Austin Cupp

CS 462

11/16/2022

During the time between late November and early December in 2020, a large scale cyberattack occurred against the technology and home appliance organization named Whirlpool Corporation. Whirlpool Corporation is one of the largest home and business technology and application makers across the entire world, with appliances under its name and other names such as KitchenAid, Consul, Hotpoint, Indesit, Maytag, Brastemp, and Bauknecht. Subsidiary brands on the Whirlpool Corporation website includes Diqua, Affresh, Acros, and Yummly brands. Whirlpool has about 77,000 employees overall at 59 manufacturing & technology research centers across the world, and Whirlpool Corporation generated about 20 billion dollars in revenue for 2019.

So, who attacked the Whirlpool Corporation? The answer to that question would be Nefilim. Nefilim is a ransomware operator/gang that tends to target multibillion dollar organizations using “double-extortion" tactics in order to ensure payment from victim organizations, meaning that they first exfiltrate the data onto their own servers, then they threaten to post the information publicly, either for payment from the victim organizations, or in order to embarrass or damage the company’s reputation. In in our case, the Whirlpool Corporation suffered a ransomware attack and was a victim of the double-extortion tactics.

Ransomware is a type of malware that is created in order to permanently encrypt or “lock” the systems compromised by the cyberattacker or can be used to threaten to publish the victim's compromised confidential data. The Nefilim ransomware gang is known for going after organizations, such as Whirlpool, that use poorly secured and unpatched Citrix remote-access technology and components, which eventually reared its head as being a major vulnerability. This allowed them to then steal the data, unleash crypto-locking malware, and then use the threat of the exfiltrated data being posted to the public to try and force the affected organization, again in our case the Whirlpool Corporation, to send a payment. Once the ransomware gains access to the vulnerable machine, whether it happens through a software vulnerability, stolen access credentials meant for authorized users, or phishing emails or messages, the files and drives within the machine will be encrypted and can only be recovered with a decryption key. The decryption key is what the cyberattacker will offer to the victim in exchange for a payment.

When the Nefilim ransomware gang was able to gain access to Whirlpool Corporations’ devices, they first stole data from them, and then encrypted the devices, in turn denying Whirlpool access to the compromised devices, and then published the confidential information onto their website. What Nefilim did regarding the attack on Whirlpool Corporation, was that they gained access to Whirlpool Corporate’s information involving the corporation itself. Nefilim then committed data exfiltration, which is when malware, in this case ransomware, carries out an unauthorized data transfer from a computer. Netfilim overall was able to steal two main files from Whirlpool Corporation. The first file contained a list of what other compromised files and folders Nefilim had gained access to, while the second file was a 7zip archive file packed with sensitive Whirlpool Corporation personnel data including medical information

requests, background checks and details of employee benefits. Nefilim then posted the files to their website, with the first one being titled as, “Whirlpool_filelist.txt”, however this file was damaged and could not be opened. The second file was titled, “leak_part1.7z”, and this file was the file that contained the confidential information. Nefilim also was able to infiltrate Whirlpool Corporations network a second time, however they did not cause any damage. They did, however, leave a ransom note on the affected systems, and claimed they were in possession of gigabytes of additional data that Whirlpool Corporation would deem as valuable or sensitive.

Not too long after the cyberattack became public, Whirlpool Corporation released a statement, beginning with, "We live in a time when Illegal cybercrimes are all too prevalent across every industry. Data privacy is a top priority at Whirlpool Corporation, and we invest in the technology and processes to help protect our people, our data and our operations." "Last month Whirlpool Corporation discovered ransomware in our environment. The malware was detected and contained quickly. We are unaware of any consumer information that was exposed. There is no operational impact at this time". Afterward, it was indeed deemed true that no consumers had their information compromised, and within a few days after releasing the statement, Whirlpool Corporations’ systems were fully restored and functioning as normal. On December 26th, 2020, Nefilim posted a statement on their website, explaining their reasoning for targeting Whirlpool Corporations, saying that "this leak comes after long negotiations and unwillingness of executives of Whirlpool Corporation to uphold the interests of their stakeholders. Whirlpools cybersecurity is very fragile, which allowed us to breach their network for the second time after they stopped the negotiations”.

This is an important topic today due to the fact that Whirlpool Corporation still remains as one of the largest home and business technology and application makers across the entire world and in turn their products are in many homes and businesses across the world. Also, the Nefilim ransomware gang not only targeted Whirlpool Corporation, but also targeted the Italian eyewear and eyecare giant Luxottica (which owns the Oakley and Ray-Ban brands), the mobile network operator Orange, The SPIE Group, the German service provider Dussman Group, and the Toll Group. Furthermore, ransomware continues to be a major form of malicious software today, and so far just in 2022, there has been over 236 million ransomware attacks across the globe. Ransomware is aimed to attack both individual people as well as organizations and businesses, and it is important that individuals, organizations, and businesses remain vigilant to avoid ransomware attacks. Individuals can avoid them by not clicking on suspicious links or links marked as unsafe, keeping all relative software up to date, avoiding giving out personal information, avoiding the use of unknown USB flash drives, by not using unknown download sources and by not opening emails that appear to be suspicious. Businesses and organizations can avoid the attacks by continuing to have cybersecurity as a main priority or making it a priority if they have not done so. Businesses and organization should perform complete cybersecurity audits often in order to look for vulnerabilities such as buggy software, out of date software or non-recently updated software and insecure network practices such as easy to guess passwords or methods of authentication that are easy to bypass. Also, hiring a specialized team to do an independent evaluation of the cybersecurity is a good practice. This would allow organizations to make the necessary investments to update, upgrade, or install software to better secure their infrastructure and network model. Additionally, businesses and organizations should install network monitoring capabilities and alerts which would allow them to detect any unwanted intrusions by cyberattackers.

Sources:

Osborne, C. (2021, June 8). *A deep dive into Nefilim, a ransomware group with an eye for $1bn+ revenue companies*. ZDNET. Retrieved November 18, 2022, from https://www.zdnet.com/article/a-deep-dive-into-nefilim-a-double-extortion-ransomware-group/

Abrams, L. (2020, December 28). *Home appliance giant whirlpool hit in Nefilim Ransomware attack*. BleepingComputer. Retrieved November 15, 2022, from https://www.bleepingcomputer.com/news/security/home-appliance-giant-whirlpool-hit-in-nefilim-ransomware-attack/

Mathews, L. (2020, December 28). *International appliance giant whirlpool has been hit by Ransomware*. Forbes. Retrieved November 18, 2022, from https://www.forbes.com/sites/leemathews/2021/12/28/international-appliance-giant-whirlpool-has-been-hit-by-ransomware/?sh=1f845eb54d6e

Roberts, D. M. (2021, January 21). *Whirlpool's nephilim ransomware attack*. IDStrong. Retrieved November 20, 2022, from https://www.idstrong.com/sentinel/whirlpool-victim-of-nefilim-ransomware-attack/

Number of ransomware attacks per year 2022. Statista. (2022, August 3). Retrieved November 21, 2022, from https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/#:~:text=During%20the%20first%20half%20of,million%20cases%20to%20133%20million.

AO Kaspersky Lab. (2022, February 17). *Ransomware protection: How to keep your data safe in 2022*. usa.kaspersky.com. Retrieved November 21, 2022, from https://usa.kaspersky.com/resource-center/threats/how-to-prevent-ransomware