SAIAF

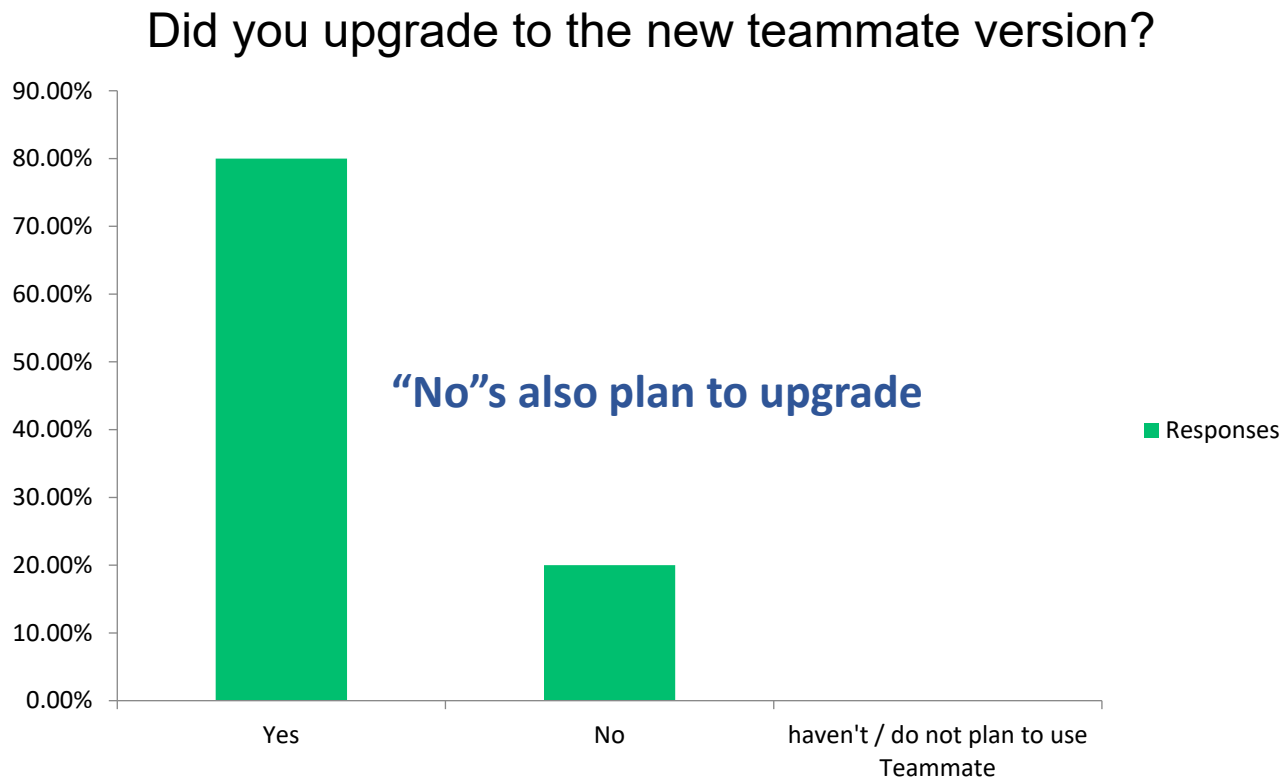
Information Technology Update

December 2, 2022

Agenda:

- Teammate Upgrade Survey Results
- Refresher – OWASP Top 10
- Refresher - ***TX-RAMP Approvals***
- Texas Cybersecurity Activity and Considerations Bulletin (Last Issue – April 2022)
- FBI Press Releases (Recent)

Teammate Update Survey Results



10 Respondents

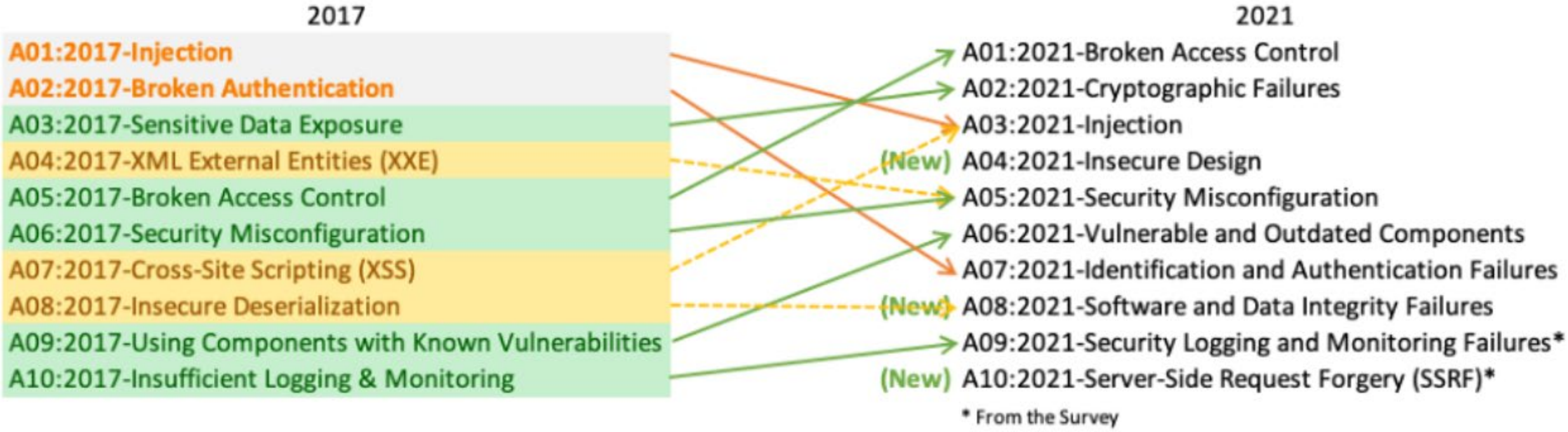
- The main reason for upgrading: ***Teammate AM End of Life****
- 7/10 agencies using Teammate + have the hosted version or plan to procure the TX-RAMP compliant hosting version.

* End of life date is early 2023

OWASP TOP 10

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



Source: https://owasp.org/www-project-top-ten/

TX-RAMP Requirements

Texas Government Code 2054.0593 mandates that state agencies as defined by Texas Government Code 2054.003(13) must only enter or renew contracts to receive cloud computing services that comply with TX-RAMP requirements beginning January 1, 2022.

A Manual is available on DIR's website at:
https://dir.texas.gov/information-security/texas-risk-and-authorization-management-program-tx-ramp

When does it take effect?

- Cloud offerings subject to TX-RAMP Level 1 certification must obtain a TX-RAMP certification to contract with state agencies or institutions of higher education and public community colleges on or after **January 1, 2024**.
- Cloud offerings subject to TX-RAMP Level 2 certification must obtain a TX-RAMP certification to contract with state agencies or institutions of higher education and public community colleges on or after **January 1, 2022**.
- Cloud offerings that obtain TX-RAMP Provisional Status must obtain a TX-RAMP certification (or equivalent StateRAMP/FedRAMP authorization) within **18 months** from the date that Provisional Status is conferred as reflected in DIR's files.

Texas Cybersecurity Activity and Considerations Bulletin (April 2022 Last issue)

Considerations to Improve Security There is no single tool, solution, or process that can eliminate the risk of ransomware attacks but adopting cybersecurity best practices and taking the proactive measures provided below can minimize an organization's risk of significant ransomware impacts.

BEST PRACTICES

- Develop a strong culture of cybersecurity awareness
- Create an incident response plan
- Establish a functional vulnerability and patch management program
- Maintain reliable backups
- Coordinate tabletop exercises with organization leadership and technical staff
- Implement multi-factor authentication (MFA)
- Deploy Endpoint Detection and Response (EDR) solutions

Source: https://dir.texas.gov/sites/default/files/2022-06/TLP%20White-%20Cybersecurity%20Activity%20and%20Considerations%20Bulletin%20_June%202022.pdf

FBI Press Releases (https://www.fbi.gov/investigate/cyber)

Subjects fall into the following areas:

- Crypto Fraud Schemes
- Identity Theft
- Cybercrime
- Cyber Stalking / Stalking
- Extortion
- Child Pornography
- Obstruction of Justice
- Wire Fraud
- Threatening elected official

✓ The next section contains just some of the more recent Releases that seemed interesting or relevant.

DIR General Public Alerts or Notices (Some of the more interesting ones)

Title	Scheme	Date Released
Investment Manager Arrested for $10 Million Cryptocurrency Ponzi Scheme **Link: https://www.justice.gov/opa/pr/investment-manager-arrested-10-million-cryptocurrency-ponzi-scheme**	According to court documents, Rathnakishore Giri, 27, of New Albany, allegedly misled investors by fraudulently promoting himself as an expert cryptocurrency trader, with a specialty in trading Bitcoin derivatives. As alleged in the indictment, Giri falsely promised investors that he would generate lucrative returns with no risk to their principal investment amount, which he guaranteed to return. In reality, Giri often allegedly used money provided by new investors to repay old investors – a hallmark of a Ponzi scheme. In addition, Giri allegedly had a record of investment failures, including a long history of losing investors' principal investments, and misled investors about reasons for delays when they sought to cash out their investments or otherwise obtain the return of their "guaranteed" principal. Giri is charged by indictment with five counts of wire fraud.	November 18, 2022
Former DMV Employee Sentenced to 5 Years in Prison for Participating in Corrupt Bribery Conspiracy involving Commercial Driver Licenses **Link: https://www.justice.gov/usao-edca/pr/former-dmv-employee-sentenced-5-years-prison-participating-corrupt-bribery-conspiracy**	According to court documents, Harris was a long-time DMV employee who had the ability to update test scores for commercial driver's license applicants in California. Using her position as a public employee at the DMV, Harris accepted bribes in exchange for fraudulently updating test scores for people pursuing commercial driver's licenses. For at least 185 commercial license applicants, Harris used her access to DMV computers to enter fraudulent test scores indicating the applicants had passed written and/or behind the wheel commercial drive tests, when in reality the applicants had not passed those tests. Harris and a co-conspirator were typically paid at least $1,500 per applicant for fraudulently updating test scores, resulting in approximately $277,500 worth of corrupt bribes.	November 3, 2022

DIR General Public Alerts or Notices (Some of the more interesting ones)

Title	Scheme	Date Released
Band Of Cybercriminals Responsible For Computer Intrusions Nationwide Indicted For RICO Conspiracy That Netted Millions **Link: https://www.justice.gov/usao-mdfl/pr/band-cybercriminals-responsible-computer-intrusions-nationwide-indicted-rico-conspiracy**	Jenkins, Michel, Propht-Francisque, Cherelus, and RICH4EVER4430 purchased on the dark web server credentials for the computer servers of Certified Public Accounting (CPA) and tax preparation firms across the country. They used those server credentials to remotely and covertly commit computer intrusions and exfiltrate the tax returns of thousands of taxpayers who were clients of those CPA and tax preparation firms. Those tax returns included the clients' names, dates of birth, Social Security numbers, and financial information. Jenkins, Michel, Propht-Francisque, Cherelus, RICH4EVER4430, and other conspirators then partnered with Jacques, Elan, Poix, Jolteus, and others to form an enterprise through which they filed thousands of false tax returns in the names of more than 9,000 identity theft victims. Members of the enterprise created and operated at least six fraudulent tax preparation businesses in south Florida, and used those businesses to file many of these false tax returns. The conspirators directed the resulting tax refunds to debit cards and bank accounts that they controlled. Also, to make the businesses appear more legitimate, members of the enterprise opened bank accounts in the names of these fraudulent tax businesses to receive fake "tax preparer fees." Members of the enterprise also registered with the Internal Revenue Service (IRS) preparer tax identification numbers using the names and information of identity theft victims, to make it appear that those victims were the individuals who were filing false returns in bulk.	November 1, 2022

DIR General Public Alerts or Notices (Some of the more interesting ones)

Title	Scheme	Date Released
Six Defendants Charged In $1 Million Covid Fraud Schemes **Link: https://www.justice.gov/usao-wdmi/pr/2022_1027_Beaty_et_al**	The indictment alleges that, between April 2020 and December 2021, Roshell Beaty and her codefendants conspired to commit wire fraud by submitting falsified and fraudulent claims and certifications for pandemic unemployment insurance benefits, in their own names and in the names of third parties, some of whom were victims of identity theft. According to the indictment, the six codefendants submitted at least 98 false and fraudulent unemployment insurance claims and related certifications in multiple states, in the names of at least 61 different individuals. In response to those claims, the states of Michigan, Indiana, California, Illinois, and Arizona paid out more than $764,000 in pandemic unemployment insurance benefits. Each of the six defendants is also charged with respective counts of wire fraud related to pandemic unemployment insurance fraud. Two defendants—Roshell Beaty and her son Christopher Branch—are charged with various counts of aggravated identity theft, for using the means of identification of other people without lawful authority, in connection with the unemployment insurance wire fraud conspiracy. Defendants Roshell Beaty, Melvin Clinton, Danielle Branch, and Christopher Bates are each charged with fraud in connection with emergency benefits. In addition to charges stemming from unemployment insurance fraud schemes, five of the six defendants are charged in the indictment with varying counts of wire fraud and conspiring to commit wire fraud in connection with their alleged fraudulent receipt of loans intended to relieve small businesses of burdens and costs associated with the pandemic. Roshell Beaty and Melvin Clinton face charges for an Economic Injury Disaster Loan in the amount of $49,900, for a purported hair and nail salon belonging to Clinton, with 10 employees. The Indictment alleges that loan proceeds were used to purchase a 2017 Jaguar F-Pace SUV. Roshell Beaty, Melvin Clinton, Danielle Branch, Christopher Bates, and Brianna Rimpson are charged in connection with Paycheck Protection Program loans, totaling $258,148, for purported small businesses.	October 27, 2022

DIR General Public Alerts or Notices (Some of the more interesting ones)

Title	Scheme	Date Released
FBI El Paso Warns the Public About Potential Federal Student Loan Forgiveness Fraud Schemes **Link: https://www.fbi.gov/contact-us/field-offices/elpaso/news/press-releases/fbi-el-paso-warns-the-public-about-potential-federal-student-loan-forgiveness-fraud-schemes**	"Scammers will constantly use their effective scam scenarios and tweak them to take advantage of a current situation affecting the community at large. The FBI typically sees this behavior when any new government aid program becomes available," said Special Agent in Charge Jeffrey R. Downey. "The FBI is providing information to the public now to help people recognize the warning signs of potentially fraudulent activity related to the forgiveness of federal student loans. Don't let a scammer trick you into revealing personally identifiable information or providing any type of payment. The U.S. government will not charge any type of processing fees or require any type of payment to have your federal student loans forgiven."	October 26, 2022
Two Men Sentenced for Nationwide Scheme to Steal Social Media Accounts and Cryptocurrency **Link: https://www.justice.gov/opa/pr/two-men-sentenced-nationwide-scheme-steal-social-media-accounts-and-cryptocurrency**	According to court documents, Meiggs and Harrington targeted executives of cryptocurrency companies and others who likely had significant amounts of cryptocurrency and those who had high value or "OG" (slang for Original Gangster) social media account names. Meiggs and Harrington conspired to hack into and take control over these victims' online accounts so they could obtain things of value, such as cryptocurrency. They used an illegal practice known as "SIM-swapping" and other techniques to access, take control of, and in some cases steal cryptocurrency from, the accounts. In "SIM swapping", cybercriminals convince a victim's cell phone carrier to reassign the victim's cell phone number from the SIM card (Subscriber Identity Module card) inside the victim's cell phone to the SIM card inside a cell phone controlled by the cybercriminals. Cybercriminals then pose as the victim with an online account provider and request that the provider send account password-reset links or an authentication code to the SIM-swapped device now controlled by the cybercriminals. The cybercriminals can then reset the victim's account log-in credentials and use the log-in credentials to access the victim's account without authorization, or "hack into" the account.	October 19, 2022

DIR General Public Alerts or Notices (Some of the more interesting ones)

Title	Scheme	Date Released
San Antonio Pair Plead Guilty to SIM Swap Scheme **Link: https://www.justice.gov/usao-wdtx/pr/san-antonio-pair-plead-guilty-sim-swap-scheme**	According to court documents, Andrew Percy Trujillo, 22, along with his co-defendant Zena Elisa Dounson, 34, of San Antonio, devised a scheme to SIM swap mobile customers' phones at a local AT&T store. Dounson was employed at the store and allowed Trujillo to add himself as an authorized user to multiple victims' AT&T accounts where Trujillo then ported a victim's SIM card credentials to his own devices' SIM cards. This caused calls and texts to the victims' phone numbers to be sent to devices controlled by Trujillo rather than the rightful owners. Co-conspirators were able to access the victims' various cryptocurrency accounts and transfer out at least $250,000 worth of cryptocurrency.	October 12, 2022
Former hacker sentenced for stealing computer power to mine cryptocurrency and stealing the personal information of more than 100 million people **Link: https://www.justice.gov/usao-wdwa/pr/former-hacker-sentenced-stealing-computer-power-mine-cryptocurrency-and-stealing**	Using Thompson's own words in texts and online chats, prosecutors showed how Thompson used a tool she built to scan Amazon Web Services accounts to look for misconfigured accounts. She then used those misconfigured accounts to hack in and download the data of more than 30 entities, including Capital One bank. With some of her illegal access, she planted cryptocurrency mining software on new servers with the income from the mining going to her online wallet. Thompson spent hundreds of hours advancing her scheme, and bragged about her illegal conduct to others via text or online forums.	October 4, 2022

DIR General Public Alerts or Notices (Some of the more interesting ones)

Title	Scheme	Date Released
FBI Columbia Warns of Potential Charity and Disaster Fraud Following Hurricane Ian **Link: https://www.fbi.gov/contact-us/field-offices/columbia/news/press-releases/fbi-columbia-warns-of-potential-charity-and-disaster-fraud-following-hurricane-ian**	Whether you are directly impacted or want to help, scammers will take advantage of a natural disaster, like Hurricane Ian, to steal your money, your personal information, or both. That is why the FBI is reminding the public to be vigilant when looking to donate to hurricane relief causes and when searching for contractors to repair damages.	October 4, 2022
Website Selling Stolen Login Credentials and Other Personally Identifying Information is Seized and Its Operator Faces Federal Charges for Conspiracy and Trafficking in Unauthorized Access Devices **Link: https://www.fbi.gov/contact-us/field-offices/columbia/news/press-releases/fbi-columbia-warns-of-potential-charity-and-disaster-fraud-following-hurricane-ian**	The federal criminal complaint alleges that Nicolai Colesnicov, age 36, of the Republic of Moldova, operated WT1SHOP, an online market that allowed vendors to sell stolen login credentials and other PII, including approximately 25,000 scanned driver's licenses/passports, 1.7 million login credentials for various online shops, 108,000 bank accounts, 21,800 credit cards. According to the affidavit filed in support of the criminal complaint, WT1SHOP provided a forum and payment mechanism for the sale and purchase of stolen PII, using Bitcoin. As detailed in the affidavit, in June 2020 Dutch law enforcement officials obtained an image of the WT1SHOP database that showed there were approximately 60,823 registered users on the site, including 91 sellers and two administrators. As of June 2020, sellers on WT1SHOP had engaged in sales of approximately 2.4 million credentials for total proceeds of approximately $4 million. The credentials sold consisted of login credentials for retailers and financial institutions, email accounts, PayPal accounts, and identification cards, as well as credentials to remotely access and operate computers, servers, and network devices without authorization. Law enforcement's review of WT1SHOP in December 2021 showed that the number of users and sellers on the website had increased to approximately 106,273 users and 94 sellers with a total of approximately 5.85 million credentials available for sale.	September 6, 2022

DIR General Public Alerts or Notices (Some of the more interesting ones)

Title	Scheme	Date Released
Former Public Utility Employee Pleads Guilty to Installing Keylogger Devices on Work Computers **Link: https://www.justice.gov/usao-ndoh/pr/former-public-utility-employee-pleads-guilty-installing-keylogger-devices-work**	Pelton installed the keylogger devices at his place of employment on two computers in a control room accessible only via an access badge. According to court records, Pelton installed one keylogger on a control room computer connected to the internet and the utility's internal network and the other on a second computer used in the delivery of services. Court documents state that the keyloggers would allow Pelton to capture an administrator's password and access features that he otherwise was unable to access.	August 10, 2022
Three Nigerian Nationals Extradited to the United States from the United Kingdom for Participating in Business Email Compromise Fraud Schemes **Link: https://www.justice.gov/opa/pr/three-nigerian-nationals-extradited-united-states-united-kingdom-participating-business-email**	According to allegations contained in the indictment, from Aug. 30, 2016, to Jan. 12, 2017, persons conspired with other individuals to obtain information about significant construction projects occurring throughout the United States, including an ongoing multi-million-dollar project at the victim University. To execute the scheme, the defendants allegedly registered a domain name similar to that of the legitimate construction company in charge of the University's project and created an email address that closely resembled that of an employee of the construction company. Using the fake email address, the co-conspirators allegedly deceived and directed the University to wire a payment of more than $1.9 million to a bank account controlled by an individual working under the direction of defendants. Upon receiving the payment, the co-conspirators allegedly laundered the stolen proceeds through a series of financial transactions designed to conceal the fraud	August 10, 2022