Google and Facebook Scams: Preventing Employees from Falling for Invoice Fraud with Domain Intelligence Tools

Posted on February 17, 2020

Business email compromise (BEC), also known as CEO fraud, whaling, email account compromise (EAC), or invoice fraud, is a tried-and-tested attack method. Since 2013, BEC scams have been responsible for close to $12 billion in company losses. And this figure continues to rise, as, in 2018 alone, the said scams cost victims $1.3 billion.

In this post, we will look more closely at two cases of invoice fraud that caused Facebook and Google to almost lose a total of $123 million just this year. We will also demonstrate how our Domain Research Suite (DRS) can help companies prevent their employees from falling for such attacks.

Table of Contents

The Attack: Even Tech Giants Can Fall Prey to an Elaborate BEC Scam

Making mistakes is a given; it is part of being human. And while committing an error is not a crime, when it comes to cybersecurity, it could lead to detrimental consequences.

In a corporate environment, one error, when overlooked, can lead to a financial loss of $3.92 million. Worse, human error is responsible for a quarter of the total number of data breaches. And as our featured incident showed, even tech giants like Facebook and Google are not immune to

risks. Earlier this year, Facebook and Google were tricked into paying out $23 million and $100 million respectively to a BEC scammer from Lithuania.

The Attacker

Evaldas Rimasauskas was a Lithuanian citizen who pled guilty on 20 March 2019 to one out of five counts of wire fraud that induced two U.S.-based Internet companies to wire over $100 million to bank accounts he was in charge of. He stands to face a maximum sentence of 30 years in prison.

The Attack Vector

Rimasauskas registered a fake company in Latvia whose name resembled that of a hardware manufacturer in Asia (i.e., Quanta Computer) that Facebook and Google did business with. He then posed as someone from Quanta Computer's accounting department to convince the victims to pay for fake invoices via email.

The Case Facts: Attackers Use Clever Social Engineering Tricks to Defraud Victims

Rimasauskas exerted great effort and spent time crafting his clever social engineering ruse to trick Facebook and Google into handing over vast sums of money. Here is a detailed account of his scam:

- Rimasauskas and his co-conspirators did in-depth reconnaissance to find a company that worked with the tech giants and which they could spoof. Their research pointed to the Taiwan-based hardware manufacturer Quanta Computer, which provides servers for the victims' data centers.

- Armed with this intel, the attacker set up a company in Latvia bearing the same name as that of the hardware manufacturer.

- The cybercriminal then set up an email account on his newly acquired domain to send forged invoices, made-up letters, fraudulent contracts, and even corporate stamps to the victims from 2013 to 2015. This tactic made the fake emails appear to have been sent by Quanta Computer's employees.

- Both Facebook and Google wired payments to the bank accounts owned by Rimasauskas that were indicated in the fake emails. All of the payments he received were subsequently laundered to banks in Cyprus, Latvia, Lithuania, Slovakia, Hong Kong, and Hungary.

- In March 2017, Rimasauskas was arrested by Lithuanian authorities. He was then extradited to the U.S., where he pleaded guilty to committing one out of the five counts of wire fraud he was charged with.

- When Rimasauskas was arrested, Quanta Computer admitted that he indeed impersonated it. Fortunately, the company did not suffer any financial losses.

- Also, in a rare but fortunate turn of events, both Google and Facebook were able to get back the money that they transferred to the scammer's offshore accounts.

While everything turned out in favor of the two tech giants, this case shows that even the most accomplished tech organizations could fall prey to ingenious invoice scams. Not all victims are quite as lucky, however.

What if a swindled company does not have the technical resources or expertise to track down attackers? And even if they manage to do so, what if they do not have the financial capacity to file a legal case? How can they prevent their employees from getting their businesses entangled in invoice fraud?

A Possible Solution: Preventing Invoice Fraud with Domain

Research Suite

BEC scammers succeed because they prey on their targets' inability to tell what is real from what is fake. Cybercriminals bank on the trust that is forged between companies that have ongoing business relationships. In fact, more often than not, email recipients do not scrutinize the addresses of who seem to be trusted contacts.

And so, they end up clicking on links to malicious sites and divulging credentials that the cybercriminals then use to compromise their accounts. Alternatively, they end up sending confidential files to eagerly waiting threat actors. Or, in this case, wiring funds to bank accounts under the cyber attackers' control to pay for goods and services that they did not receive nor even order.

As in most cases of fraud, BEC attacks are addressable. Organizations like Facebook and Google can enhance their existing security solutions and frameworks with Domain Research Suite's many components, as illustrated in the following cases.

Distinguishing between Real and Fake Domains

With WHOIS Search, recipients can check if the domain of the sender's email address matches that of their supplier. Let us say, for instance, that the attacker used the domain quantatvv[.]com in their scam. Note that this was not the domain Rimasauskas used – it was a randomly chosen typo version of quantatw.com for demonstration purposes only.

A WHOIS Search can easily help distinguish between the supplier's real domain (i.e., quantatw.com) and a potentially spoofed one. Take a look at the results for each domain below.

WHOIS record for quantatw.com

Domain age

Created Date: March 27, 1997 05:00:00 UTC

Updated Date: March 29, 2019 02:04:35 UTC

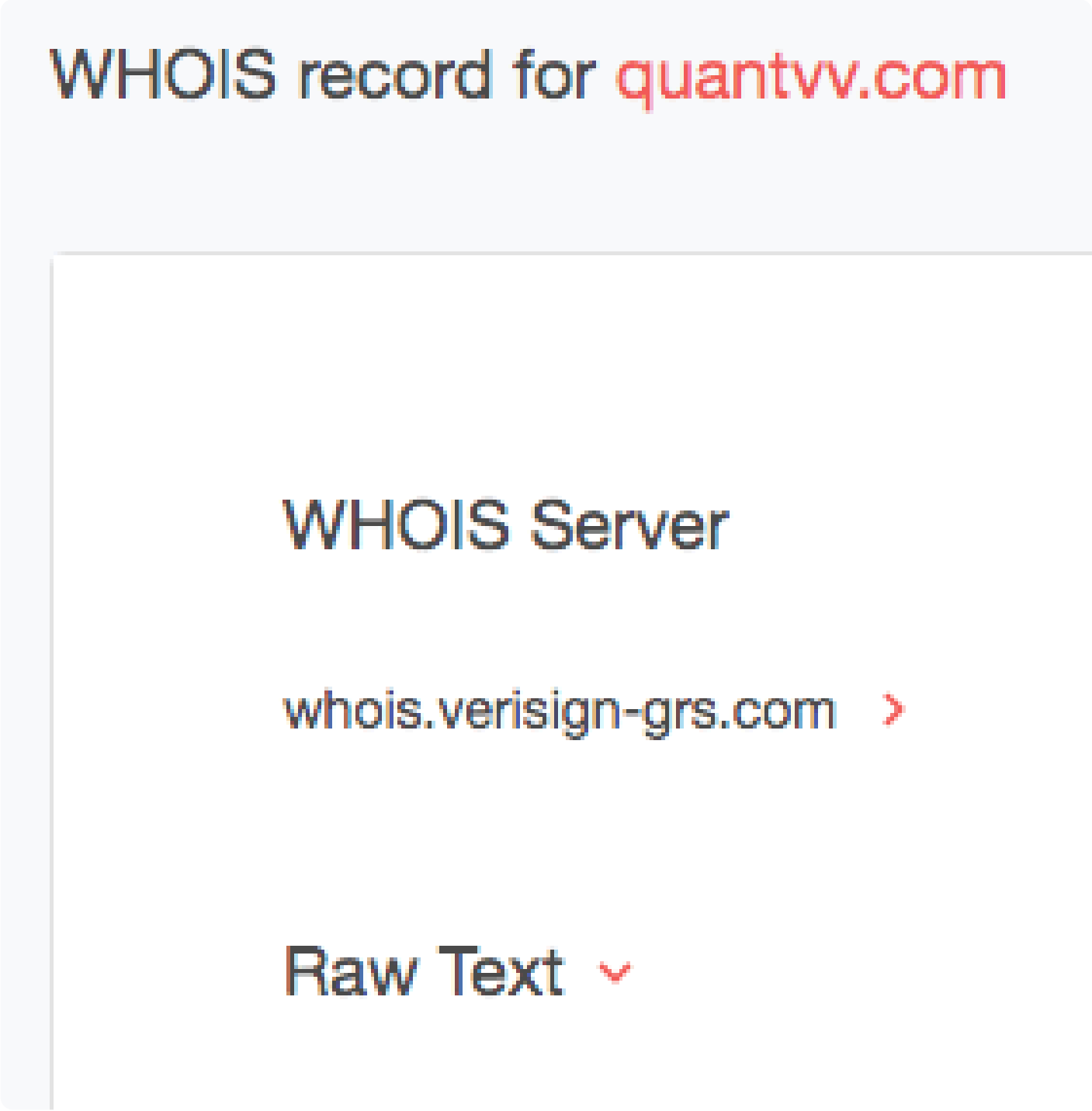
Expires Date: March 28, 2029 04:00:00 UTC

Estimated Domain Age: 8273 day(s)

Registrar Name

Network Solutions, LLC ›

WHOIS Server



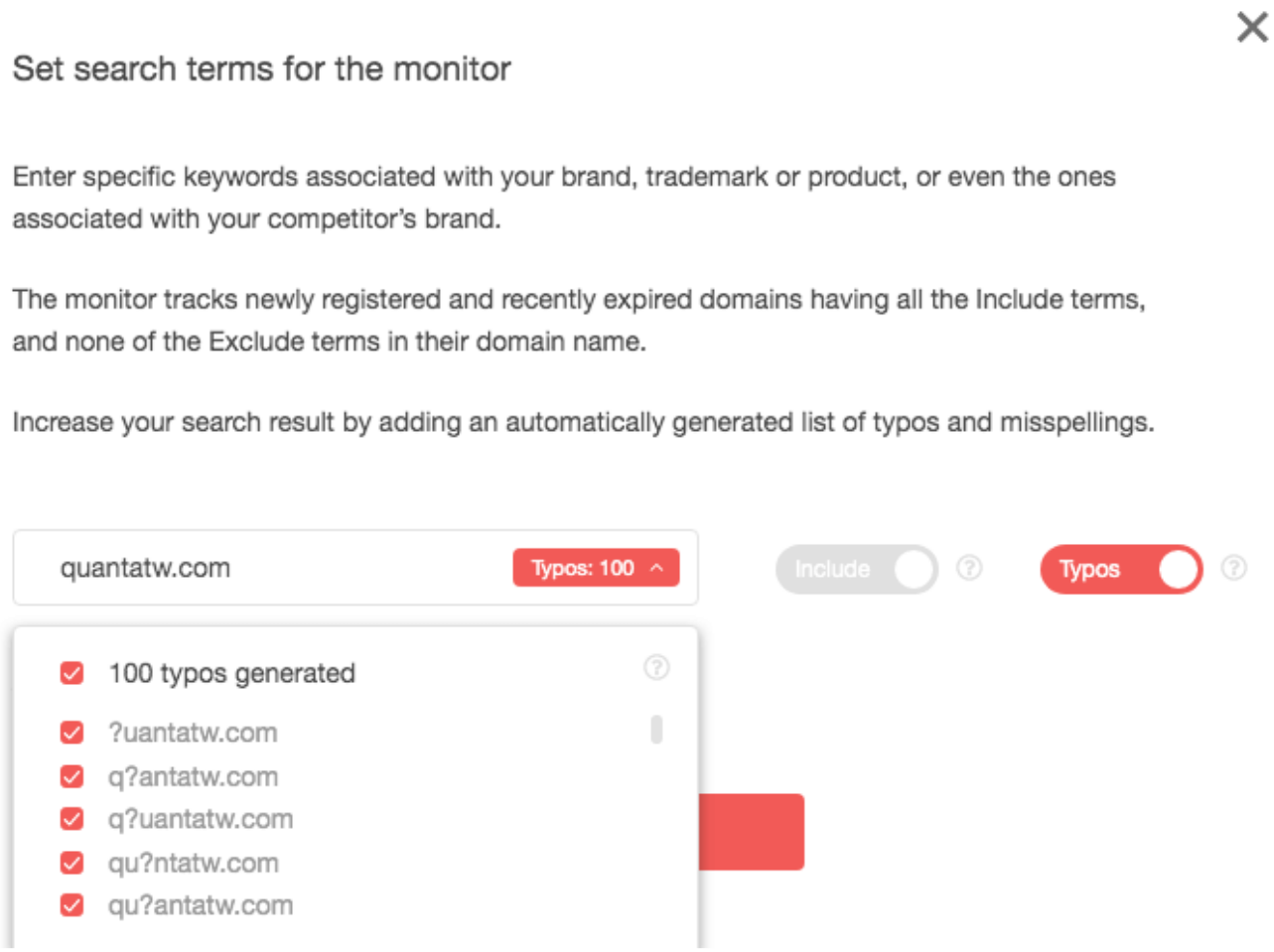
Based on its WHOIS record, quantatvv[.]com is not even registered and thus should not be active. It is dormant but we have seen such domains abused in attacks in the past. Take the case of Spammy Bear

, for instance, where threat actors exploited a weakness in GoDaddy's network to use inactive yet legitimate domains to wreak havoc with sextortion and bomb threats throughout 2018. The Spammy Bear operators hijacked thousands of dormant domains for their spam campaign by registering free GoDaddy accounts and telling its automated Domain Name System (DNS) service to allow them to send emails with those domains from an Internet address under their control.

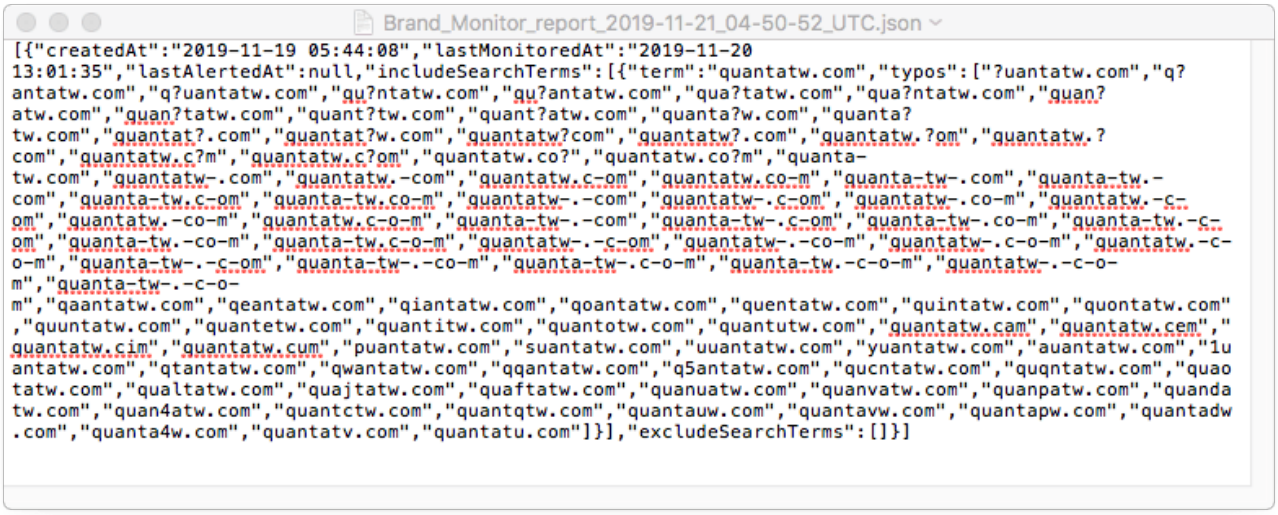
Taking a Proactive Stance to Cybersquatting

Quanta Computer, meanwhile, which unknowingly ended up being abused as part of Rimasauskas's scam, can prevent similar incidents from happening in the future with the help of another Domain Research Suite component, Brand Monitor. This tool allows users to keep track of unscrupulous individuals who may be dragging its name into attacks. Here is a guide to using it:

- Type your domain name in the Advanced input field and click the Add to monitoring button. To track down potential phishing, cybersquatting, and spoofed domains, be sure to turn on the typos feature by toggling the button on. Doing that instantly tells a company like Quanta Computer that at least 100 misspelled variations of its domain name will be included in the tracker.



- While not all of the 100 domains on the list are automatically malicious, it is advisable to monitor them in case they are used in attacks against the company's clients. It takes 24 hours for Brand Monitor to record changes made to any of the domains on the list. After that, you can download the list in the JSON format. Here's the report for quantatw.com:



- Screen the domains to make sure that none of them belongs to you or a legitimate company. If any of them do, take these off the list.

- Now, armed with a list of sites that can be compromised or purchased to cause harm to your clients, you can advise them to potentially block the suspicious domains from accessing their networks or, at the very least, deal with them scrupulously.

- Block these domains from your network as well, in case they are used to swindle your own employees.

Proving You Are Not Part of a Cybersquatting Attack

Now, let us say that one of your clients asks you if you've recently sent an invoice for the purchase of 10 servers. It turns out that you did not. As this sounds suspicious, it would be a good idea to ask the client for the invoice sender's email address so you can investigate the case.

You learned that the questionable email was sent from the domain quantatv[.]com. Note that this domain was randomly picked from the Brand Monitor misspelled domain results for quantatw.com. We are not saying it is malicious. It is just used for demonstration purposes.

Query both domains on WHOIS Search for a comparison. The table below show the details from their WHOIS records:

Detail	quantatw.com (Real Domain)	quantatv.com (Misspelled Domain Variant)
Created date	27 March 1997 05:00 UTC	20 December 2016 14:30 UTC
Updated date	29 March 2019 02:04 UTC	30 November 2018 17:14 UTC
Expires	28 March 2029 04:00 UTC	20 December 2019 14:30 UTC
Estimated domain age	8,272 days	1,063 days
Registrar name	Network Solutions, LLC	eName Technology Co., Ltd.
WHOIS server	whoisnetworksolutions.com	whois.ename.com
Nameservers	DNS6.QUANTATW.COM DNS7.QUANTATW.COM GTMCN.QUANTATW.COM	dns3.dns.com dns4.dns.com
Status	clientTransferProhibited	clientDeleteProhibited clientTransferProhibited
Registrant organization	Perfect Privacy, LLC	
Registrant state/province	Florida	Fujian
Registrant country	UNITED STATES	CHINA

With this information, you can confidently indicate that the email did not come from anyone in your company. Tell the client the differences between your and the questionable domains' records.Also, you may advise that quantatv[.]com, for instance, is newly registered and talk about the dangers that newly registered domains pose. Emphasize the difference in location looking atwhere the domains are hosted as well.

In case the owner of the misspelled domain turns out to be a fraudster, it would be wise to add his name to a tracker in Registrant Monitor, another Domain Research Suite component. Doing so is an excellent way to keep track of identified malicious individuals' activities.

Concluding Thoughts: Lessons Learned from the Facebook and Google Invoice Fraud Case

Organizations, regardless of their size, could become victims of costly invoice fraud. That said, they should invest in educating and training their employees to exercise due diligence before approving financial transactions. Facebook and Google were lucky to have recovered their money from the scammer, but others such as the following are not as fortunate:

- Tecnimont Pvt Ltd: In January 2018, the Indian subsidiary of Tecnimont SpA fell victim to an orchestrated scam coming from an email account that highly resembled the legitimate email address of its CEO. The company transferred a total of $18.6 million to the scammers' account in Hong Kong within a week.

- First Business Bank: The bank was the target of three BEC scam attempts. Had these succeeded, it could have lost close to $200,000.

- Nikkei: The media giant lost $29 million to BEC scammers at the beginning of this month when one of its employees from its U.S. subsidiary was tricked into wiring the funds to a fraudulent account.

These stories make it crucial for organizations to be wary of committing seemingly harmless errors

that could cost their business millions in losses. To avoid suffering the same, they can:

- Educate and train their employees to spot signs of BEC scams. Remind them of the importance of paying attention to even the tiniest details (e.g., misspellings in email addresses and domain names, unlisted account numbers in corporate records, etc.), especially when handling financial transactions or confidential data.

- Add extra layers of authentication and verification measures to their IT infrastructure to reduce the chance of human error. Integrating readily available enterprise-grade APIs into their existing systems and solutions can help spot suspicious entities attempting to defraud them.

- Monitor the integrity of their entire domain infrastructure with tools such as Domain Research Suite. They can use WHOIS Search to quickly identify the owner of a suspicious domain as we showed in this post. The tool can also be employed to reveal differences between the WHOIS records of two or more domains (i.e., the legitimate domain of your supplier and that of the one posing as said supplier). Brand Monitor, meanwhile, can clue them in to potentially malicious domains that may be trying to spoof their companies in phishing, cybersquatting, and other attacks. Registrant Monitor, on the other hand, can be used to keep track of a known threat actor's malicious domain-related activity. And these are just three of the seven tools that companies can use to ensure the integrity of their domain.

- Subject their domain to regular health checks to patch vulnerabilities, secure open ports, keep records up-to-date, and address misconfigurations with the help of solutions like Threat Intelligence Platform.

For more information on how our solutions can help your business avoid financial losses that result from cyberattacks like BEC and other scams, feel free to contact us at support@whoisxmlapi.com.