Covid-19 and Cyber Attacks

Jarratt Davis

Kevin Luse

Justin Prosser

Devlin Williams

**Introduction**

It is easy to see that 2020 has started off differently than any year in recent memory with the COVID-19 virus changing how the world operates day-to-day. In order to prevent spread, many states like Virginia have created “Stay at Home” orders to help the healthcare system in managing COVID-19 but this policy is also in other countries, not just the United States. This has compelled many employers to either enforce or allow their businesses to operate in a modified manner. Businesses are either running with limited employees in the place of operation or allowing them to work from home using company-issued devices or personal devices with connection tools like VPN, a tool used to help establish a secure connection (Hoffman, 2019). Davis warns of VPN updaters being manipulated by threat actors in order to insert malware (2020). Cimpanu warns of Kapersky’s findings on the increase in Remote Desktop Protocol, or RDP, exploitations that cybercriminals are using. RDP is another potential tool that people are using to work remotely (2020). However, as more people are working remotely online, it is creating more opportunities for threat actors.

Government bodies and healthcare systems are working to create solutions to the problems the virus has caused. They have pushed out information in order to help the public but this has also created an attack vector for malicious actors. By either attaching malicious links or malware to emails designed to look like those sent out by the legitimate bodies, threat actors are looking for ways to compromise target computers or take information (Symanovich). Government programs such as the Small Business Administration, the department tasked with handling the COVID-19 loans for small businesses, have also been targeted due to the high number of applicants for the federal loans (Vizard, 2020). Healthcare research companies have also been targets. The biotechnology research firm 10x Genomics and the UK-based Hammersmith Medicines Research were breached during this outbreak, both companies are working COVID-19 related research (Davis, 2020). These examples are just some of the ones that were discovered, but they also posed the question of how are these attacks occurring?

**Technical**

There are several approaches for threat actors to initiate a phishing attempt during this outbreak, according to Symanovich. The emails are disguised as CDC alerts, Health advice, or Workplace policy updates and within these emails, there is either a link or an attachment that executes the threat actor’s malware. But how would this malware look if we broke down the malware to its code? Our goal was to create a program/script that was simple enough for a beginner programmer to replicate and launch with minimal understanding of how it works. For our first method of attack (intended for Windows users), we created a script using python. This script then used a variety of libraries to call methods or functions to then look through the victim's computer and gain information. Some of the information that we will be looking for are as follows: Operating system (checks version), Pictures, Documents, Downloads, Clipboard, etc. Once this information is gathered the program then initiates a key listener and stores the values in a text file that was created when the program was first executed. The program is then set up to send all the information gathered to a dummy email for extraction. If successful and the program runs into no errors, the program is then instructed to wipe its trail by deleting log files and all files that it has created. However, these settings can be adjusted for further reconnaissance and stay on the victim's machine for as long as necessary. This kind of program is one of the warnings by Symanovich. The information gathered by this could be used by a threat actor to compile a word list in order to brute-force attack a victim computer or login to a website or other accounts.

Our second attack (intended for Mac users) is based on a different form of malware that creates a backdoor into the victim's machine that will allow us to create a remote session where we can either perform reconnaissance or take control of the machine. However, we took this script a step further and disguised the script. We started off by creating a listener using a program called Empire. This program is commonly known as an open-source post-exploitation framework and Powershell endpoint. It has a wide range of modules used by all skill levels and adapts well with network communications. Once the listener was created, we then staged how the exploit would be used. This then provided us with encrypted code that would then be put on the server that we would be hosting. The reason why we would want to put the code on a server is that we can then bypass antivirus or spyware and can be reached from anywhere. We then created an AppleScript that would connect to the remote server that we are hosting, which then pulls the script that we created from the server. To make things more interesting, the server that we are hosting also contains a real pdf that is pulled down as well and tricks the victim into believing that they opened an authentic pdf while creating a backdoor into their system. Once we establish a connection with the victim's system, we are then capable of performing reconnaissance on the system or even take it over and put other malicious programs on it. After being able to replicate a potential attack, our next thought process is how would we protect businesses or individuals from becoming prey?

**Mitigation**

The easiest way to prevent a phishing attempt from succeeding is user training. Symanovich, from Norton, mentions the following as suggestions:

* **Beware of online requests for personal information.** A coronavirus-themed email that seeks personal information like your Social Security number or login information is a phishing scam. Legitimate government agencies won’t ask for that information. Never respond to the email with your personal data.
* **Check the email address or link.** You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it’s obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses. Delete the email.
* **Watch for spelling and grammatical mistakes.** If an email includes spelling, punctuation, and grammar errors, it’s likely a sign you’ve received a phishing email. Delete it.
* **Look for generic greetings.** Phishing emails are unlikely to use your name. Greetings like “Dear sir or madam” signal an email is not legitimate.
* **Avoid emails that insist you act now.** Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now. Instead, delete the message.
* **Train your email filter.** No one is perfect so taking the time to make sure your email is filtering out unwanted messages reduces the overall risk of clicking on a phishing email. (Specter, 2016)

For businesses that are still trying to maintain normal operations, there are several steps that could be taken to protect the company’s systems. (Guruswamy, 2019)

* **Invest in other forms of protection.** User training might not be enough to protect your business, so creating/ buying spam filters will prevent a lot of spam from getting to your users.
* **Switch to a more secure service.** If you are still getting a lot of spam then switching to another service that is more secure with better customization will hopefully suit exactly what your business needs.
* **Isolate users from certain sites.** Keep on top of various phishing attacks via blocking or other means that adds another layer of protection to your users. Also, try isolating your email server as much as possible.

**Conclusion**

As the current situation in the world continues to change and evolve individuals and companies need to remain vigilant in their practices. The method of the attacks, including delivery as well as execution, and how to attempt to mitigate the problem have been covered. As technology evolves and defenses improve, threat actors will continue to adapt as well in order to try to remain profitable. Ultimately it comes down to the individual using smart practices and the companies attempting to block incoming threats. As long as businesses and individuals remain vigilant this targeted attack can become less effective.

**References**

Cimpanu, C. (2020, April 29). Kaspersky: RDP brute-force attacks have gone up since start of COVID-19. Retrieved April 29, 2020, from <https://www.zdnet.com/article/kaspersky-rdp-brute-force-attacks-have-gone-up-since-start-of-covid-19/>

Davis, J. (2020, April 8). Another COVID-19 Research Firm Targeted by Ransomware Attack. Retrieved April 27, 2020, from <https://healthitsecurity.com/news/another-covid-19-research-firm-targeted-by-ransomware-attack>

Executive Order Number 55 pages 1-3, 2020. <https://www.governor.virginia.gov/media/governorvirginiagov/executive-actions/EO-55-Temporary-Stay-at-Home-Order-Due-to-Novel-Coronavirus-(COVID-19).pdf>

Guruswamy, K., Cohen, L., Robert, Strassman, M., Jennings, R. Vizard, M. (2019, December 5). How to Mitigate Phishing Threats inYour Organization. Retrieved from <https://securityboulevard.com/2019/12/how-to-mitigate-phishing-threats-inyour-organization/>

Hoffman, C. (2019, November 23). What Is a VPN, and Why Would I Need One? Retrieved April 27, 2020, from <https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/>

Spector, Lincoln. “5 Ways to Stop Spam from Invading Your Email.” *PCWorld*, PCWorld, 7 June 2016,

[www.pcworld.com/article/3072435/5-ways-to-stop-spam-from-invading-your-email.html](http://www.pcworld.com/article/3072435/5-ways-to-stop-spam-from-invading-your-email.html)

Symanovich, S. (n.d.). Beware of these coronavirus scams. Retrieved April 27, 2020, from <https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html>

Vizard, M. (2020, April 23). SBA Loan Program for COVID-19 Relief Suffers Data Breach. Retrieved April 27, 2020, from <https://securityboulevard.com/2020/04/sba-loan-program-for-covid-19-relief-suffers-data-breach/>