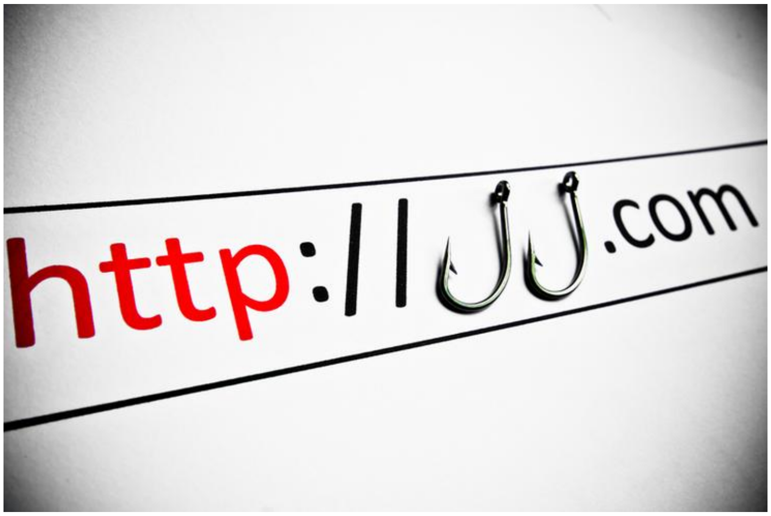
The phishing issue: Michael Connory demonstrates how vulnerable you really are

How Connory easily exposed flaky cyber security controls at a $10 billion financial services organisation

Byron Connolly (CIO)
23 January, 2019 13:20

0

0 Comments



Security In Depth's Michael Connory hacked his first computer, an IBM System/370 mainframe, when he was 12 years old. There were games on the machine that he wanted to play.

These days in his role as an ethical hacker, he could probably set up a social engineering attack on your organisation in a matter of minutes.

Last week, Connory demonstrated to *CIO Australia* how easy it is for someone with his skills to breach your defences using his company's simulated cyber-attack solution, Candiru.

Just prior to Christmas, Connory and his team created and sent out a simple phishing email to convince staff at the local office of a $10 billion financial services company to hand over some of their personal details. His team was

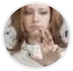
Editor's Recommendations

Does your company need an AI ethics committee?

How CIOs can prepare for a new world of open data

Mind your metaphors: Why CIOs' choice of corporate jargon counts

Why CIO tenures in Australia are getting shorter


Australian companies suck at data analytics

engaged by the organisation to set up the phishing attack and will subsequently be hosting cyber security training for its staff in a few weeks.

The phishing email, titled ‘Thank you for your hard work,’ was sent to 140 staff at the organisation. Upon opening the email, staff were presented with a fake movie voucher offer which when clicked, sent them to a portal where they were asked to provide personal information such as their usernames, passwords and phone numbers.

It was prior to Christmas so some staff were on holiday. Despite this, 41 people clicked the link in the email and provided their details.

“We can see that a lot of the individuals didn’t open the email but some did – the reality is that many people [fall victim],” said Connory. “We can sit on this and then start to utilise Outlook web access or Gmail or whatever it is and then access [personal] emails that way.”

Around three hours into the phishing campaign, a staff member figured out it was SPAM and alerted the rest of the organisation, said Connory.

Connory said his organisation uses two methods during its regular hacking activities. The first is to use a “binding piece of technology” where malicious software is combined with another item such as a picture.

READ MORE
OPINION: Human factor weak link in health data security

The second method, which the organisation prefers, is to send out a keylogger to gain access to a computer.

“An example might be a bank – we don’t want to target its customers, we think that’s dumb and slow, we want to target the bank itself. We want to be indistinguishable – we don’t want to be found. We can have a clean computer and a clean IP address,” Connory said.

Candiru can also monitor when a third party managed service provider or security technology a company is using will pick up an attack. The financial services firm was using Outlook 365 and the Mimecast cloud-based email security software.

Connory said the Mimecast product only picked up 18 per cent of the emails.

READ MORE
Burning down the house: CEO attitudes to cyber security all wrong

“The [financial services company’s] third party managed service provider, they were told about it and didn’t do anything. When they were told about it, they just told people it wasn’t serious and not to worry about it,” he said.

Ice Bucket Challenge co-founder gets his voice back

Tweets by @CIO_Australia

CIO Australia
@CIO_Australia

Judge rejects Yahoo data breach settlement
cio.com.au/article/656852…

Judge rejects Yahoo data breach settlement
A judge has rejected Yahoo's proposed settle…
cio.com.au

Embed View on Twitter

Web Events

How to power your work and unleash enterprise agility

CIO Executive Council WebEvent | Enterprise Agility – Facilitation, Integration and Enablement

CIO Live Webinar - Future of Work: How to meet the demand of digital

Read more

NTT Data Zone

"When we checked the processes, out of those people who clicked on it, only one-third actually followed the process of how to deal with it. So the incident response program for that organisation completely broke down, the reporting of the incident broke down, the managed services and the technology behind it broke down.

"From this particular focus, we were able to identify significant gaps in the organisational structure. Now, this is an organisation that manages more than $10 billion in funds and has more than 50,000 members. And this is one of many."

Cyber education is not good enough

READ MORE
Rise in children's identities being sold on the dark web

Organisations are not doing the best job of rolling out cyber security education programs for their staff, according to Connory.

"The first component is they provide an induction and say, 'don't click on links you don't know, try to identify the link, have a look and see if there's a sense of urgency behind it [the email message].'

"The email that we sent [to staff at the financial services firm] said, 'if you do this by Friday, you get your [movie] vouchers. We even spelt the HR director's name incorrectly. If somebody really wanted to do it [send a phishing email], they wouldn't make those mistakes. We did it on purpose," he said.

Companies teach their staff to look out for suspect emails but they don't necessarily put into practice what they are taught and they often don't do another round of cyber security training for another year or two, Connory said.

"I did a review recently of a company that was breached and is in serious trouble. They had spent hundreds of millions of dollars on new cyber security processes which still failed," he said. "Nobody is communicating and there is no process involved [in managing attacks].

He said that Chinese cyber espionage group APT10 has taken advantage of this lack of communication across organisations. This threat actor targets managed IT service providers to access the IP data of both the MSPs themselves and their customers.

"This is what APT10 did. If I get access to one [company's] Gmail account and create an email address within one account which is seen to be ok, I can then start to translate that across to everybody else. This means you won't get that notification that [it's a potential attack].

"One of the tactics people use is to send a file that the user sees and asks, 'hang on, what's going on here? I haven't received a file, I haven't done anything.' And by you creating a conversation, what's occurring is that the system is learning that this is an ok and trusted communication. And from this

Related Whitepapers

Gaining Visibility into Risk and the ROI of Your Security Program

Fighting Fraud in Financial Services? How Blockchain Can Help

Only Adobe Acrobat

I can send files, I can attach viruses and malicious code into your email because I have access to it and send it internally."

Follow CIO Australia on Twitter and Like us on Facebook… Twitter: @CIO_Australia, Facebook: CIO Australia, or take part in the CIO conversation on LinkedIn: CIO Australia

Follow Byron Connolly on Twitter: @ByronConnolly

Join the CIO Australia group on LinkedIn. The group is open to CIOs, IT Directors, COOs, CTOs and senior IT managers.

Tags hacker phishing email cyber-attack email scam Ethical Hacker white hacker Security in Depth Michael Connory Candiru

More about Australia Facebook IBM Mimecast Twitter

0 Comments

Read next

Aussie IT spend to increase in 2019, despite recession rumours and trade ...

Business execs, academics call for urgent debate on AI ethics

The week in security: GDPR gets real for Google

CSO Online

In pictures: CIO Executive Council Pathways graduation

In pictures: Turning insight into action - and your competitive edge - ...

Swinburne Uni and Capgemini launch blockchain centre

Centre of Excellence will take blockchain-based solutions "from proof of concept to production"

1. Latest credential-stuffing attacks confirm we’re still reusing too many passwords
2. Microsoft rolls out new enterprise compliance and security dashboards for a GDPR world
3. Law enforcement shuts down xDedic marketplace for hacked servers
4. The week in security: GDPR gets real for Google
5. Cisco business routers targeted after patch, at least 9,000 vulnerable

1. SAP restructuring to cost up to US$1b
2. Slack says it has 10 million daily active users
3. TECH(talk): The collaboration software market is on the move
4. Cisco extends ACI to public cloud
5. Chief executive of Victoria’s Cenitex to depart

1. Former DXC vice president joins FTS Group
2. Cloud in focus as SAP prepares for company-wide restructuring
3. Cohda Wireless and Kapsch picked for driverless car pilot
4. EY acquires Plaut IT, deepens SAP expertise
5. DXC buys EG service business in Microsoft Dynamics drive

1. TECH(talk): The collaboration software market is on the move
2. Linux Foundation backs a group to boost edge networking
3. Eclipse releases GlassFish 5.1 for Java EE 8
4. Python code completion gets an assist from machine learning
5. Collaboration software spending to hit US$45b as team chat app demand booms

1. Industry, business leaders call for urgent debate on AI ethics
2. Xero implements machine learning for better customer personalisation
3. 5 lessons from building the KIIS brand
4. Former Ticketek CMO and country chief promoted as ticketing giant restructures
5. 5 values-led advertising campaigns by big brands