October 2020 ♦ Issue 10

Solutions

INSIDE THIS ISSUE

AaSys Group will be closed on the Following Days:

- Thursday, November 26, 2020 in observance of Thanksgiving
- Friday, November 27, 2020 AaSys Helpdesk will close at 3PM
- Thursday, December 24, 2020 AaSys Helpdesk will close at 3PM
- Friday, December 25, 2020 in observance of Christmas Day
- Thursday, December 31, 2020 AaSys Helpdesk will close at 3PM
- Friday, January 1, 2021 in observance of New Year's Day

"Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations."

AaSys®
Solutions are our Business

Department of Treasury Releases Advisory

October is National Cybersecurity Awareness Month, designated to raising awareness about the importance of cybersecurity across our nation, ensuring that we all have the resources and knowledge needed to be safer and more secure online. But while corporations are trying to continue to be safe and use best practices, the U.S Department of Treasury put out a stark advisory to financial institutions, cyber insurance firms, and companies that facilitate payments on behalf of victims of ransomware attacks, that they may be violating OFAC regulations.

On October 1, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued a warning to advise companies that they may be essentially breaking the law if they engage in money exchange with bad actors due to a ransomware attack. The advisory read in part, "Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations."

Ransomware is a type of malware that threatens to publish the victim's sensitive data or perpetually block access to it unless a ransom is paid.

Continued on page 2

Over the years, our consumption of data has increased dramatically making everyone using the Internet more vulnerable to attacks and making cybercriminals more brazen with their efforts to obtain sensitive data. Data is the new commodity, and bad actors understand how important that information is to many organizations, therefore ransomware attacks have been more successful than not. But our government has drawn a line in the sand. Negotiating with cybercriminals, in their view, encourages them to strike again and making their next demand more outrageous than the first and may even put our national security interest at risk.

But this new advisory puts U.S companies between a rock and hard place. Those who fall victim to such ransomware attacks will either have to refuse the demand, in some cases with catastrophic commercial consequences or pay the demand without OFAC authorization and be in potential violation of U.S. sanctions law. Anyone who helped facilitate a payout due to a ransomware attack may not only be in violation of U.S. sanctions, but may also be subject to civil penalties even if they did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

Ransomware attacks will not stop, but organizations must take all the necessary steps to protect their data by making sure they are educated on the potential risks. OFAC has advised they will look at the type of compliance process victims have in place when determining a penalty for anyone who violated sanctions. More now than ever it is important that your organization has a solid compliance plan in place that will help mitigate any type of attack. If you need assistance with ransomware compliance issues, please reach out to your AaSys Account Executive today. It will not only be important to your businesses health but it also protects our national interest.

Sources:
https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
https://blog.rapid7.com/2020/10/06/ransomware-payments-and-sanctions-u-s-treasury-advisory/#:~:text=On%20Oct.,entities%20risks%20violating%20the%20law.
https://www.justice.gov/criminal-ccips/page/file/1252341/download
https://www.securitymagazine.com/articles/93533-department-of-treasury-releases-advisory-on-potential-sanctions-risks-for-facilitating-ransomware-payments

National Cybersecurity Awareness Month - Ransomware

Now in its 17th year, National Cybersecurity Awareness Month (NCSAM) continues to raise awareness about the importance of cybersecurity across our nation, ensuring that we all have the resources needed to be safer and more secure online. Although cybersecurity should remain at the forefront every day, National Cybersecurity Awareness Month features collaborations from the industry's best on how to make the Internet safer for everyone.

Each year, the campaign tries to raise awareness and educate the public and businesses on the dangers that lurk on the Internet while also addressing certain themes. This year, the theme is "Do Your Part. #BeCyberSmart." This theme encourages individuals and organizations to own their role in protecting their part of cyberspace, stressing personal accountability and the importance of taking proactive steps to enhance cybersecurity. Each day we depend on technology to complete our daily activities as well as perform some of our most important civic duties. While we are still in a pandemic, cybercriminals are using this to conduct an unprecedented amount of attacks. Having a month designated to cybersecurity safety stresses the fact it is imperative that we all work together to keep the online space protected and safe.

One of the most dangerous cybersecurity threats is ransomware. Ransomware is malware that locks down data by encrypting it and basically holding it hostage until a ransom is paid. Ransomware has been around for a while but the strategies in which criminals use them have progressed and experts believe they are getting worse. Ransomware gangs have sprung up all over the world within the last couple of years. Their demands have become more egregious and they are moving to not only target the financial sector, but also manufacturing and government entities. The theory is these ransomware gangs are seeking victims who cannot afford to have significant down time, thus making the likelihood for them to pay up very high. They have also changed tactics by stealing the sensitive data before they encrypt it.

Continued on page 4

If the victim does not pay, the cybercriminal will use the data as a bargaining chip and threaten to release the information if their demands are not met. This essentially is extortion. But victims not only have to worry about the sensitive data released, they also have to worry about the implications of possibly breaking privacy laws, being out of compliance with regulators and now possibly being sanctioned by the United States Department of Treasury if they give in and pay the ransom.

Ransomware is something that everyone should take extremely seriously and ensure that all measures are taken to prevent such an attack. Phishing and ransomware usually work hand in hand, such that a failure to prevent a phishing attempt is typically the gateway to a successful ransomware attack.

Organizations must protect themselves by:

- Looking for signs of suspicious emails and training all employees on how to recognize such emails.
- Making sure your antivirus software is up to date and running.
- Never clicking on links that are unverified.
- Having a plan for how to respond to a ransomware attack, and testing it, and then testing it again!
- Knowing and understanding what's connected to your network.
- Making sure software patches are always up to date.
- Creating an effective backup strategy.
- Making sure all data is backed up daily.
- Never downloading media files or software from unknown websites.

As the month of October comes to an end and the recognition of Cybersecurity Awareness Month moves to next year, take time to review some of the resources provided by The National Cybersecurity Alliance and Stop. Think. Connect. Campaign. As our world continues to become more digitalized everyone must remain vigilant. While being more connected through the Internet brings more efficiency and cost savings, what we all must realize is cyber threats are best combated by sharing vital information and making sure each one of us is educated on the potential risk.

AaSys understands the risk organizations face on daily basis. As a leader within the network security industry AaSys utilizes a layered approach to securing networks and system hardening. By using the most stringent cybersecurity frameworks, AaSys can help protect your organization without sacrificing functionality and performance. To learn more, contact your AaSys Account Executive today.

Sources:
https://www.cisa.gov/national-cyber-security-awareness-month
https://staysafeonline.org/cybersecurity-awareness-month/
https://www.zdnet.com/article/ransomware-11-steps-you-should-take-to-protect-against-disaster/
https://www.zdnet.com/article/ransomware-gang-donates-part-of-ransom-demands-to-charity-organizations/