19 MINUTES

A Minute-by-Minute Account of Collective Defense in Action.

COFENSE.COM

IT WAS A **CUNNINGLY CRAFTED** PHISH.

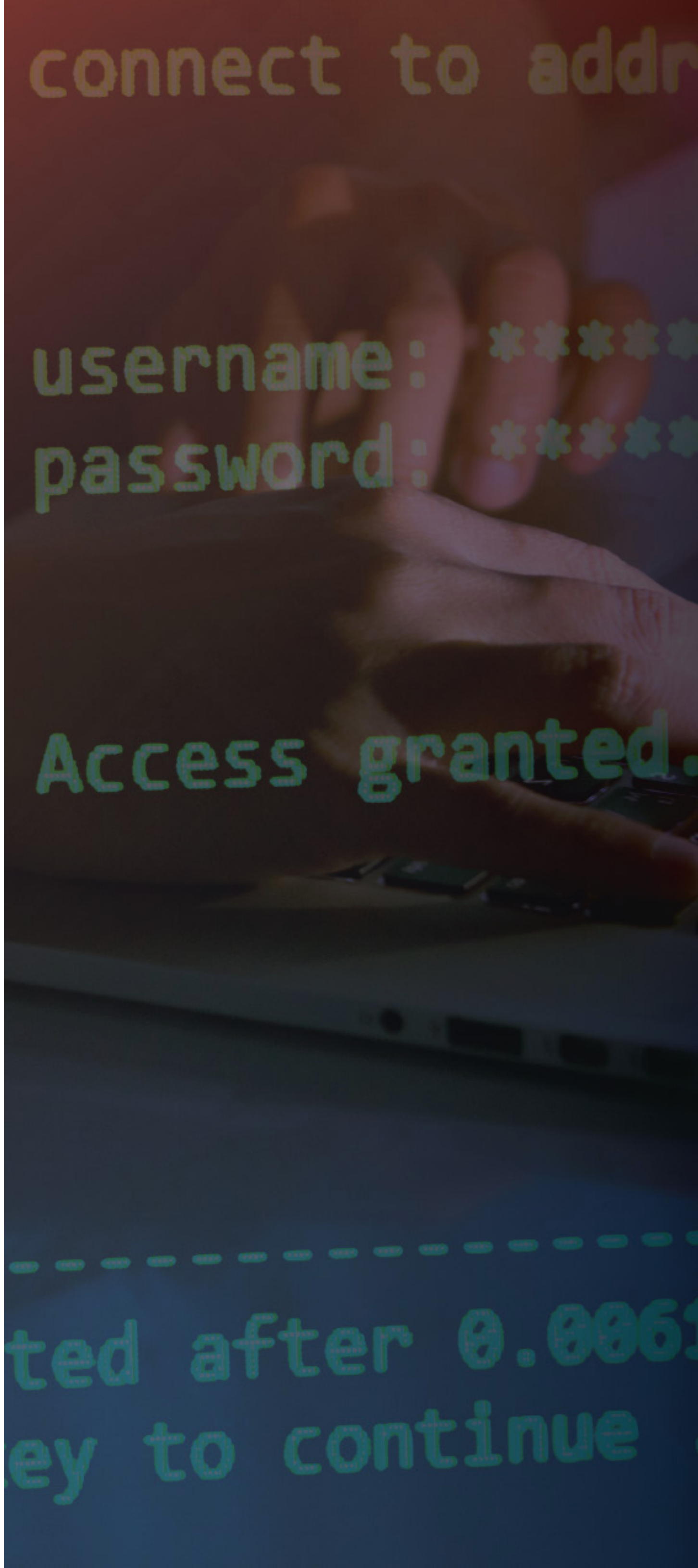
Employees of a healthcare company were going about their day. The usual mundane emails piled up in their inboxes. So when they received a message from their CEO, employees paid attention. It wasn't the typical meeting invite or question from a colleague.

The email asked them to read and agree to a company policy. Simple. Just click on a link, which took them to a login page—from there, they'd enter their credentials and go to the policy page.

But the sender wasn't the CEO. He was a talented fraudster.

The attacker aimed to harvest passwords, gain file system access, and reroute electronic payroll deposits. **And he almost succeeded.**

> *Following is a minute-by-minute description of what happened—how users and security professionals worked together to save the day.*



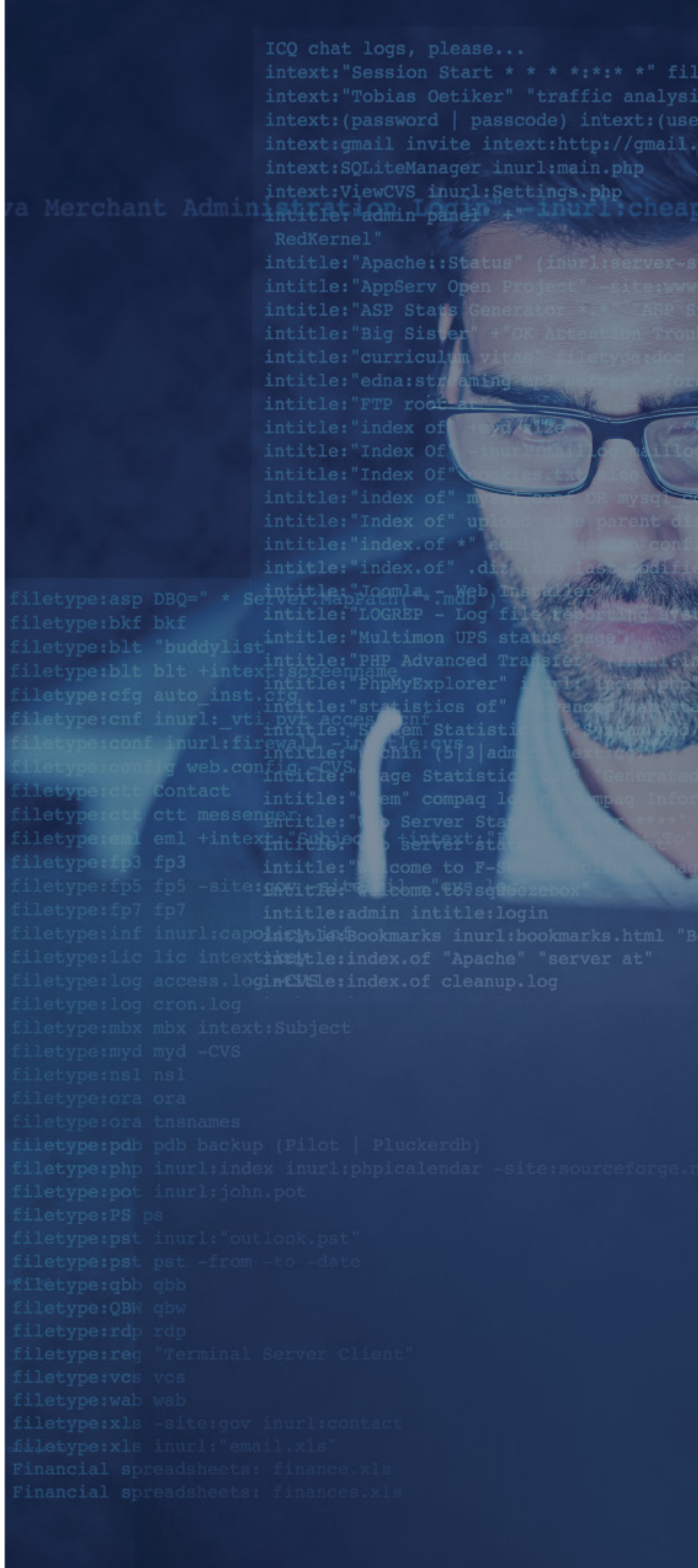
11:48 AM

THE SPEAR PHISHING CAMPAIGN **LAUNCHES.**

The email showed the attacker "had really done his homework," according to the company's Vice President of Information Security. "The email looked and sounded exactly as though our CEO had sent it."

It was a sophisticated twist on business email compromise (BEC), which according to the FBI, defrauds businesses of over $12 billion annually.[1]

Most BEC scams ask their targets to wire funds. In this case, the attacker used credential phishing to reroute electronic transfers himself.



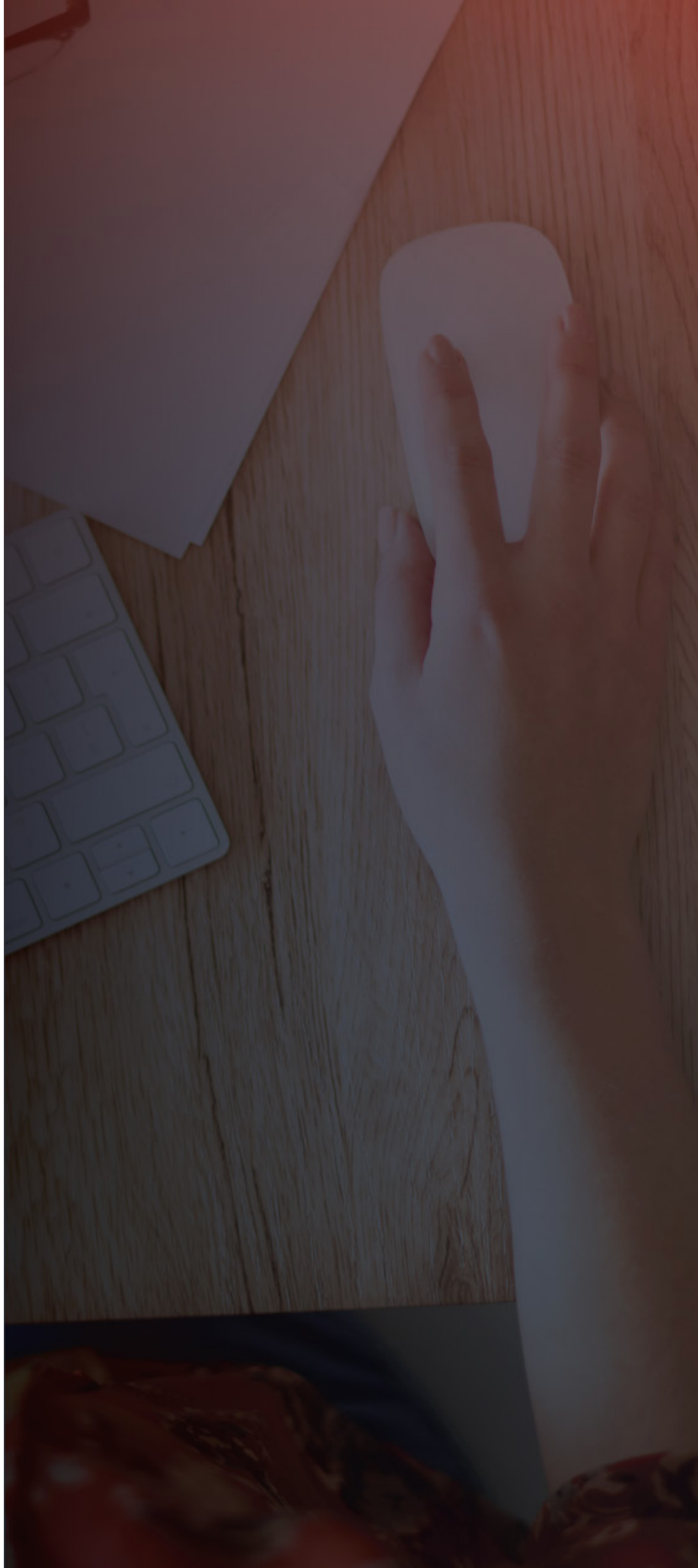
```
ICQ chat logs, please...
intext:"Session Start * * * *:*:* *" fil
intext:"Tobias Oetiker" "traffic analysi
intext:(password | passcode) intext:(use
intext:gmail invite intext:http://gmail.
intext:SQLiteManager inurl:main.php
intext:ViewCVS inurl:Settings.php
a Merchant Administration Login" -inurl:cheap
intitle:"admin panel" +"
 RedKernel"
intitle:"Apache::Status" (inurl:server-s
intitle:"AppServ Open Project" -site:www
intitle:"ASP Stats Generator *.*" "ASP S
intitle:"Big Sister" +"OK Attention Trou
intitle:"curriculum vitae" filetype:doc
intitle:"edna:streaming
intitle:"FTP root at"
intitle:"index of
intitle:"Index Of
intitle:"Index Of"
intitle:"index of"
intitle:"Index of" up
intitle:"index.of *"
intitle:"index.of" .di
intitle:"Joomla - Web Installer"
intitle:"LOGREP - Log file reporting sys
intitle:"Multimon UPS status page"
intitle:"PHP Advanced Transfer"
intitle:"PhpMyExplorer"
intitle:"statistics of"
intitle:"System Statisti
intitle:"urchin (5|3|adm
intitle:"Usage Statistic
intitle:" em" compaq lo
intitle:"Web Server Sta
intitle:" o server sta
intitle:"Welcome to F-S
intitle:"welcome.to.squeezebox"
intitle:admin intitle:login
intitle:Bookmarks inurl:bookmarks.html "B
intitle:index.of "Apache" "server at"
intitle:index.of cleanup.log

filetype:asp DBQ=" * Server.MapPath("*.mdb")
filetype:bkf bkf
filetype:blt "buddylist"
filetype:blt blt +intext:screenname
filetype:cfg auto_inst.cfg
filetype:cnf inurl:_vti_pvt access.cnf
filetype:conf inurl:firewall -intitle:cvs
filetype:config web.config -CVS
filetype:ctt Contact
filetype:ctt ctt messenger
filetype:eml eml +intext:"Subject" +intext:"
filetype:fp3 fp3
filetype:fp5 fp5 -site:gov -site:mil -"cvs lo
filetype:fp7 fp7
filetype:inf inurl:capolicy.inf
filetype:lic lic intext:key
filetype:log access.log -CVS
filetype:log cron.log
filetype:mbx mbx intext:Subject
filetype:myd myd -CVS
filetype:nsl nsl
filetype:ora ora
filetype:ora tnsnames
filetype:pdb pdb backup (Pilot | Pluckerdb)
filetype:php inurl:index inurl:phpicalendar -site:sourceforge.n
filetype:pot inurl:john.pot
filetype:PS ps
filetype:pst inurl:"outlook.pst"
filetype:pst pst -from -to -date
filetype:qbb qbb
filetype:QBW qbw
filetype:rdp rdp
filetype:reg "Terminal Server Client"
filetype:vcs vcs
filetype:wab wab
filetype:xls -site:gov inurl:contact
filetype:xls inurl:"email.xls"
Financial spreadsheets: finance.xls
Financial spreadsheets: finances.xls
```

11:49 AM

EMPLOYEES BEGIN **REPORTING THE EMAIL** AS SUSPICIOUS.

The email was quite convincing. Many employees clicked. Fortunately, enough well-trained users looked at the message carefully. The company uses Cofense PhishMeTM for phishing awareness training. It also equips users with the Cofense ReporterTM plug-in to report suspicious emails with a single click.

One of the simulated phishes the company had used in training spoofed the HR department—like the email the attacker sent, the simulation asked users to click an embedded link to agree to a corporate policy.

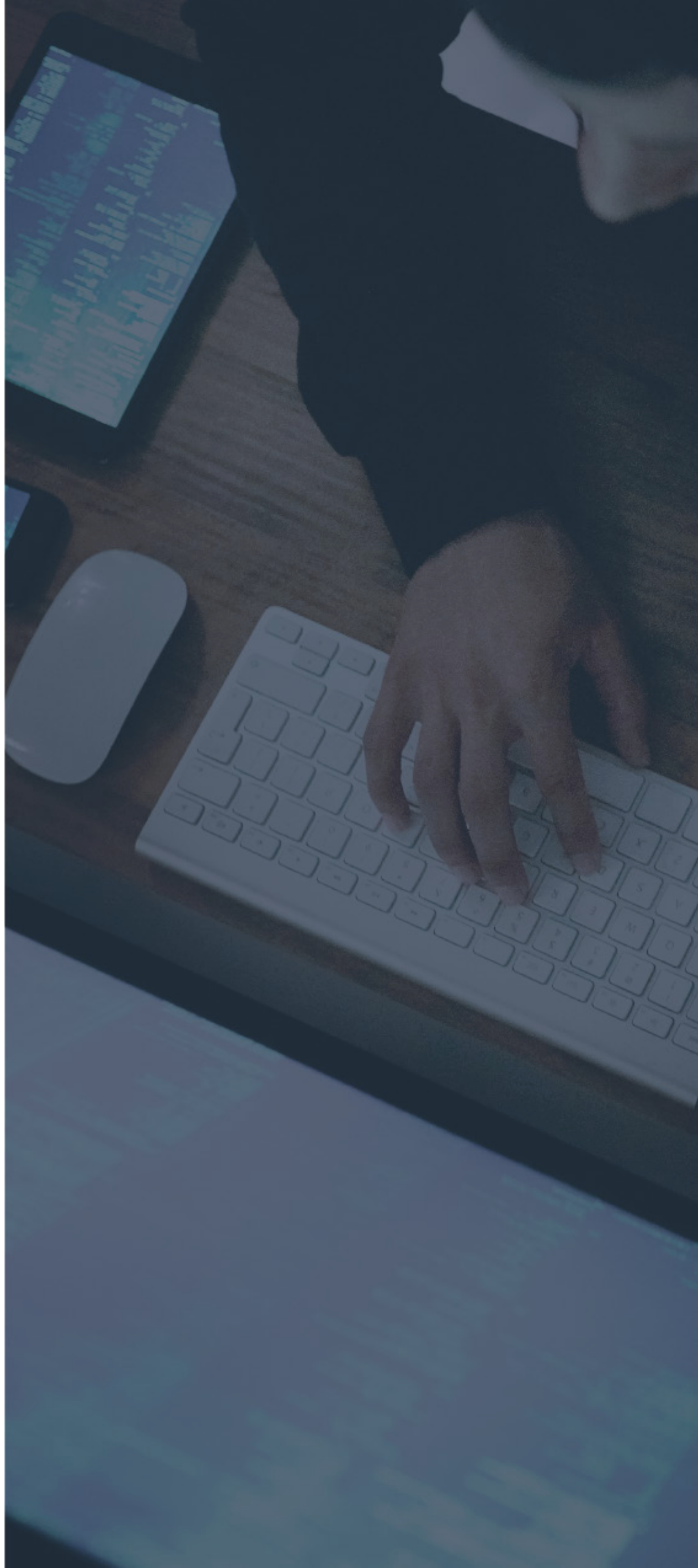


11:49 AM

THE REPORTED EMAILS GO TO **COFENSE TRIAGE** FOR ANALYSIS.

The company relies on Cofense Managed Triage for phishing response. Reported emails first undergo automated analysis. Then human analysts at the Cofense Phishing Defense Center (PDC) investigate further to verify whether an email is malicious.

PDC research shows that crimeware as a percentage of reported emails can range from practically nothing to over 90% monthly. From one month to the next, it's not unusual for a company to see dramatic swings.

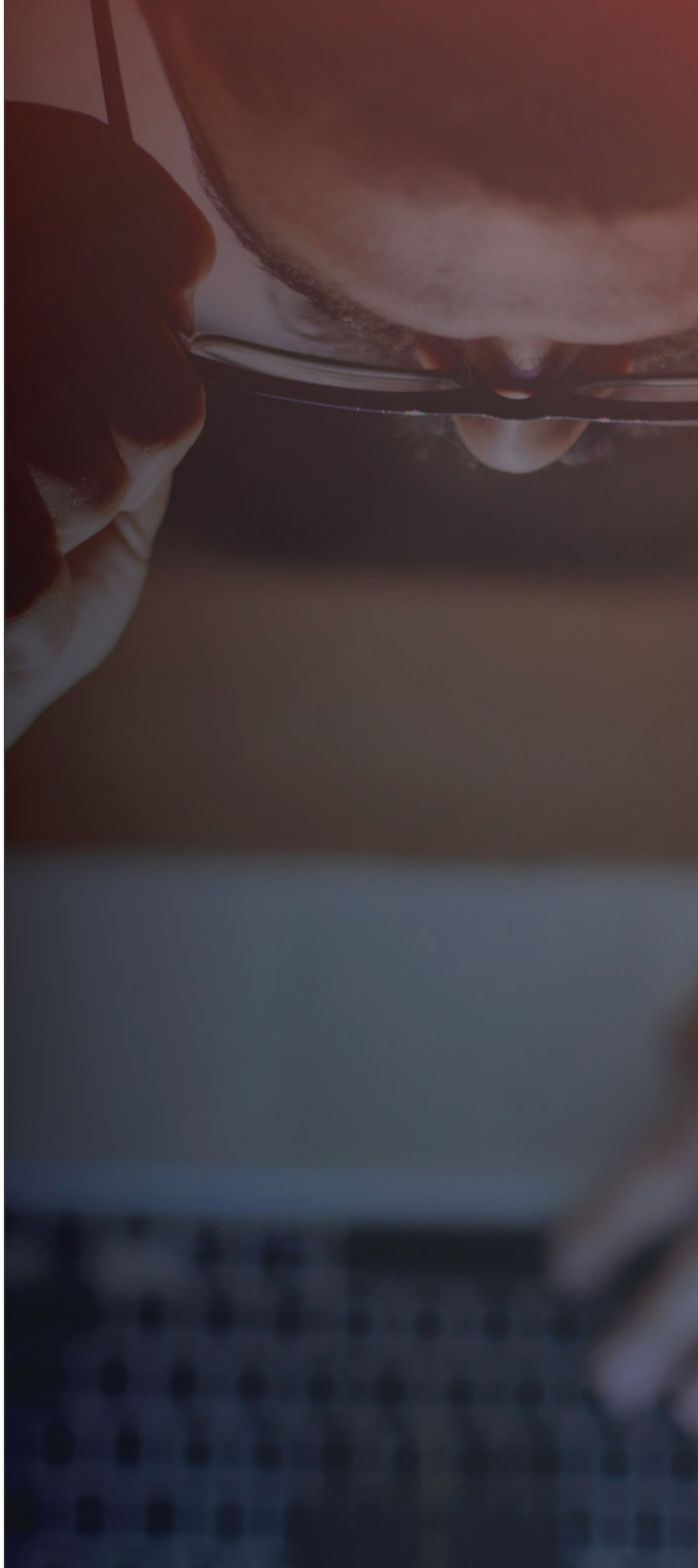


12:00 PM

THE INVESTIGATION **ESCALATES.**

As more users reported the suspicious email and more evidence emerged, the PDC escalated the initial investigation. The threat analyst conferred with his manager on duty.

Cofense Triage groups malicious emails into common clusters. The PDC team then applies human intelligence to confirm a phishing campaign. The approach combines the best of both worlds: Automation greatly accelerates email analysis at scale, while human vetting makes use of insights machines can't deliver.

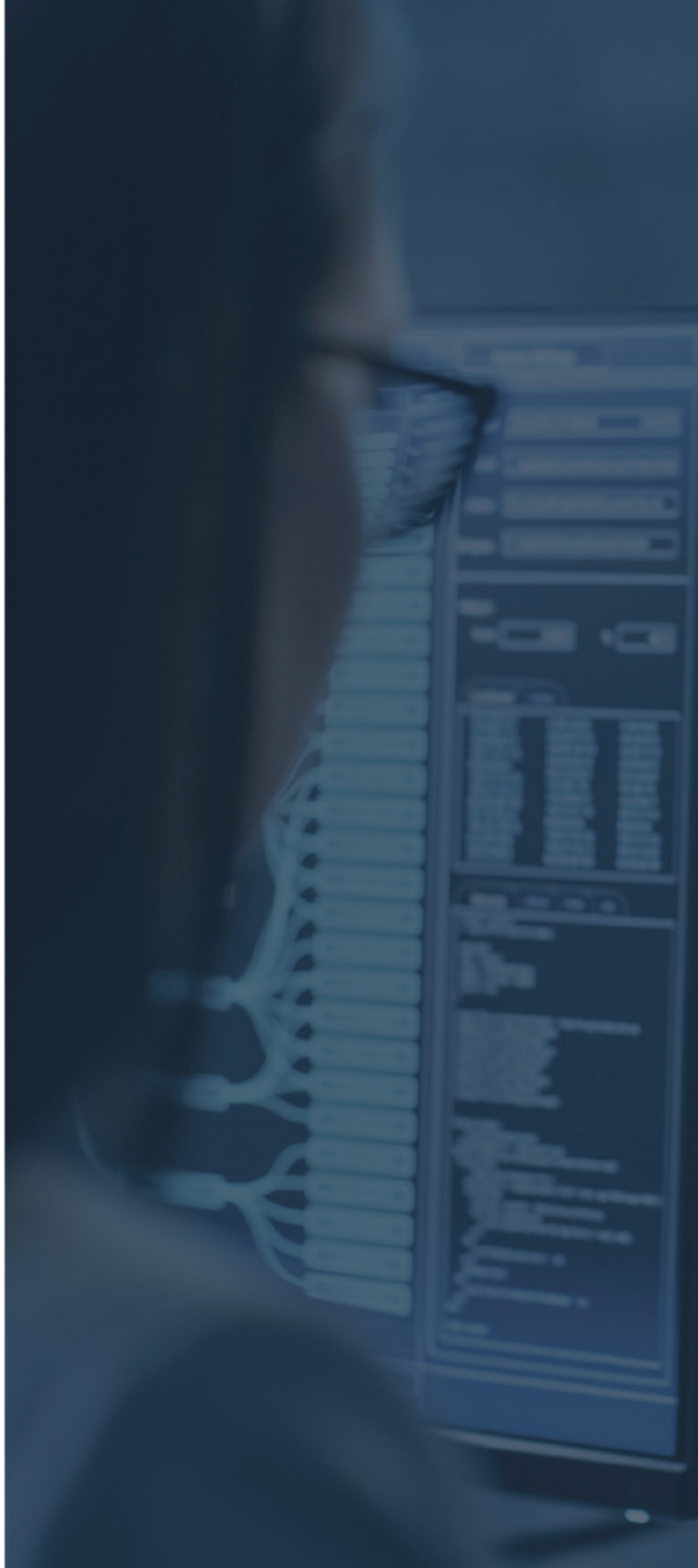


12:07 PM

COFENSE COMPLETES THE INVESTIGATION AND **ALERTS THE COMPANY.**

Upon wrapping up the investigation, the PDC called the company's VP of Information Security. Cofense Triage automation and human expertise enables the company to respond to the threat in real time.

The possibility of a breach is detected in minutes, not months. Not bad, when you consider that IBM Security and the Ponemon Institute report the average business detects a breach in 196 days[2]—and the majority of breaches begin as phishing emails.



12:07 PM

THE HEALTHCARE COMPANY **RESPONDS.**

After consulting with Cofense, the company blocked the phishing site and began to mitigate the attack. Incident responders retracted the bad email from inboxes, monitored behavior from affected Office365 accounts, and disrupted any lateral movement.

“We removed the email quickly,” said the VP of Information Security, “though in the space of a few minutes a lot of people clicked. Once we contained the threat, we started on repair and recovery work, seeing who clicked and mitigating problems linked to their accounts.”

“ALL OF THIS WAS THE RESULT OF A SINGLE WELL-CRAFTED **PHISHING EMAIL.**”

He adds, “If we hadn’t been prepared, the damage would have been worse. We were able to retract the email in under 20 minutes.”

Can your organization stop complex phishing attacks, quickly and efficiently, to protect your bottom line? To learn more about phishing response and Cofense solutions, check out our Incident Response Resource Center.

ABOUT COFENSE

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyberattacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization-wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response and reduce the risk of compromise. Learn more at https://cofense.com

SOURCES

1. Securityweek.com, 2018.
2. Securityintelligence.com, 2018.