COVID-19 & Cyber Attacks

A Presentation by Defensury Inc.

Table of Contents

COVID-19 & Cyber Attacks

- The cyber security industry has never had a more important role to play than keeping mission-critical organizations and agencies safe from cyber attacks during this COVID-19 pandemic.
- No single health crisis after the emergence of the internet has changed the technology landscape more than the emergence and impact of COVID-19
- The lockdown in countries and sudden activation of **“work from home”** policies by organizations have put IT systems to the test as more than a third of the world’s corporate workforce have to conduct business activities in the confines of their homes exposing the difficulties in managing the security of IT assets used by staff and ensuring confidentiality, integrity and availability of corporate data.

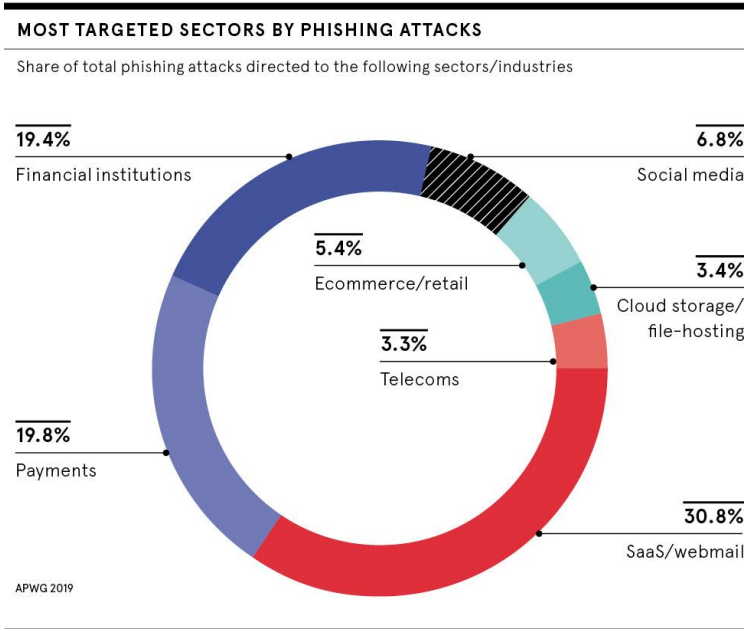
COVID-19 & Cyber Attacks Continued

- The Department of Homeland Security's Cyber Security & Infrastructure Security Agency lists critical industries as medical and health care, telecommunications, defense, food and agriculture, transportation and logistics, electric power, petroleum, water, wastewater, law enforcement and public works.

COVID-19 & Cyber Attacks Continued

- Below is a breakout of specific phishing attacks across the globe:

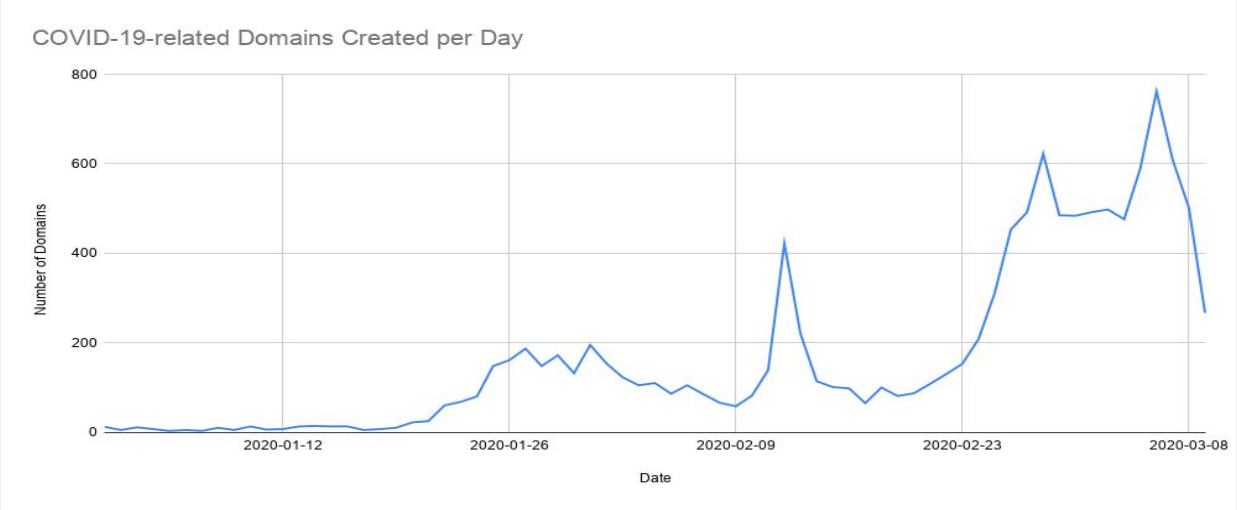
Image from Raconteur.net



COVID-19 & Cyber Attacks Continued

- Since January 29th, when cyber security firms began tracking malicious activity associated with COVID-19, Proofpoint (a software company) has recorded 500,000 messages, 300,000 malicious URLs, and 200,000 malicious attachments with COVID-19 themes within 140 campaigns.

Graph showing the registrations of COVID-19-related domains per day in 2020. Recorded Future analysts created a query to find domain registrations of URLs containing “corona,” “covid19,” or “covid2019.”



Attack Methods

- Credential Phishing Emails
  - Using a company-wide email to target retail companies, and other businesses, this style of attack uses concerns about infected staff members to try and lure victims to click a specific link leading to Microsoft Office credential phishing.
    - One example was a specific campaign used in the US entitled, ***"COVID-19 Infected Our Staff"*** which was listed in the subject line. This then hooks the reader and leads to the body, which claims "a staff member of our company has contracted this deadly disease (COVID-19)"
    - The email then encourages the recipient to open/download a malicious attachment entitled **"follow the company's new protocol"**. The attachment then links to a webpage that spoofs the Microsoft Office login and asks the user for their credentials. In return the attacker receives all login information from the user.

Attack Methods Continued

- Malware & Ransomware
  - Malware & Ransomware campaigns can target manufacturing, construction, transport, healthcare, automotive, energy and aerospace using the GuLoader and Agent Tesla tools.
    - They may spoof a user/reader by using real addresses such as the World Health Organization (WHO).
    - The subject could be something to the effect of, ***“Breaking!!! COVID-19 Solution Announced by WHO As A Cure is Finally Discovered”***.
    - Opening, or running the attachment then has GuLoader installing Agent Tesla, a Trojan written in Visual Basic that can steal usernames, passwords, and credit card information from the user’s system.

Attack Methods Continued

- Video Conferencing
  - Video communication platforms like Zoom and Google Classroom have come under attack.
    - Victims may get an email saying your company is having a Zoom meeting with a link to download what appears to be a file with the word “Zoom” in it. This will then lead to another malware attack if it is in fact a false Zoom link
- Text Alerts
  - Text alerts with links related to COVID-19 supposedly from the government can be sent via the standard messaging app on smartphones. It is easy to fake text messages because there isn’t a standard way for senders to be verified by Internet providers.
- Obtain Sensitive Information
  - Typically a link to a fake login page, or to convince the victim to send resources (money and even equipment) via fake invoices, fake purchase orders and even fake charities.

Consequences

- Identity Theft
- Intellectual Property Theft
- Bank Fraud
- Health Record Theft
- Data Loss from One’s Business
- Significant Legal Liability
- Negative Media/Public Relations Attention

Common Mistakes

- The work from home dynamic creates a very opportunistic situation for hackers and phishers. Every home device or wireless connection is a potential entry point. Moreover, with employees justifiably focusing on other things--their children, pets, health concerns, finances, etc.--data security is understandably not top of mind and employees' typical safeguards against cyber attacks are down.
  - Not understanding what a "phishing" email is
  - Opening emails that are from a source out of fear thinking it is from one's business/employer/employee
- Not using a secured network
- Malicious applications e.g. downloaded games on work/business computers
- Connecting non secure devices (USB, private cell phones, etc.) to your computer

Risk Mitigation

- Appropriate Planning
- Company Policies Put in Place
- Employee Education and Communication
- Having Owners and Employees Install a VPN (Virtual Private Network) on Their Computer at Home
  - Do All Company Employees, Subcontractors and Relevant Third Parties Have Clear Instructions and Guidance on How to Conduct Their Work in a Secure Manner?
- Adopt Strong Passwords
- Backup Your Data
- Check Spelling and Grammar Before Opening an Email or Clicking a Link

Risk Mitigation Continued

- Ensure the Latest Firmware is Installed
- Logout Frequently
- Always Check the Source/Sender of an Email or Attachment
- Ensure to Verify the Validity of the Website
- Never Download any Non-Work Applications or Software to Your Work Computer
- Just Remember to NEVER Connect Any Private/Unknown Devices to Your Work Computer
- When Not Working on Your Computer--SHUT IT DOWN!

Q&A & Notes