Focus On...

Helping you bring your organization into focus.™

June 2020 • Volume 10, Issue 6

CYBER

In These Uncertain Times, The Prometheus Team Is Here To Help

The Prometheus Team recognizes that we are operating during unprecedented times. The world in which you, your businesses, and all of us function has changed drastically and quickly. We also understand that many of you are fully occupied managing day-to-day operations in a new environment. To give back and alleviate capacity issues, we are allowing customers to activate our 24/7 SOC, Prometheus, for free for three weeks to help you push through.

While you and your team are concerned with other matters, the Prometheus team will monitor alerts on your behalf and notify you if anything urgent requires your attention.

In order to activate this service, we have made it incredibly simple:

- *Call Cheryl Buntin at (813) 309-4482.*
- *Schedule a "Prometheus Kick-off Call" between Monday, June 8 – Tuesday, June 30.*
- *Discuss deployment details with our team.*
- *Deploy Prometheus through the month of June.*

Prometheus stands in solidarity with our customers during COVID-19. We realize the impact it is having on our customers, and all businesses around the world. Prometheus understands what your IT teams are currently dealing with and we are ready and willing to do what we can to help ease the capacity concerns you're facing.

We are in this with you and will continue playing our part to assist you through these uncertain times.

PROMETHEUS
by Focus Audits

Inside This Issue

Cyber: In These Uncertain Times, The Prometheus Team Is Here To Help

Cyber: Microsoft Warns of COVID-19 Phishing Emails Spreading RAT

Finance: Interagency Statement on Loan Modifications (Revised)

Compliance: OCC Finalizes Rewrite of CRA Rules

Awareness: Creating a Cyber Secure Home

FOCUS AUDITS™

Microsoft Warns of COVID-19 Phishing Emails Spreading RAT

An ongoing "massive" COVID-19-themed phishing campaign is attempting to install the NetSupport Manager remote access tool on Windows devices, according to a series of alerts from the Microsoft Security Intelligence team.

NetSupport Manager is a legitimate administrative tool for remote system administrative access, but attackers can turn this tool into a remote access Trojan, or RAT. This then gives threat actors complete control over an infected device and gives them the ability to move laterally through other parts of the targeted network.

This latest phishing campaign to leverage the COVID-19 pandemic started on May 12 and is ongoing, according to Microsoft. It's also using "several hundred" unique attachments, mainly malicious Excel documents that hide the NetSupport Manager.

"The hundreds of unique Excel files in this campaign use highly obfuscated formulas, but all of them connect to the same URL to download the payload," according to Microsoft. "NetSupport Manager is known for being abused by attackers to gain remote access to and run commands on compromised machines."

The Microsoft alert did not say if this phishing campaign was targeting to a particular geographic region, or how successful these attacks have been so far. Earlier this month, the company sent out another warning about a malicious spam campaign leveraging a COVID-19 theme and targeting victims in the U.S. and South Korea. These attacks were also attempting to install RATs on infected devices.

COVID-19 Theme

In the phishing campaign that Microsoft described [last month], the attacks start with messages pretending to be sent from the Johns Hopkins University, which has been a major source of news about COVID-19, offering daily updates on the number of infections and deaths worldwide.

These phishing emails include an attached malicious Excel file. If opened, it displays a New York Times report on COVID-19 deaths in the U.S.

Once the attachment is opened, malicious macros are enabled that prompt the user to "enable content." This allows the NetSupport Manager installation file to download onto the victim's device from a remote site controlled by the attackers, Microsoft reports.

In the next stage, the NetSupport Manager file is launched as a legitimate desktop Windows Manager executable, which further tricks the victims into granting other permissions that allow for the final payload to be downloaded onto the infected device.

In the final stage, malware then downloads additional components, such as Visual Basic script and an obfuscated PowerSploit-based PowerShell script, which then connect to the command-and-control server, according to Microsoft.

Attackers have been weaponizing the NetSupport Manager tool for some time. In March, for example, researchers at security firm Prevailion uncovered the Russian-based TA505 threat group conducting a business email compromise attack that embedded NetSupport into a victim's Google Drive account to enable remote access control.

Source: *Bank Info Security, Akshaya Asokan (asokan_akshaya), May 22, 2020*

FINANCE

Interagency Statement on Loan Modifications (Revised)

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was signed into law on March 27, 2020 and included a forbearance program for federally backed mortgage loans and protection for borrowers from negative credit reporting due to forbearance. Federal regulators also provided financial institutions with the option to temporarily suspend certain requirements related to troubled debt restructurings (TDR) due to the loan modifications. Section 4013 of the CARES Act, Temporary Relief from Troubled Debt Restructurings, clarified the federal regulatory agencies' (Agencies) interpretation of GAAP accounting rules for COVID-19-related loan modifications.

Generally, modifications of loan terms do not automatically result in a TDR if the modification was a) related to COVID-19; b) provided for a loan than was not more than 30 days past due on December 31, 2019; and c) executed between March 1, 2020 and December 31, 2020 (or earlier). The Agencies have confirmed that short-term modifications made on a good faith basis in response to COVID-19 to borrowers who were current prior to the relief, are not TDRs. This includes payment deferrals, fee waivers, payment extensions, and related deferments. Borrowers that were current prior to payment accommodations would not be reported as past due. Loans that had been adversely classified or risk-rated or that were non-performing or on non-accrual before relief was granted would continue to be subject to the existing classification rules and reporting applicable to that institution.

Most institutions recognize that commercial borrowers in certain industries, such as the hotel, restaurant, event, and retail industries, may be moving into financial distress despite loan modifications and have remained diligent in efforts to properly risk rate and monitor these credits in relation to potential future defaults. Lenders should be proactive and consider downgrading credits that have elevated risk due to the COVID-19 conditions.

As a general rule, borrowers who have been granted a loan modification due to COVID-19 and that was less than 30 days past due at time of modification, should be risk rated as Pass/Watch. The rationale, during this temporary period for which the modification was granted, is that these borrowers now represent more risk than borrowers with a similar risk rating that did not request modifications. Additionally, these credits require a higher degree of monitoring and allows for further downgrading in relation to identified distress or deterioration in the repayment capacity or collateral coverage.

While lenders are encouraged to work with borrowers, any agreement to forebear or modify the terms of the loans should include additional provisions that continue to protect the lender's position, such as additional financial reporting requirements, future default waivers, and additional guarantees or security. It is also important for lenders to ensure that modifications granted do not adversely impact their loan contracts or agreements, such as a force majeure provisions, or other specific covenants that could trigger a default.

For more information, refer to Interagency Statement on Loan Modifications by Financial Institutions Working with Customers Affected by the Coronavirus (Revised) and Frequently Asked Questions for Financial Institutions Affected by the Coronavirus Disease 2019 (Referred to as COVID-19).

Focus On...

COMPLIANCE

OCC Finalizes Rewrite of CRA Rules

On May 20th, the Office of the Comptroller of Currency announced it had released a final rule "strengthening and modernizing" the agency's CRA regulations. "The final rule will increase bank CRA-related lending, investment, and services in low- and moderate-income communities where there is significant need for credit, more responsible lending, and greater access to banking services," the OCC said in a statement. "The final rule reflects careful consideration of the more than 7,500 comments stakeholders submitted in response to the notice of proposed rulemaking announced on December 12, 2019."

The proposal, issued jointly by the FDIC and the OCC, was never joined by the Federal Reserve. FDIC Chairman Jelena McWilliams said the agency supports the rulemaking effort but is not yet ready to sign off on the rule given what's going on in the country right now. "The CRA proposal the OCC and the FDIC issued last December was a culmination of a multi-year effort by the prudential banking regulators to modernize CRA regulations for the first time in a quarter of a century," McWilliams said in a statement.

"While the FDIC strongly supports the efforts to make the CRA rules clearer, more transparent, and less subjective, the agency is not prepared to finalize the CRA proposal at this time," McWilliams added. "The FDIC recognizes the herculean effort community banks are making to support America's small businesses and families during this challenging time and encourages financial institutions to work constructively with borrowers affected by COVID-19."

Fed Chair Jerome H. ("Jay") Powell told lawmakers early this year he was not certain when or if the Fed might act on the joint proposal, or any, on the issue. He also said discussions among the Fed and the other two regulators on this issue had ceased after the release of the December proposal.

In addition to the new rule, the OCC published a revised list of CRA qualifying activities. The final rule is effective October 1, 2020 and only applies to OCC regulated financial institutions.

Focus On...

AWARENESS

Creating a Cyber Secure Home

Overview
In the past, building a home network was nothing more than installing a wireless router and several computers. Today, as so many of us are working, connecting, or learning from home, we have to pay more attention to creating a strong cyber secure home. Here are four simple steps to do just that.

Your Wireless Network
Almost every home network starts with a wireless (or Wi-Fi) network. This is what enables your devices to connect to the Internet. Most home wireless networks are controlled by your Internet router or a separate, dedicated wireless access point. They both work the same way: by broadcasting wireless signals which allow the devices in your house to connect to the Internet. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it.

1. Change the default administrator password to your Internet router or wireless access point, whichever is controlling your wireless network. The administrator account is what allows you to configure the settings for your wireless network.
2. Ensure that only devices you trust can connect to your wireless network. Do this by enabling strong security. Doing so requires a password to connect to your home network and encrypts online activities once connected.
3. Ensure the password used to connect to your wireless network is a strong password that is different from the administrator password. Remember, your devices store passwords, so you only need to enter the password once for each device.

If you're not sure how to do these steps, check your Internet Service Provider's website or check the website of the vendor for your router or wireless access point.

Passwords
Use a strong, unique password for each of your devices and online accounts. The key words here are strong and unique. The longer your password the stronger it is. Try using a series of words that are easy to remember, such as ***sunshine-doughnuts-happy***.

A unique password means using a different password for each device and online account. Use a password manager to remember all those strong passwords, which is a security program that securely stores all your passwords for you in an encrypted, virtual safe.

Additionally, enable two-step verification whenever available, especially for your online accounts. It uses your password, but also adds a second authentication step, such as a code sent to your smartphone or an app on your smartphone that generates the code for you. This is probably the most important step you can take, and it's much easier than you think.

Your Devices
The next step is knowing what devices are connected to your wireless home network and making sure all of those devices are trusted and secure. This used to be simple when you had just a computer. However, today almost anything can connect to your home network, including your smartphones, TVs, gaming consoles, baby monitors, printers, speakers, or perhaps even your car. Once you have identified all the devices on your home network, ensure that each of them is secure. The best way to do this is to change any default passwords on them and enable automatic updating wherever possible.

Backups
Sometimes, no matter how careful you are, you may be hacked. If that is the case, often the only way you can recover your personal information is to restore from a backup. Make sure you are doing regular backups of any important information and verify that you can restore from them. Most mobile devices support automatic backups to the Cloud. For most computers, you may have to purchase some type of backup software or service, which are relatively low-priced and simple to use.

Source: Randy Marchany, CISO of Virginia Tech, Guest Editor
SANS Security Awareness