EP 8 Cyberwarfare (1/3) : can phishing bring down big fish ?

De : Spintank
A : Orange
Février 2020

– Joe:

Jeanne is a Star Wars fan. Like all lightsaber addicts, she is looking forward to December 2019...the release date for the last episode of her favorite saga. So when she's contacted through Twitter with an offer to watch the long-awaited movie before the premiere... she clicks without a moment's hesitation...

She lands on a site that looks exactly like a streaming platform. Full screen mode, with a player featuring a still from the movie. As soon as the film starts loading, she is prompted to fill in her credit card information.

That's when Jeanne gets suspicious: the url for the site is unusual and how could she possibly access the movie when everyone else is queuing at the cinema? She closes the tab, goes back to her news feed.

Without really realizing it, Jeanne has just been caught in a web of malicious attacks, details of which can be found in a Tech Republic article. Her brief scrape was one of 285,103 attempts to infect users or collect personal data... and again, I'm only talking about attacks linked to the Star Wars saga in 2019.

Hi Chloe!

– Chloe:

Hi Joe.

– Joe:

Welcome to the Memo, the podcast that deciphers digital news for you. Today, we begin a series of three episodes on cyberwar. Cyber-warfare is the kind of hostility that comes without combat, gunshots, or explosions. Conflicts on the web, that often start with small attacks...like the one Jeanne avoided. How does it work? That's what we'll be talking about for our first episode.

– Chloe:

Let's start with this portmanteau word: phishing, as in P.H.I.S.H.I.N.G. It's helpful to understand where it comes from: According to an article in the Journal du Net, it's a mix of the word "fishing," with an F, and "phreaking" with a PH, a term used to describe the practice of hacking phone lines, usually to place free calls. The metaphor speaks for itself... [It is also found in "Hameçonnage", the French translation]

To make a long story short, phishing is a form of identity theft that consists of trying to trick an Internet user into revealing personal data.

This is probably not the first time you've heard about phishing: it's one of the most common kind of cyberattacks... you've probably received strange messages asking you to lend money to a friend, or to click on a link in order to be wired astronomical sums of money...

– Joe:

Right. My spam box is full of emails like this. So how come we are hearing about them now?

– Chloe:

Well, these attacks are evolving! The emails can seem cheesy, but some of these attacks are growing increasingly sophisticated. Take our Star Wars fan: the bait appeared on her Twitter feed, probably via a Star Wars hashtag or some such. She might also have stumbled across it by googling "Star Wars Online"... The method used by these attacks is what Kaspersky's experts call Dark SEO: the ability to optimize the content of certain messages so that they organically appear in news feeds and searches. It works particularly well with trendy topics, like Star Wars, which interests a lot of people...

– Joe:

Do they also use other techniques ?

– Chloe:

Oh yes. In fact, Phishing is among the five things to watch in 2020, according to Centrify CEO Tim Steinkopf. He wrote in Forbes that phishing "will continue to move away from using email as the preferred medium and focus more on text messaging." He also describes how AI could allow hackers to look and sound like a trusted person during a video call. The aim of course being to convince people, like a chief executive, for instance, to deliver key information... The case is extreme, but according to Le Parisien, there had been one case of scam in France where criminals used the silicone mask of a minister to extort funds from public figures...

– Joe:

So forms of phishing are evolving along with technological advances. But Chloe, the one thing all these attacks have in common is their goal: to get the victim to release information...

– Chloe:

… That's right. The first way to do this is to use multiple platforms to reach the maximum number of people, as we just mentioned. But you also have to convince the Internet user to release information. And hackers have become experts in this field. Daniela Oliveira, associate professor at the University of Florida, even explains that "We are all susceptible to phishing because phishing tricks the way our brain makes decisions."

– Joe :

What do you mean?

– Chloe :

The MIT Technology Review identified several examples in an article called "How phishing attacks trick our brains ». For starters, mood plays an important role. People who are feeling happy and not stressed are *less* likely to detect deception. Another lever is authority. Phishers are particularly good at forging messages that use the graphic codes of a trusted institution or

popular site like Amazon. Other messages may manipulate our emotions to get us to suspend our disbelief... Under these conditions, even simple emails can become difficult to detect.

– Joe :

And...so it works ?

– Marine :

Increasingly well. A ZDNet article on corporate phishing reports on an experiment conducted by the security consulting firm Coalfire. They sent phishing emails to 525 companies. And they collected information on nearly three quarters of them... How come? 20% of employees had fallen into the trap and willingly shared their access and internal passcodes…[[The year before that, only 10% of them had trusted the emails.]] So you can see what makes phishing so effective: all it takes is one deceived employee to access information that can unlock access to a much larger system.

– Joe:

But then how do we deal with it?

– Chloe:

To begin with, it is essential to stay informed about such practices and the forms they can take. According to Daniela Oliveira, 45% of Internet users do not know what phishing is...

A number of actions have been put in place to contain phishing. Orange launched a fake campaign last summer offering unlimited 6G. You had to click on a link... which then redirected you to a page that raised awareness about phishing and scams. As another example, Google launched a very educational quiz to test one’s ability to detect scams. The link is in the description if you want to test your knowledge: I can tell you, it’s not easy...

– Joe :

Yes, when I took the test, I fell for what could have been a scam at least twice…

– Marine :

I mean... Even Amazon’s CEO can be framed! We recently heard about Jeff Bezos' phone being hacked by Saudi Arabia. The case was a sophisticated form of phishing: A Wired article this January revealed that the source of the hack came from two messages sent back in November 2018 by Mohammed bin Salman, the Crown Prince and Deputy Prime Minister of Saudi Arabia. One contained a video and the other a photo of a woman who looked like Lauren Sanchez with whom Bezos had a secret relationship. Both files contained malware that infected the device.

– Joe:

[[Is that really the same thing?]]

– Chloe:

No, what’s different here is that the attack was highly personalized. Bezos knew Mohammed bin Salman, had even given him his number in person a few months before. But the idea is the same: you use your victim's trust to extort information or exploit a loophole...

– Joe:

That’s what people are calling Spearphishing…

– Chloe:

Yes: while phishing is like casting a net out into the world-wide web, spearfishing is a much more precise form of attack. It’s a similar method, but you add social engineering into the equation.

Who emails you regularly? Who is your boss? Your accountant... The more information I get about you (through other phishing campaigns for instance) the more I’ll be able to design THE perfect message that will make you yield confidential information.

– Joe:

That’s a particularly efficient strategy when it comes to cyber espionage.

– Chloe:

Exactly. One case I read about in a ZDNet article from January 30 is particularly telling. Just as the diplomatic escalation was reaching new heights after a U.S. drone killed Qassem Soleimani, a powerful Iranian general, U.S. federal officials began receiving emails mimicking questionnaires from Westat, an organization that has worked with more than 80 federal agencies for at least 16 years. Behind these emails were two cyber-espionage groups linked to Iran...attached to the emails were Excel sheets with two malwares: One designed to break into computer systems, the other to steal passwords.

– Joe:

And to find out what happens once your password is released, you’ll have to wait for the next episode of our cyberwarfare series... Thank you very much Chloe and thank you for listening to us. You’ll find no nasty surprises in the description below, only bona fide links to the articles we quoted. See you soon for the upcoming issue of the Memo.

Sources :

Phishers prey on fans of 'Star Wars: The Rise of Skywalker' film (Tech republic)

Phishing : définition, traduction (Journal du net)

Six Cybersecurity Predictions For 2020 (Forbes)

L’audacieuse arnaque au «faux Jean-Yves Le Drian» arrive devant la justice (Le Parisien)

How phishing attacks trick our brains (MIT Technology Review)

Les courriels de phishing en entreprise ça marche encore, voici pourquoi (ZDNet)

Phishing Quiz (Google)

Everything We Know About the Jeff Bezos Phone Hack (Wired)

Iranian hackers target US government workers in new campaign (ZDNet)

De la 6G illimitée pendant 100 ans ? La fausse pub d’Orange pour alerter contre le phishing (Le Parisien)