Digital Forensics Alumni

Associazione
Digital Forensics Alumni

DFA Open Day 2018

I conti delle aziende sempre più a rischio a causa di phishing, malware e social engineering

… ovvero "come perdere un milione di euro attraverso la posta elettronica e accorgersene troppo tardi"

Paolo Dal Checco
Consulente Informatico Forense

Chi sono

- PhD @UniTO nel gruppo di Sicurezza delle Reti e degli Elaboratori
- In passato CTO c/o società di sviluppo software crittografici
- Albo CTU e Periti Procura/Tribunale Torino, CCIAA TO
- Professore a Contratto di Sicurezza Informatica @ UniTO (SUISS)
- Consulente Informatico Forense per Privati, Aziende, Avvocati, Procure, Tribunali, F.F.O.O.
- Tra i fondatori dell'Associazione DEFTA (www.deftlinux.net) e ONIF (www.onif.it)
- Direttivo Associazione IISFA, socio AIP, Tech & Law, Clusit, AssoB.it
- Contatti:
  - www.dalchecco.it / www.ransomware.it / www.bitcoinforensics.it
  - @forensico / paolo@dalchecco.it

Casistiche di truffe/furti alle aziende

- Man in the mail
- CEO Fraud
- Banking Trojan/Man in the Browser
- Dipendente Infedele (furto codice, client, know-how)
- Finti investimenti
- Ransomware (cifratura e ricatto / furto ed estorsione per non divulgare)

- **Cominciamo con il Man in The Mail…**

Tutto comincia con un cambio IBAN o richiesta bonifico…

- Motivazioni più svariate (conto in banca temporaneamente modificato, filiale estera, accertamenti/accreditamenti in corso, etc…)
- La richiesta proviene da fornitori, client (Man in The Mail)
- La richiesta di bonifico può arrivare da soci, colleghi ,collaboratori, legali, etc… (CEO Fraud)

Oppure era già cominciato prima?

- Spesso la richiesta di bonifico viene vista come l'inizio della truffa… ma in genere tutto comincia molto prima.
- Le attività d'infezione, phishing o social engineering iniziano anche mesi prima

Chi ci casca ancora?

- Fonte FBI/IC3 http://www.ic3.gov/media/2015/150122.aspx
  - From 10/01/2013 to 12/01/2014, the following statistics are reported:
  - Total U.S. victims: 1198
  - Total U.S. dollar loss: $179,755,367.08
  - Total non-U.S. victims: 928
  - Total non-U.S. dollar loss: $35,217,136.22
  - Combined victims: 2126
  - Combined dollar loss: **$214,972,503.30**

- Pesante **sottostima**, la realtà è ben peggiore
- *"The FBI assesses with high confidence the number of victims and the total dollar loss will continue to increase."*

Chi sono le vittime?

- Non è sempre l'azienda italiana la vittima
- Aziende che importano/esportano merce
- Manifatturiere con relazioni commerciali con paesi diversi
- Aziende la cui struttura è desumibile online
- Aziende con relazioni di fiducia con le banche
- Aziende con vulnerabilità su posta o poca educazione alla sicurezza
- Non sempre si punta ai conti, anche ai prodotti (spedizioni in destinazioni errate)

Se n'è parlato in TV…

… e sui giornali.

Così si sostituiscono al venditore

Hacker e falsi conti in banca per rubare soldi alle aziende

I consigli

Ti trovi in: Home Page › Sicurezza › Minacce

Aziende italiane vittime di frode via posta elettronica

9 COMMENTI

di Valerio Porcu, 12 novembre, 2014 12:46

Lo studio Di.Fo.B segnala una pericolosa truffa che sta colpendo molte società italiane e che passa dalla posta elettronica.

Mi piace 14 Tweet 7 Pin it Share 3 +1 1 Share 1

IBM ThinkPad T520i Monitor 15.6" LED Intel Core i3-2350..
ePRICE.it
€1179.99

IBM THINKPAD W540 CI7/4800MQ 1TB+ 256GBSSD 8GB 15.6IN N..
eGlobalMarket

È in corso una **truffa ai danni delle aziende di import/export** che ha colpito anche molte società italiane. Ne dà notizia lo studio Di.Fo.B di Torino, che spiega come una violazione della posta elettronica si sta rivelando il mezzo perfetto per ottenere bonifici fraudolenti e provocare ingenti perdite di denaro.

In sintesi, l'attacco consiste nel **violare la casella di posta elettronica della vittima**. Il primo passo è quindi un messaggio di phishing o un altro tipo di attacco che permetta di monitorare l'email e impostare un attacco del tipo man-in-the-middle (MITM).

IBM

Cremona/Palazzo Trecchi/Sala del teatro
Via Sigismondo Trecchi 20
19 novembre 17:00

ISCRIVITI SUBITO

La Provincia COBOX

Guarda anche: minacce sicurezza

Domande e Risposte

Hai un dubbio o una domanda? Chiedi alla nostra community!

Titolo Messaggio

Ma le truffe aumentano e si evolvono

- Non si tratta di trojan bancari (stile Zeus, Dridex, Dyre)
- Primi casi trattati personalmente dal 2011
- Le vittime e le cifre sono aumentate, le modalità evolute
- I criminali non si limitano più alla posta elettronica: telefonano (falsificando con **SpoofCard**), usano Skype o mandano fax
- I delinquent usano **SIM Swap**, chiedono spedizioni merce e non bonifici, possono acquisire dati e ricattare, criptare e ricattare, etc…



Ad aprile 2015 le FFOO agiscono…

LA STAMPA TECNOLOGIA

SEGUICI SU ACCEDI

Facebook lancia Moments, l'app per condividere foto in priva... | Arriva SOS-Matematica.it: la risposta gratis susmartphone ai... | Visual Computing a Modena, al via il primo Master universi... | Kickstarter arriva in Italia | Sony, tutti i nuovi videogiochi per PlayStation

Nigerian Drops: così donne e aziende erano truffate online (dall'Italia)

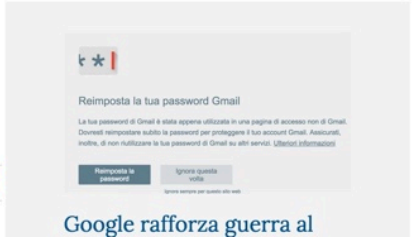
Pagamenti di imprese dirottati su conti esteri, signore adescate sui social: come operava un giro internazionale di frodi informatiche con epicentro a Torino.

Foto via Flickr/23905174@N00

Condividi 102 Tweet 16 +1 0

CAROLA FREDIANI 28/04/2015

LEGGI ANCHE



Google rafforza guerra al

…e nuovamente a giugno 2015

MAGAZINE | 10 giugno 2015

Phishing contro aziende: 62 arresti in Italia e all'estero, smantellata rete internazionale

CAROLA FREDIANI

COMMENTI

Foto via Flickr/23905174@N00

Tutto è partito da un **pagamento di 33mila euro**. Un'operazione di routine, un bonifico effettuato da **un'azienda veneta del settore alimentare**, che attraverso una sua consociata spagnola aveva pagato un proprio fornitore. O meglio, quello che pensava essere un proprio fornitore, non sospettando che dietro alla richiesta di un **cambio di codice Iban** su cui versare i soldi si celasse una organizzazione internazionale dedita a frodi informatiche a danno di imprese e riciclaggio. Che aveva prima hackerato il

Non solo in Italia, in tutta Europa

Press releases

Eurojust and Europol in massive joint action against cybercriminals

ES FR IT NL PL

Disclaimer: *The press releases above have been translated from the original version in the EN language. Eurojust cannot be held responsible for the quality of the translation. In the event of any discrepancies, please consult the original EN version of the press release.*

The Hague, 10 June 2015

Yesterday, a total of 49 suspects were arrested and 58 searches carried out in the framework of a massive joint action against cybercrime led by Italian, Spanish and Polish judicial and police authorities with the support of Belgium, the UK and Georgia. The action day represents the successful conclusion of three linked Eurojust cases coordinated by the Italian, Spanish and Polish National Desks, with Europol providing real-time support to the law enforcement authorities operating on the ground.

Da dove ~~vengono~~ si connettono i truffatori?

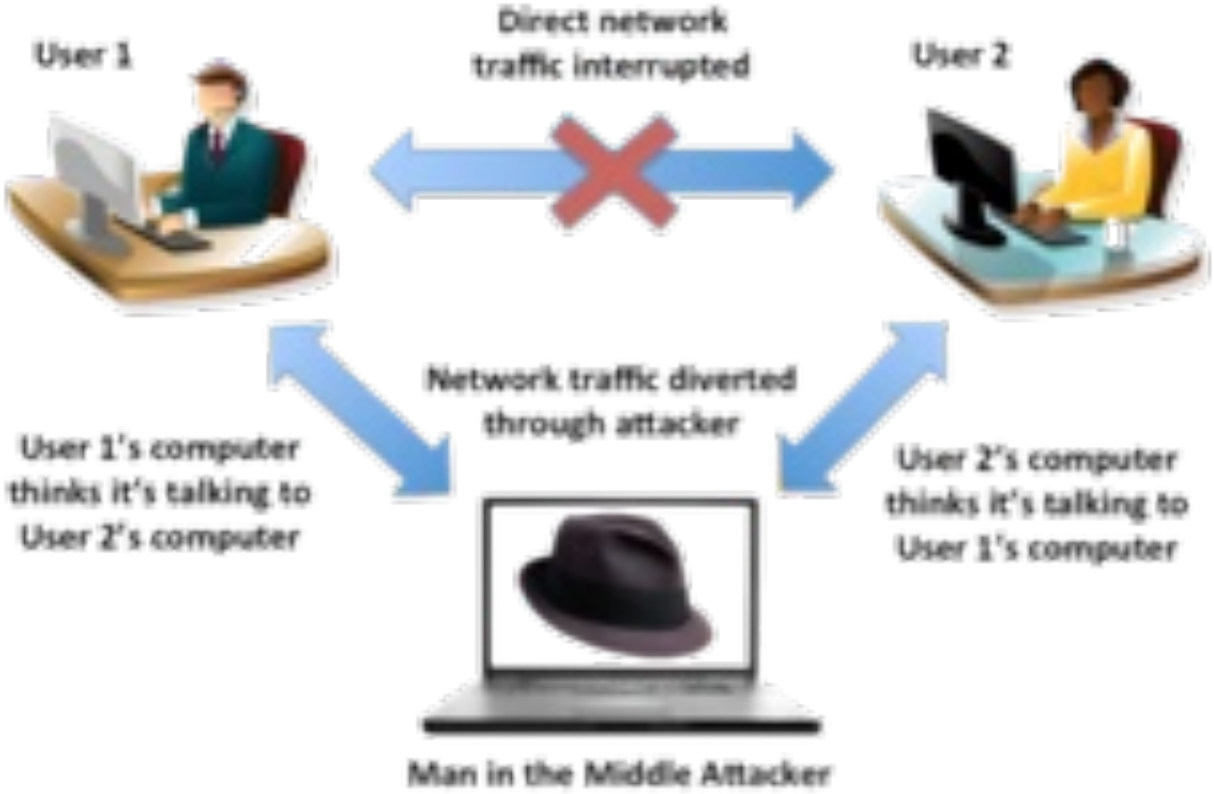
- "A gestire le attività di phishing era una rete di **nigeriani**, **camerunensi** e **senegalesi**, alcuni residenti in Italia." – LA STAMPA
- "The suspects, mainly from **Nigeria** and **Cameroon**, transferred the illicit profits outside of the European Union through a sophisticated network of money laundering transactions." – EUROJUST
- Il giro di money laundering (ma sembra anche di phishing) coinvolge **Italia**, **Spagna**, **Polonia**, **Belgio** e **Regno Unito**.

Alcuni riscontri diretti

- Durante alcune indagini difensive abbiamo operato anche noi delle attività di localizzazione (del tutto lecite ☺) confermando quanto rilevato dalle FFOO

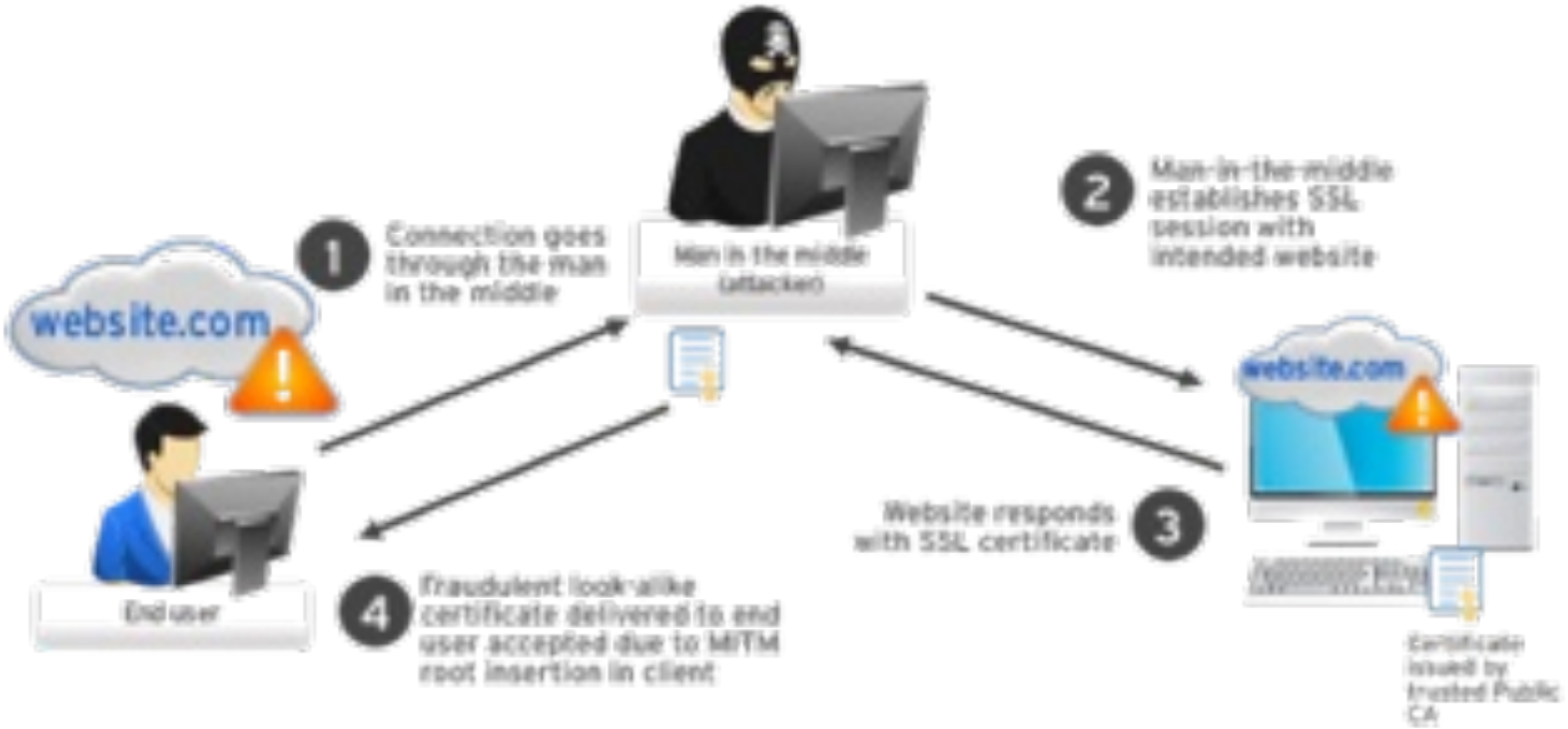
Man in the mail?

- Il termine deriva da "Man in the middle", noto per attività di sniffing e packet injection…



Man in the mail?

- … oppure nell hijacking di sessioni web tramite dns/arp poisoning, routing e certificati falsi



Man in the mail?

- Qui è tutto più "semplice", il delinquente:
  1. Entra nella posta di uno dei due interlocutori e si ascolta
  2. Crea una mail simile a quella di uno o di entrambi
  3. Si sostituisce a uno o a entrambi e si porta avanti la trattativa
  4. Sostituisce l'IBAN originale con il proprio
  5. Svuota il conto utilizzando dei muli
- sales@steelcompany.com diventa:
  - sales@steeelcompany.com
  - sales@steelcompany-com.gr (esempio di azienda greca)
  - sales-steelcompany@gmail.com

Come avviene l'intrusione?

- Brute Force
- Phishing
- Trojan
- Nessuna intrusione
  - Organigramma aziendale online
  - Leak (Facebook, Linkedin, Twitter, etc..)

A volte la modifica avviene direttamente sulla casella…

- Non sempre l'invio con la richiesta di bonifico fraudolento avviene da email esterne
- In alcuni casi i delinquent monitorano la casella e fanno le modifiche via IMAP, prima che il cliente faccia in tempo a guardare o scaricare la posta
- La mail sembra arrivare dall'indirizzo email reale, con header RFCC822 coerenti e corretti
  - Spesso in questo caso il consulente decreta che l'indirizzo compromesso è l'altro (quello corretto) oppure che si tratta di un insider

Senza domini è ancora più semplice…

- Spesso il delinquente non registra domini, usa free email
- Cambia il mittente nei dati di configurazione della webmail
- Le mail passano i controlli antispam

… soprattutto se la vittima usa Outlook

- Se si usano cliente come Outlook, il mittente visualizzato è il nome impostato dal delinquente, non il vero indirizzo
- Certamente cliccando su Reply si vedrà il vero indirizzo
- Spesso però non si presta attenzione o i domini/nick del «reply to» sono simili a quelli originali

Come prevedere le truffe?

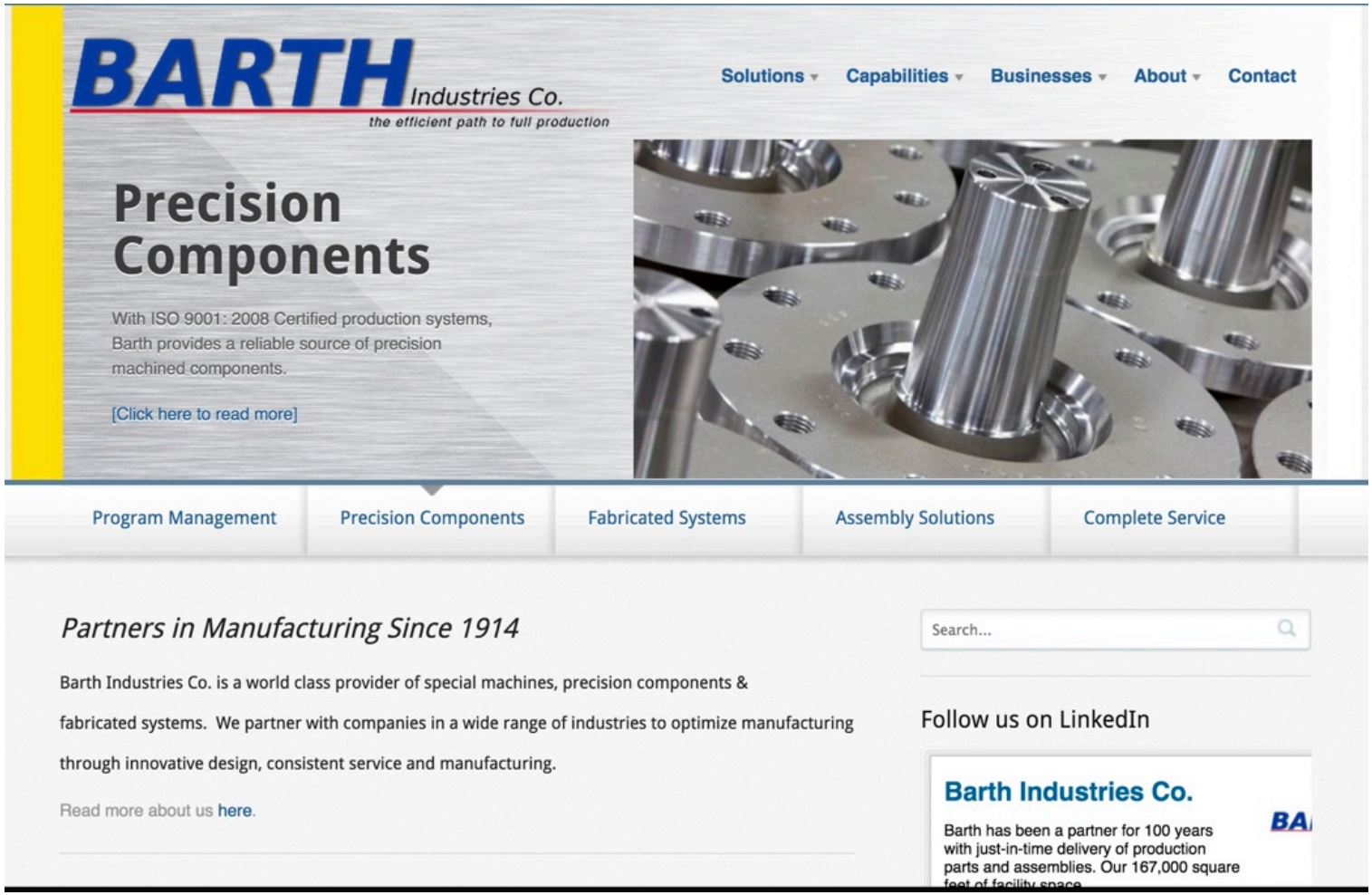
Come prevedere le truffe?

- Tramite alert su caratteristiche dei domini utilizzati dai truffatori si possono rilevaer e monitorare in tempo reale le future truffe (o vedere quelle in corso)
- Decine di alert ogni giorno, tra cui ad esempio:
  - barthindustriies.com -> barthindustries.com
  - aiengiineers.com -> aiengineers.com
  - foundatiionfitness.net -> foundationfitness.net
  - ameriicansnuff.com -> americansnuff.com
- Ho già provato ad avvisarne alcuni…

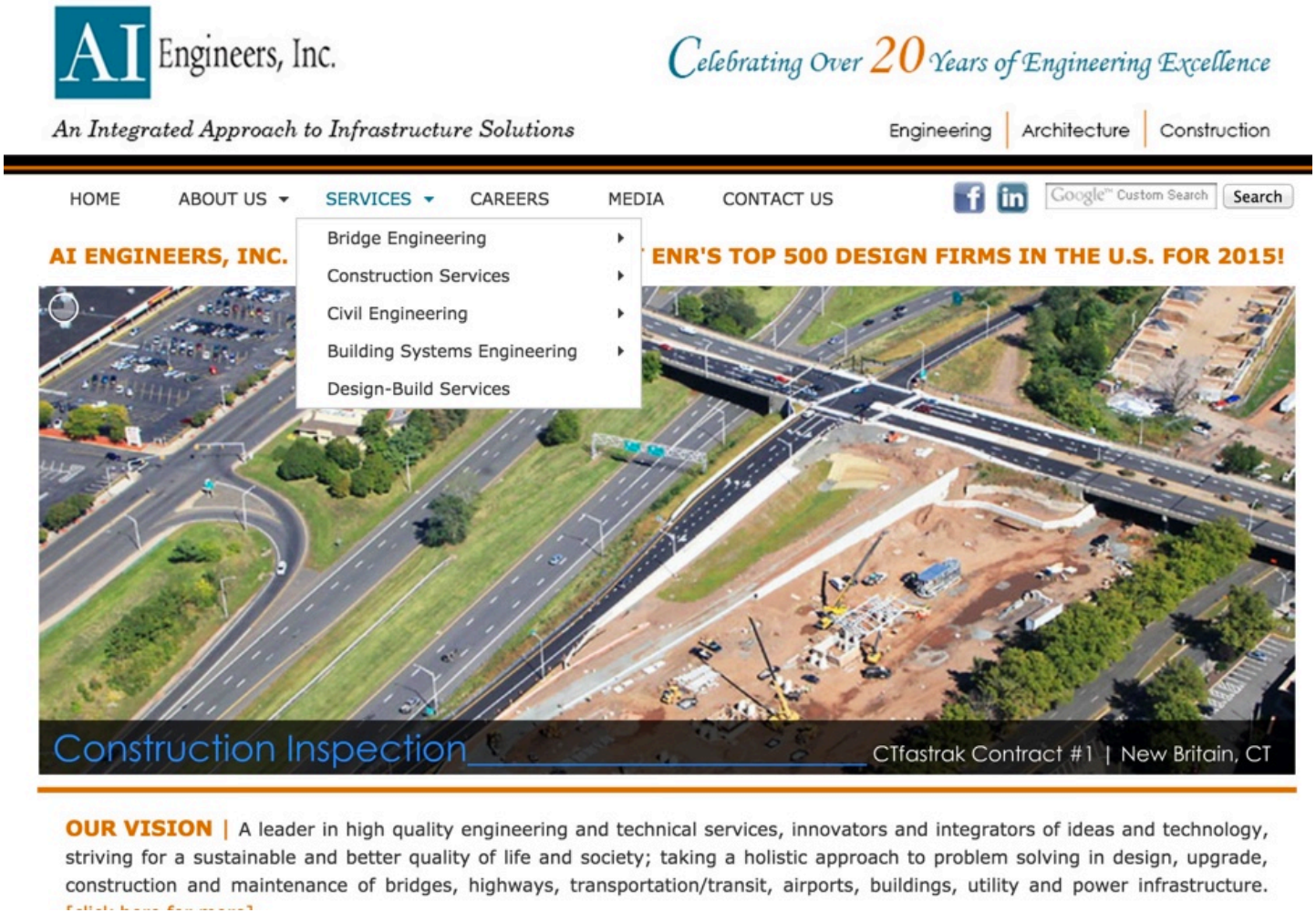
Come prevedere le truffe?

- Esempio: www.google.com/search?q=%22Tai4ted%40outlook.com%22
  - https://domainbigdata.com/outlook.com/mj/Xsk5ny98gV2bvYTGsy-VJw
  - https://www.cutestat.com/email/tai4ted-outlook.com
- Si può lavorare anche a livello di reverse IP o reverse DNS (con registrar piccoli)

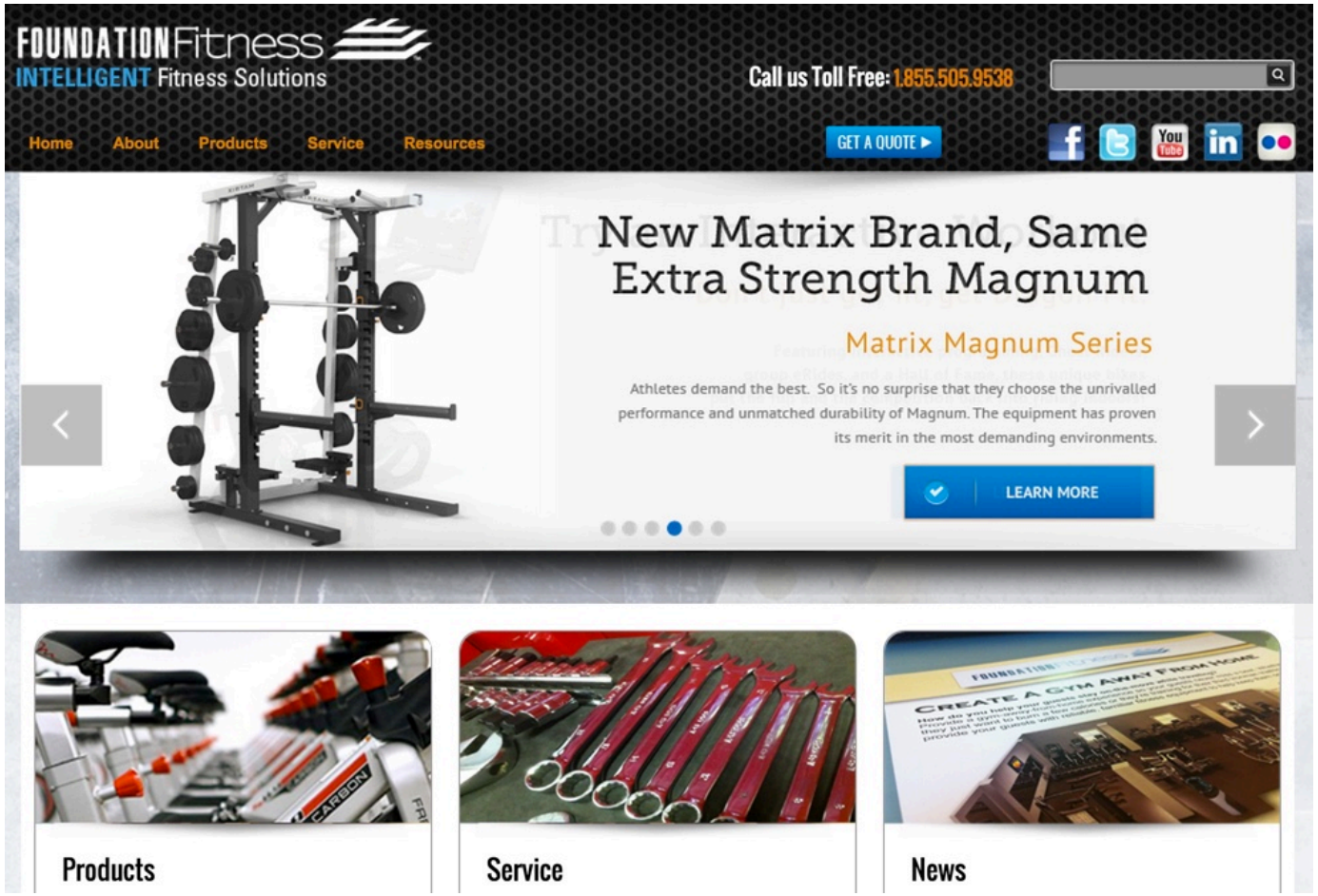
Come prevedere le truffe?



Come prevedere le truffe?



Come prevedere le truffe?



Come capire se siamo attaccati?

- Accessi da IP anomali (last account activity, etc…)
- Verifica presenza Inoltri/forward email (in genere a livello di **postmaster**)
- Verifica domini simili al nostro (Domain Typo Finder)
  - es. dalchecco-it.com, dalchecco.it (”i” maiuscol al posto della “elle”)
- Global Security/Network check
- Tenere presenti che potrebbe essere attaccata la controparte

Domain Typo Finder Results

4 Results

NOTE: Recent changes in registrant data may not be reflected in this view.
Click on the typo to view the most recent Whois record.

Export to CSV and open as a spreadsheet!

Domain	Registrant	Registration Count
Foundationfitness.org	Foundation Fitness	7
Foundationfitness.net	Foundation Fitness, LLC	5
Foundationfitness.com	Foundation Productions LLC	741
Foundatiionfitness.net	VistaPrint Technologies Ltd	482,936

Come proteggersi?

- Regole e filtri antiS[P | C]AM sulla posta elettronica
- Autenticazione a due fattori e pwd robuste
- Antivirus/Antispyware/Firewall/SIEM/UTM
- Brand Protection (Domain Typo Alert)
- Cautela nell'aprire allegati
  - Online File Conversion tools (es. Zamzar) o Word Viewer
- Awareness/Educazione
  - Non fornire le proprie credenziali di posta
  - I file .SCR, PF, ZIP, EXE sono pericolosi
  - Chiedere riscontro di cambi improvvisi di IBAN e richieste che manifestano esigenza di fretta e segretezza
  - Attenzione al mittente delle mail (esclusi utilizzatori di Outlook)

Questiions? 

@forensico

paolo@dalchecco.it

www.dalchecco.it