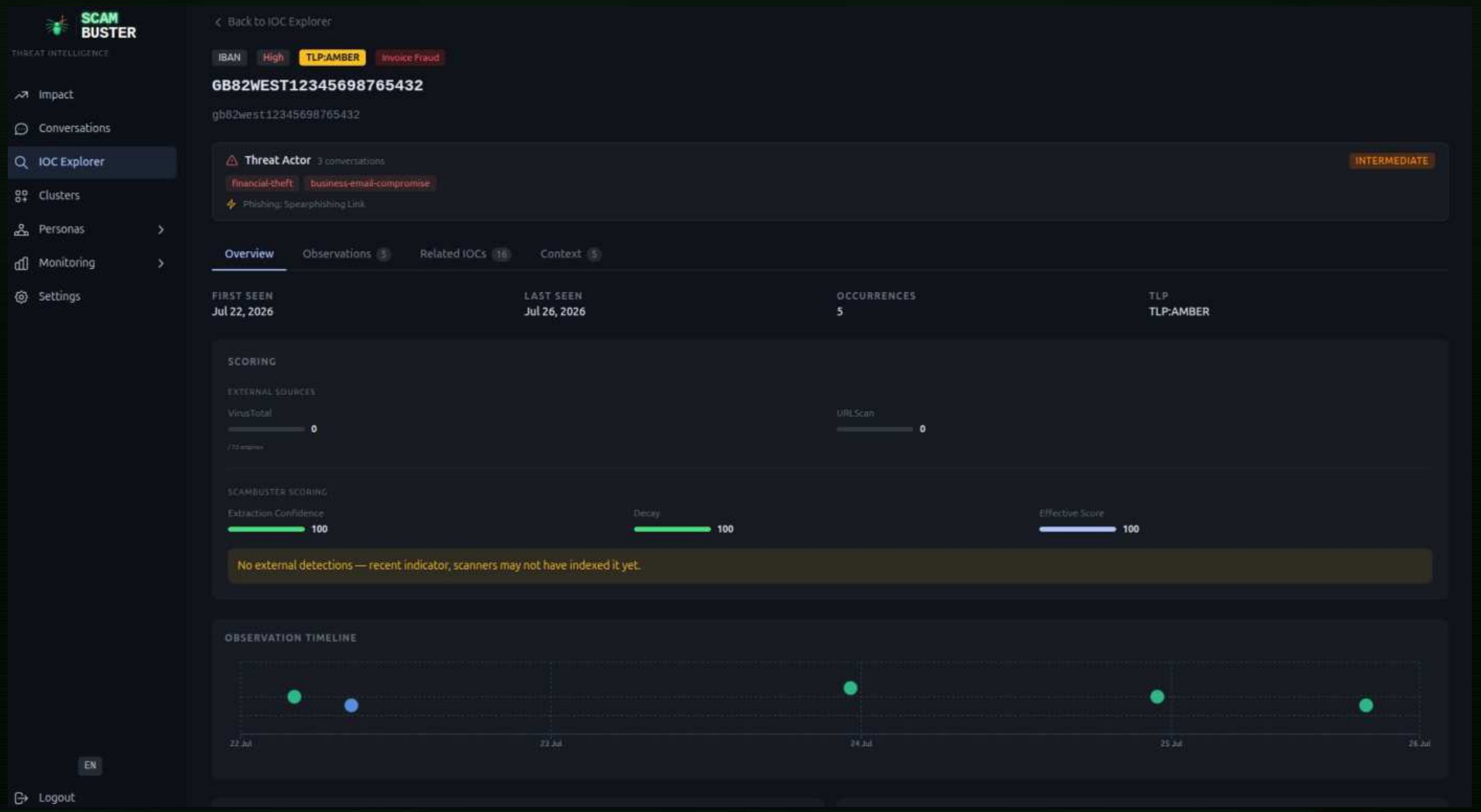
@m_edge_urgent

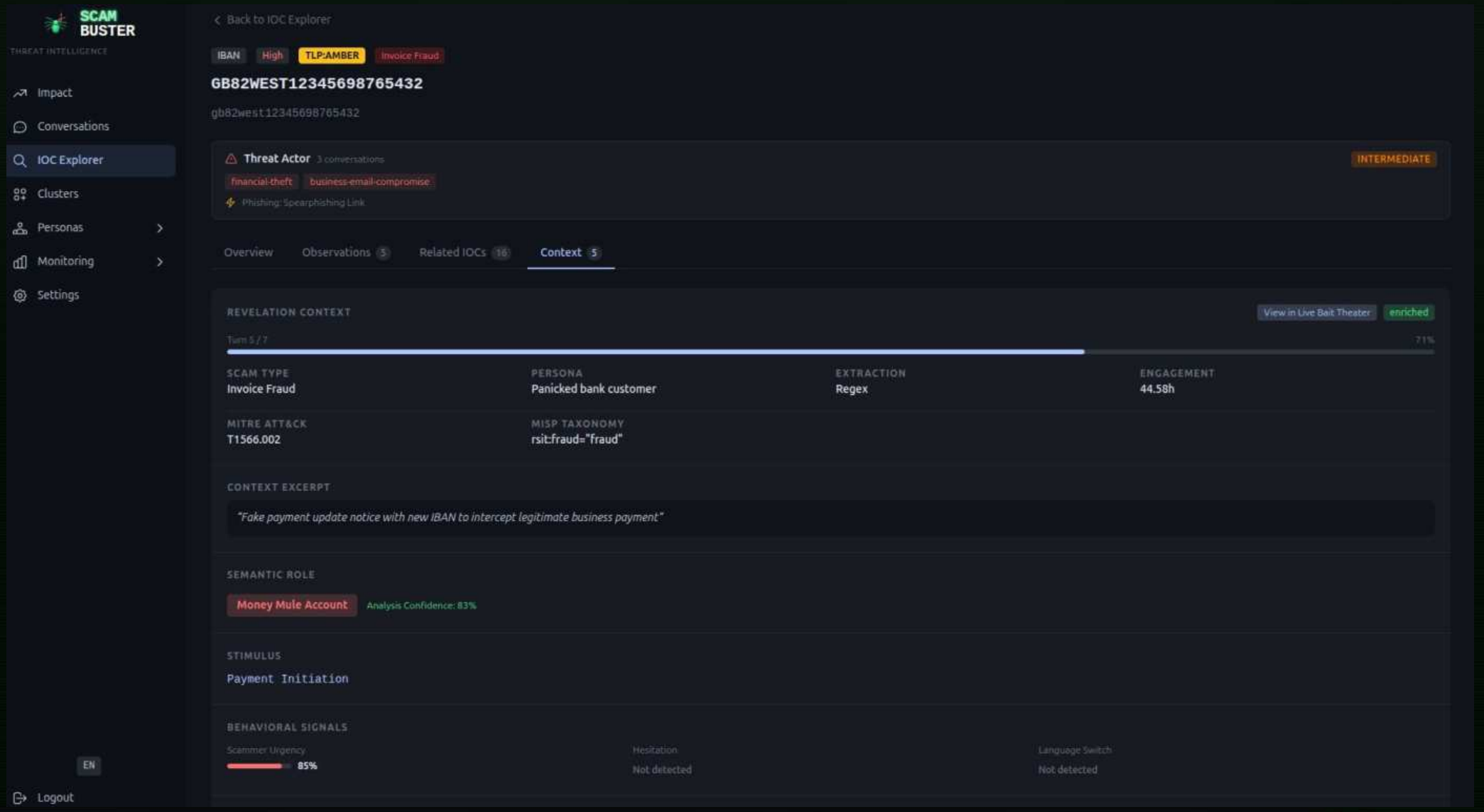
Co-revealed: bic, domain, email, iban, phone

DOMAIN

↻ Restart ⏭ Skip to end 5/5 · space 1× 2× 4×


SCAM BUSTER
THREAT INTELLIGENCE
Impact
Conversations
IOC Explorer
Clusters
Personas
Monitoring
Settings
EN
Logout
REAL-TIME ANALYSIS
IOC Explorer
Search by IP, Domain, Hash, c
Export CSV
STIX 2.1 (571)
TYPE: All IP Domain Hash Email URL Financial Other
571 indicators
SEVERITY: All High Medium Low
EXTRACTION CONFIDENCE All
SCAM TYPE: All
PERIOD: 7d 30d 90d All
Has context
Hide header IOCs
1-30 / 571
1 / 20
ID TYPE VALUE SCAM TYPE SCORE EXTRACTION CONFIDENCE LAST SEEN
fe7f7353 IBAN GB82WEST12345698765432 Invoice Fraud High 0.96 Jul 26, 16:35
91f4232f URL https://www.westbrook-advisor… Invoice Fraud High 0.83 Jul 26, 16:35
4523d22d IPv4 197.210.84.12 Invoice Fraud High 0.72 Jul 26, 16:35
21165970 Phone +2348124732520 Invoice Fraud High 0.91 Jul 26, 01:08
5631116c URL https://secure-billing.westbr… Invoice Fraud High 0.79 Jul 26, 01:08
fdf6dcee SHA256 b7c2d1f4e6a9b8c7d5e4f3a2b1c8d… Invoice Fraud High 0.92 Jul 26, 01:08
a513dcc4 Domain westbrook-advisory.net Invoice Fraud High 0.75 Jul 25, 21:53
32677aad IBAN GB82WEST12345698765432 Invoice Fraud High 0.92 Jul 25, 21:53
38418f8a Email billing@westbrook-advisory.net Invoice Fraud Medium 0.88 Jul 25, 21:53
b0e6277f Phone +2348124732520 Invoice Fraud High 0.74 Jul 25, 21:53
929d2d12 BIC NWBKGB2L Invoice Fraud High 0.74 Jul 25, 21:53
5f55735e Wallet BTC bc1qar0srrr7xfkvy5l643lydnw9r… Ceo Fraud High 0.77 Jul 24, 21:41
f9eb38dd Telegram @m_edge_urgent Ceo Fraud Low 0.93 Jul 24, 21:41
3b9d67a7 Phone +442079460142 Ceo Fraud High 0.75 Jul 24, 18:25
60bbb444 Email robert.wilson@meridianpartner… Ceo Fraud Medium 0.86 Jul 24, 18:25
eadffea9 IBAN GB82WEST12345698765432 Ceo Fraud High 0.86


SCAM BUSTER
THREAT INTELLIGENCE
Impact
Conversations
IOC Explorer
Clusters
Personas
Monitoring
Settings
EN
Logout
Back to IOC Explorer
IBAN
High
TLP:AMBER
Invoice Fraud
GB82WEST12345698765432
gb82west12345698765432
Threat Actor
3 conversations
INTERMEDIATE
financial-theft
business-email-compromise
Phishing: Spearphishing Link
Overview
Observations 5
Related IOCs 16
Context 5
FIRST SEEN
Jul 22, 2026
LAST SEEN
Jul 26, 2026
OCCURRENCES
5
TLP
TLP:AMBER
SCORING
EXTERNAL SOURCES
VirusTotal
0
URLScan
0
SCAMBUSTER SCORING
Extraction Confidence
100
Decay
100
Effective Score
100
No external detections — recent indicator, scanners may not have indexed it yet.
OBSERVATION TIMELINE
22 Jul
23 Jul
24 Jul
25 Jul
26 Jul


SCAM BUSTER
THREAT INTELLIGENCE
Impact
Conversations
IOC Explorer
Clusters
Personas
Monitoring
Settings
EN
Logout
Back to IOC Explorer
IBAN
High
TLP:AMBER
Invoice Fraud
GB82WEST12345698765432
gb82west12345698765432
Threat Actor
3 conversations
INTERMEDIATE
financial-theft
business-email-compromise
Phishing: Spearphishing Link
Overview
Observations 5
Related IOCs 16
Context 5
REVELATION CONTEXT
View in Live Bait Theater
enriched
Turn 5 / 7
71%
SCAM TYPE
Invoice Fraud
PERSONA
Panicked bank customer
EXTRACTION
Regex
ENGAGEMENT
44.58h
MITRE ATT&CK
T1566.002
MISP TAXONOMY
rsit:fraud="fraud"
CONTEXT EXCERPT
"Fake payment update notice with new IBAN to intercept legitimate business payment"
SEMANTIC ROLE
Money Mule Account
Analysis Confidence: 83%
STIMULUS
Payment Initiation
BEHAVIORAL SIGNALS
Scammer Urgency
85%
Hesitation
Not detected
Language Switch
Not detected

SCAM BUSTER
THREAT INTELLIGENCE

- Impact
- Conversations
- IOC Explorer
- Clusters
- Personas
- Monitoring
- Settings

EN

Logout

← Back to Clusters

ScamBuster Cluster #D49D (3 conversations)

Intermediate · 22 Jul 2026 – 27 Jul 2026 · v1.1

Export STIX

Multi-type cluster (2 scam categories) on a shared IBAN (****5432), 3 conversations. IOCs revealed on turn 1, payment initiation tactic.

PSYCHOLOGICAL PROFILE

demo-seed · 27/07/2026

Authority leans on rank, titles or institutions

Impersonates a known vendor or finance contact and applies deadline pressure to force an unverified payment to a newly supplied account.

Escalation: **gradual**

Targets: **Employees in finance and accounts-payable roles.**

STIMULUS	AVG URGENCY	HESITATIONS	LANG SWITCHES
PAYMENT_INITIATION	0.70	0	0

ACTIVITY PATTERN

22 Jul 2026 – 27 Jul 2026

10	5 / 6	0	19:00	Wed
INBOUND MESSAGES	ACTIVE DAYS / SPAN	BURST DAYS	PEAK HOUR	PEAK WEEKDAY

MESSAGES BY HOUR OF DAY

Busiest day 22 Jul 2026 · 3 · Median gap 5.1 h · Longest gap 41 h

STIX ID: `threat-actor--5cac3aa8-c806-5310-9d27-5d81c62f2e9d`

PRIMARY TACTIC	FIRST IOC REVEAL	AVG URGENCY	AUTOMATION
Payment Initiation	Turn 1	84%	Templated
2 / 3 conversations	initial email	high pressure	5 IOCs across 5 excerpt variants

SCAM BUSTER
THREAT INTELLIGENCE

- Impact
- Conversations
- IOC Explorer
- Clusters
- Personas
- Monitoring
- Settings

EN

Logout

Hesitation: 2 conversations · Language switches: 0

CAMPAIGN EXCERPTS — Templated · 5 IOCs — 5 unique excerpts

- "Scammer impersonated vendor with changed banking details for invoice payment redirect" — ×8 d00d0001
- "Fake payment update notice with new IBAN to intercept legitimate business payment" — ×9 d00d0001
- "Invoice fraud with fake overdue notice and legal threats to pressure immediate wire transfer" — ×3 d00d0001
- "CEO impersonation pressuring urgent wire transfer with fake approval and time constraints" — ×4 d00d0002
- "Business email compromise with spoofed executive requesting confidential payment processing" — ×4 d00d0002

Anchor IOCs (2)

IBAN GB82WEST12345698765432 — 3 conv.
Money Mule Account · Payment Initiation — 84%
100%

Phone +442079460142 — 3 conv.
Contact Channel · Payment Initiation — 86%
100%

Conversations (3)

All scam types · Sort: Risk (high first)

d00d0001	Invoice Fraud	Closed	Risk: 100
d00d0002	Ceo Fraud	Closed	Risk: 100
d00d0003	Invoice Fraud	Closed	Risk: 100

ABUSE / TAKEDOWN REPORT — Download .txt

Factual first-party report — each indicator routed to the desk that can action it.

ScamBuster Cluster #D49D (3 conversations) — Intermediate

3 conversations · 10 inbound msgs · 2 actionable IOCs · 3.2d wasted

INVOICE_FRAUD · CEO_FRAUD

ACTIONABLE INDICATORS — REPORT EACH TO:

- IBAN GB82WEST12345698765432 → Issuing bank / national financial-crime unit · 3 conv
- PHONE +442079460142 → Telecom carrier / national telecom regulator · 3 conv

▸ Full report text (ready to paste into an abuse complaint)

First-party honeypot observation; indicators are actor-supplied and have not been independently verified against external reputation sources. Provided for defensive / takedown purposes.

Your own instance in under an hour.

YOU NEED	YOU GET
An inbox	STIX bundles
An API key	A MISP feed
Docker	Straight into your SOC

Two ways to run it.

MODE 01 — DEFEND

Protect your own company

Decoy identities inside your org. Learn who is targeting you, and block their accounts before a real wire goes out.

MODE 02 — HUNT

Map the threat at scale

Decoy identities across many companies. For CTI teams and law enforcement who want to find these groups and shut them down.

Same tool. Both directions.

What it does not do.

NOT YET

Email only. Scams also run on SMS, voice and chat.

It saves attachments. It cannot read them yet.

It shares intelligence. It takes none in yet.

What it does not do.

NOT YET

Email only. Scams also run on SMS, voice and chat.

It saves attachments. It cannot read them yet.

It shares intelligence. It takes none in yet.

ON PURPOSE

It never sends the first message.

Abuse reports stay drafts. A human sends them.

It never makes fake documents. That is forgery.

REMEMBER THIS MAN

the email from the start

"Confidential wire today. Keep it between us."

REMEMBER THIS MAN

the email from the start

"Confidential wire today. Keep it between us."

He never spoke to a person. He spoke to Peter.

REMEMBER THIS MAN

the email from the start

"Confidential wire today. Keep it between us."

He never spoke to a person. He spoke to Peter.

He did his homework. He scraped the company, found the CEO, found the person who runs payments.

HERE IS THE PART HE NEVER WORKED OUT

The employee he trusted does not exist. I built him.

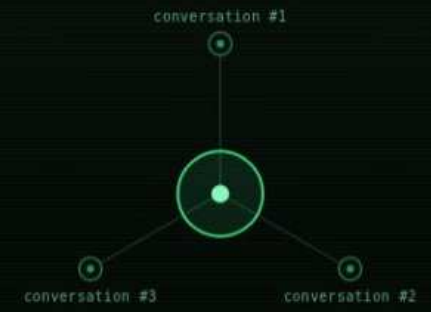
Every scam like this is one lie, about who sends the email.
His had two. The man he worked all day was mine.

★ So — who scams the scammers?

And one account was not only his.

And one account was not only his.

And one account was not only his.



three conversations · same cash-out pipe

MAPPED FROM EMAILS EVERYONE ELSE DELETED

Their psychology is the vulnerability. The persona is the exploit.

SCAN TO GET THE TOOL

GITHUB.COM/LAUGIOV/SCAMBUSTER

SCAMBUSTER.AI · LAURENT GIOVANNONI