Microsoft takes legal action against COVID-19-related cybercrime

blogs.microsoft.com/on-the-issues/2020/07/07/digital-crimes-unit-covid-19-cybercrime/

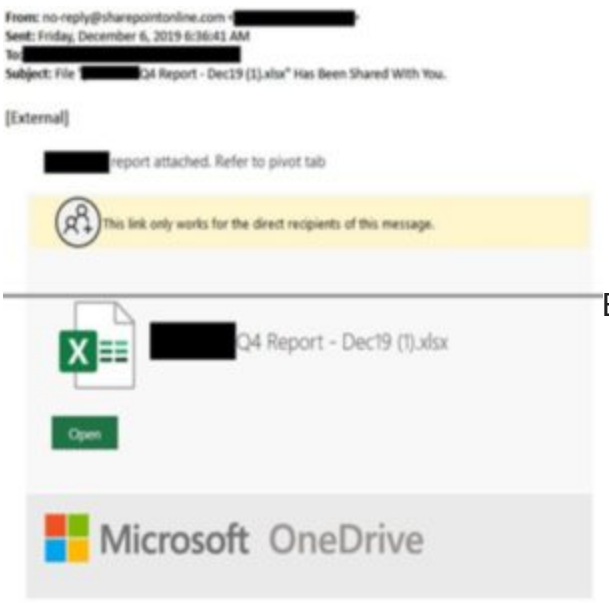
July 7, 2020

Today, the U.S. District Court for the Eastern District of Virginia unsealed documents detailing Microsoft's work to disrupt cybercriminals that were taking advantage of the COVID-19 pandemic in an attempt to defraud customers in 62 countries around the world. Our civil case has resulted in a court order allowing Microsoft to seize control of key domains in the criminals' infrastructure so that it can no longer be used to execute cyberattacks.

Microsoft's Digital Crimes Unit (DCU) first observed these criminals in December 2019, when they deployed a sophisticated, new phishing scheme designed to compromise Microsoft customer accounts. The criminals attempted to gain access to customer email, contact lists, sensitive documents and other valuable information. Based on patterns discovered at that time, Microsoft utilized technical means to block the criminals' activity and disable the malicious application used in the attack. Recently, Microsoft observed renewed attempts by the same criminals, this time using COVID-19-related lures in the phishing emails to target victims.

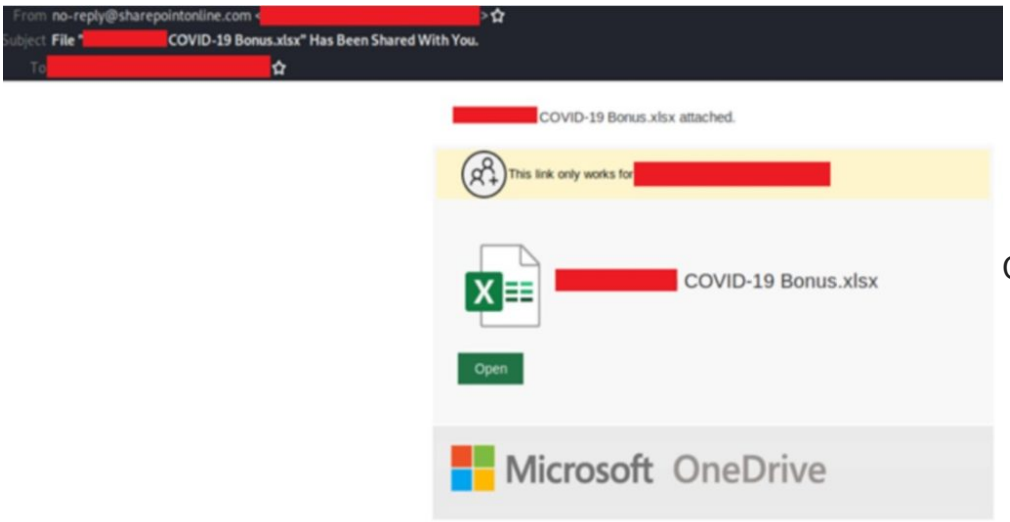
This malicious activity is yet another form of business email compromise (BEC) attack, which has increased in complexity, sophistication and frequency in recent years. According to the FBI's 2019 Internet Crime Report, the most-costly complaints received by their Internet Crime Complaint Center (IC3) involved BEC crimes, with losses of over $1.7 billion, representing nearly half of all financial losses due to cybercrime. While most of the public's attention in recent years has justifiably focused on the malign acts of nation state actors, the increasing economic harm caused by cybercriminals must also be considered and confronted by the public and private sectors. For our part, Microsoft and our Digital Crimes Unit will continue to investigate and disrupt cybercriminals and will seek to work with law enforcement agencies around the world, whenever possible, to stop these crimes.

These cybercriminals designed the phishing emails to look like they originated from an employer or other trusted source and frequently targeted business leaders across a variety of industries, attempting to compromise accounts, steal information and redirect wire transfers. When the group first began carrying out this scheme, the phishing emails contained deceptive messages associated with generic business activities. For example, the malicious link in the email was titled with business terms such as "Q4 Report – Dec19," as seen below.



Business-themed phishing email

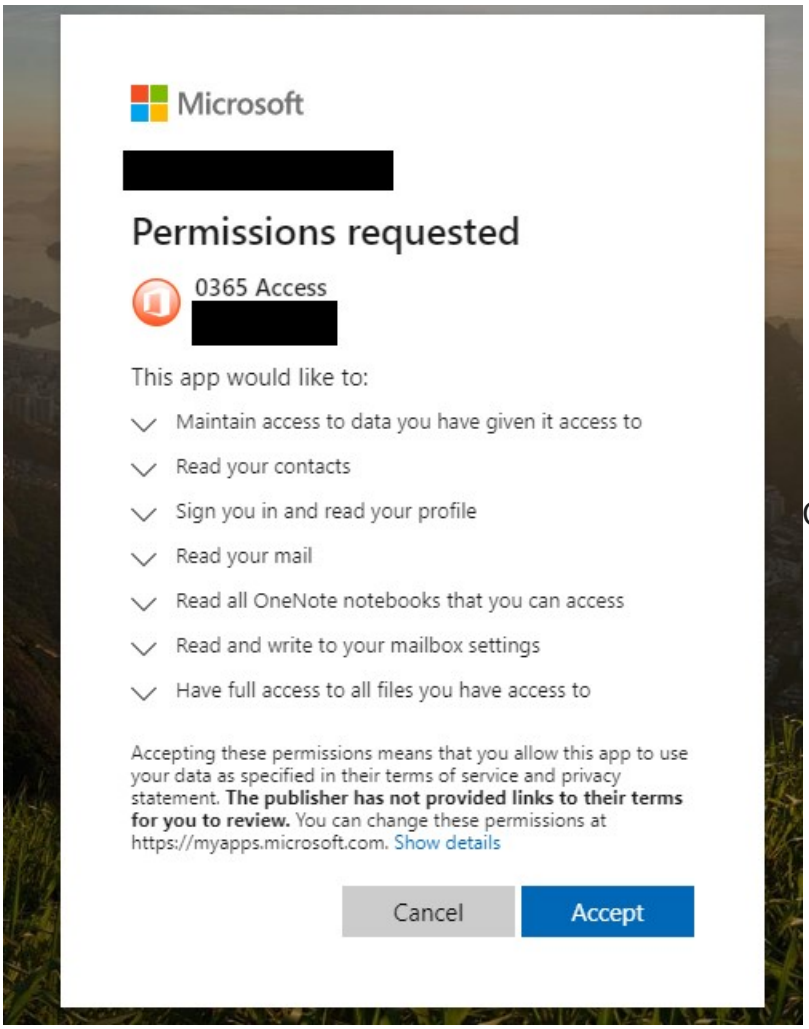
With these recent efforts, however, the phishing emails instead contained messages regarding COVID-19 as a means to exploit pandemic-related financial concerns and induce targeted victims to click on malicious links. For example, using terms such as "COVID-19 Bonus," as seen here.



COVID-19-themed phishing email

Once victims clicked on the deceptive links, they were ultimately prompted to grant access permissions to a malicious web application (web app). Web apps are familiar-looking as they are widely used in organizations to drive productivity, create efficiencies and increase security in a distributed network. Unknown to the victim, these malicious web apps were controlled by the criminals, who, with fraudulently obtained permission, could access the victim's Microsoft Office 365 account. This scheme enabled unauthorized access without explicitly requiring the victims to directly give up their login credentials at a fake website or similar interface, as they would in a more traditional phishing campaign.

After clicking through the consent prompt for the malicious web app (pictured below), the victim unwittingly granted criminals permission to access and control the victims' Office 365 account contents, including email, contacts, notes and material stored in the victims' OneDrive for Business cloud storage space and corporate SharePoint document management and storage system.



Consent screen of the malicious web app

Microsoft takes many measures to monitor and block malicious web apps based on telemetry indicating atypical behavior and has continued to enhance our protections based on this activity. In cases where criminals suddenly and massively scale their activity and move quickly to adapt their techniques to evade Microsoft's built-in defensive mechanisms, additional measures such as the legal action filed in this case are necessary. This unique civil case against COVID-19-themed BEC attacks has allowed us to proactively disable key domains that are part of the criminals' malicious infrastructure, which is a critical step in protecting our customers.

As we've observed, cybercriminals have been adapting their lures to take advantage of current events, using COVID-19-related themes to deceive victims. While the lures may have changed, the underlying threats remain, evolve and grow, and it's more important than ever to remain vigilant against cyberattacks.

To further protect yourself against phishing campaigns, including BEC, we recommend, first, that you enable two-factor authentication on all business and personal email accounts. Second, learn how to spot phishing schemes and protect yourself from them. Third, use SmartScreen and consider blocking email auto-forwarding to make it harder for

cybercriminals to steal your information. Businesses can learn how to recognize and remediate these types of attacks and also take these steps to increase the security of their organizations.

Tags: business, COVID-19, cyberattacks, cybercrime, Digital Crimes Unit, Office 365, phishing