CYBERCONTAINMENT 3 -CORONHACKING : PROFITING FROM DEATH-

Arch0nte

04/2020

Technical Explanations

If you already know what is phishing, what is a ransomware and how to protect you from it, you can skip this part!

Else, welcome to the technical explanation section, where I explain the technical jargon commonly used in the media ☺

First of all, what is a ransomware? A ransomware is a software that a hacker makes you download and that encrypts your computer, phone or pretty much any device, rendering it inoperable. After your device has been encrypted, it is almost impossible to unlock it without the proper password. The hacker will then sell you this password for a large amount of money in cryptocurrency (or just take your money and never give you the password).

How can hackers infect my computer with a ransomware? Well, there are a lot of different ways but the entry point, which is the first contaminated device in a network, is usually reached by using phishing techniques.

Figure 1: Artist rendering of a hacker phishing

Fishing? No, phishing: Phishing is the act of baiting someone online into doing an action which will compromise their device, for instance, clicking on a link or opening an attachment in a mail. To achieve that goal, the hacker could either try to pass themselves as representatives from your bank, phone company, the government, a colleague, … Anything to make you open that attachment, or click on that link. Here is a very quick example : If I tell you to click on this link to find the BBC's website : https://bbc.com you'll be going elsewhere ! (it is actually a nice tutorial on how to avoid getting scammed by phishing emails [1])

DoS, and nothing to do with the state department: A Denial of Service attack is an attack in which the hacker wants to render an online service, website, or server unusable by over spamming it with requests. A very quick solution is just to limit the number of connections authorized from one origin! But hackers found a way around years ago, the DDoS or Distributed Denial of Service. This means that they'll use hundreds of thousands of previously infected computers (called a botnet) to spam the service they want to down. This new form renders the previous protection useless.

Now that you know the vocabulary, let's get into the heart of the topic!

What happened?

Ok so unless you're living in a hut in the middle of the Amazonian forest, you should have noticed the global pandemic forcing about 1 billion people into confinement and which has killed about 130k persons worldwide as I'm writing these lines. Because of this, companies, governments and people are now spending more and more time online, which makes them more and more susceptible to attacks ang guess what ? There has been a sharp increase in the online illegal activities [2].

These attacks are not only targeting companies but also hospitals [3], governmental agencies [4][5] and even the WHO [6]. Which would be a complete and utter d*** move at any time but in the heart of the pandemic? That's like trying to rob the fireman carrying you out of a burning house. Some hacker groups have publicly expressed that they won't attack in any fashion anyone working in the field of healthcare but other, both for money or paid by states [7] (Fancy Bear is infamous for being suspected of being an outlet of the Russian foreign military intelligence, the GRU) are profiteering of the opportunity that more internet traffic, a huge sense of urgency and a global crisis have created.

Some of these attacks were "just" DDOS attacks ([5]) but most were much more elaborate, often using phishing to gain a foothold inside an organization's network and then using it as a gateway to infect more devices, often with the ultimate goal of locking down the entire business activity with a ransomware [8].

So, to sum up: both money hungry criminals and state-paid actors have targeted healthcare companies, hospitals and international organizations. And that, as you can imagine, severely disrupted their ability to heal and organize the crisis. Because there is such a need for urgent help, hackers hoped that it would force companies, especially hospitals, to pay the ransom because they need their IT infrastructure to save lives.

How to protect yourself?

So, here are 3 tips to be safe when using the internet:

1 – Constant vigilance

Figure 2: Alastor Moody reminding everyone that "constant vigilance" is the only way to be safe in the grim world of ~~magic~~ internet

Whether you're a company, an international organization or simply someone who uses the internet, you **always** need to be weary. People **will** try to scam you. Companies **will** try to harness your private data. And then get robbed of this data by hackers [9]. So be very mindful of where you click, and who you talk to. **Don't save** your passwords in your browser, don't use obvious passwords, build your own complex passwords and most importantly **never** give anyone your password over the internet. Even if your interlocutor is someone you trust with that information, you take the risk of either of your devices being compromised and losing that password. Always logout of a service when you stop using it (or people could steal your session without ever needing your password). If you want more details on how to be as weary as possible, I highly recommend this: [1]

2 – Use the right tools

This one is mostly for people not used to the cybersecurity world. There are hundreds of anti-virus software of varying quality. Never trust the ones installed by default on your Windows (Windows live defender, McAfee, …) and try to use of the top ones on the market that give overall protection and not just viruses. I'd recommend Kaspersky or Bitdefender, whose free versions are

still great! Mobiles and tablets also need protection but I'm much less experienced in that field so I'll let you figure that part out ^^

3 – Backups, Backups, Backups

This one, is for everyone (even the ones who already know about it, because NO ONE does it often enough). Backup your essential data, photos, videos and documents on an offline Hard-drive not connected to anything while not doing a backup. That way if anything happens to your computer (malicious or not), you still have all of your vital information.

This might sound like paranoia but trust me, shit happens ! And the reality of trying to salvage what you can from a disaster-struck disk while knowing that it contains critical work documents worth hundreds of thousands of dollars or even just photos of cherished moments that could be lost forever if you make a single mistake **is not worth** the laziness of not doing backups.

So, do backups, both your heart and the IT guy who'll work on your PC will thank you ^^.

Conclusion

First of all, thanks everyone for reading these blogs ☺. If I made even just one of you think about the way you use the web and beware of its dangers, I'd consider this a victory ^^

Then, if you have any returns or questions, feel free to email me at archonte@hackademint.org or to @me on Discord (you can find me via the HackademINT server (https://discord.gg/skTeWVg)-- Archonte#4358).

Finally, I hope everyone's feeling alright despite the disease and the confinement! If not and you wanna chat a little bit, hit me up on Discord !

Bibliography

[1] : https://www.wired.com/2017/03/phishing-scams-fool-even-tech-nerds-heres-avoid/

[2] : https://www.cnet.com/news/as-coronavirus-crisis-worsens-hacking-is-increasing-security-experts-say/

[3] : https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing

[4] : https://www.motherjones.com/politics/2020/03/illinois-ransomware-coronavirus/

[5] : https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

[6] : https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

[7] : https://www.wired.com/story/coronavirus-phishing-ad-fraud-clearview-security-news/

[8] : https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-003/

[9] : https://en.wikipedia.org/wiki/Yahoo!_data_breaches

Images

Figure 1 : https://www.nps.gov/articles/fly-fishing.htm

Figure 2 : https://twitter.com/wizardingworld/status/1197560307788533760/photo/1

Figure 3 : An Easter Egg