SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION
Cyber Alert
PHOENIX DIVISION

Approved for Release: 22 August 2019

SIR Number: SIR-00328362177

(U//FOUO) PHOENIX BI-WEEKLY CYBER REPORT FROM 7 JUNE 2019 TO 20 JUNE 2019

SOURCE: (U) A documentary source.

(U//FOUO) This FBI Phoenix Bi-Weekly Cyber Report provides InfraGard, Strategic Partners and Law Enforcement with a summary of relevant Cyber highlights for the two week period of 7 June 2019 to 20 June 2019. This summary includes information derived from multiple FBI Cyber products, Cyber Guardian incidents affecting Arizona, and the Internet Crime Complaint Center (IC3).

(U) FBI PIN, PSA, FLASH and OTHER CYBER REPORTS

(U//FOUO) On 10 June 2019, the FBI disseminated a Public Service Announcement (PSA) titled, "Cyber Actors Exploit 'Secure' Websites In Phishing Campaigns." Websites with addresses that start with "https" are supposed to provide privacy and security to visitors. After all, the "s" stands for "secure" in HTTPS: Hypertext Transfer Protocol Secure. In fact, cyber security training has focused on encouraging people to look for the lock icon that appears in the web browser address bar on these secure sites. The presence of "https" and the lock icon are supposed to indicate the web traffic is encrypted and that visitors can share data safely. Unfortunately, cyber criminals are banking on the public's trust of "https" and the lock icon. They are more frequently incorporating website certificates—third-party verification that a site is secure—when they send potential victims emails that

imitate trustworthy companies or email contacts. These phishing schemes are used to acquire sensitive logins or other information by luring them to a malicious website that looks secure. For additional information, see FBI Alert Number I-061019-PSA at the InfraGard Portal.

(U) On 10 June 2019, the FBI provided a MS-ISAC cybersecurity advisory titled, "A Vulnerability in Exim Could Allow for Remote Command Execution." A vulnerability has been discovered in Exim, which could allow for local attackers to execute arbitrary system commands when sending mail to a particular recipient. Remote attackers can take advantage of this vulnerability as well through similar means. Exim is a mail transfer agent used to deploy mail servers on Unix-like systems. Successful exploitation of this vulnerability will enable the attacker to perform command execution as root in the context of the mail server. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. There is currently a working exploit of this vulnerability on Exploit DB. Open source resources reveal that currently there are more than 4.7 million devices running a vulnerable version of Exim. This vulnerability does not affect the latest version Exim 4.92. Systems affected: Exim versions 4.87 to 4.91. For additional information, see MS-ISAC advisory 2019-061 at the InfraGard Portal.

(U) On 11 June 2019, the FBI provided a MS-ISAC cybersecurity advisory titled, "Multiple Vulnerabilities in Adobe ColdFusion Could Allow for Arbitrary Code Execution (APSB19-27)." Adobe ColdFusion is a web application development platform. Successful exploitation of the most severe of these vulnerabilities could result in an attacker executing arbitrary code in the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights. There are no reports of these vulnerabilities being exploited in the wild. Systems affected: ColdFusion 2018 for All versions prior to Update 3; ColdFusion 2016 for All versions prior to Update 10; and ColdFusion 11 for All versions prior to Update 18. For additional information, see MS-ISAC advisory 2019-062 at the InfraGard Portal.

(U) On 11 June 2019, the FBI provided a MS-ISAC cybersecurity advisory titled, "A Vulnerability in Adobe Flash Could Allow for Arbitrary Code Execution (APSB19-30)." Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation this vulnerability could result in an attacker executing arbitrary code in the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights. There are no reports of this vulnerability being exploited in the wild. Systems affected: Adobe Flash Player Desktop Runtime for Windows, macOS and Linux versions prior to 32.0.0.192. For additional information, see MS-ISAC advisory 2019-063 at the InfraGard Portal.

(U) On 11 June 2019, the FBI provided a MS-ISAC cybersecurity advisory titled, "Critical Patches Issued for Microsoft Products, 11 June 2019." Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for code execution. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as

the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. There are currently no reports of these vulnerabilities being exploited in the wild. For additional information, see MS-ISAC advisory 2019-064 at the InfraGard Portal.

(U) On 14 June 2019, the FBI provided a MS-ISAC cybersecurity advisory titled, "A Vulnerability in VLCMedia Player Could Allow for Arbitrary Code Execution." Mozilla Thunderbird is an email client. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. There are currently no reports of these vulnerabilities being exploited in the wild. Systems affected: Mozilla Thunderbird versions prior to 60.7.1. For additional information, see MS-ISAC advisory 2019-065 at the InfraGard Portal.

(U) On 17 June 2019, the FBI provided a MS-ISAC cybersecurity advisory titled, "Multiple Vulnerabilities in Mozilla Thunderbird Could Allow for Arbitrary Code Execution." VLC is a cross-platform multimedia player and framework. Successful exploitation of this vulnerability could allow for arbitrary code execution in the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights. Failed exploitation could result in a denial-of-service condition. There are currently no reports of this vulnerability being exploited in the wild. Systems affected: VLCMedia Player versions prior to 3.0.7. For additional information, see MS-ISAC advisory 2019-066 at the InfraGard Portal.

(U) On 19 June 2019, the FBI provided a Intelligence and National Security Alliance (INSA) Cyber Council Report titled, "The national security challenges of Fifth Generation (5G) Wireless Communication - Winning the Race to 5G, Securely." The expanded capacity of Fifth Generation (5G) wireless communications will support innovative data-intensive applications, many operating under the rubric of the Internet of Things (IoT), ranging from Smart Cities and autonomous vehicles to advanced medical imaging and the widespread use of virtual reality. Once implemented widely, Americans will come to accept the increased productivity, profitability, and quality of life that 5G enables as the new norm. Whichever country comes to dominate 5G infrastructure – through hardware, software, and technical standards – is likely to have enormous economic and commercial advantages across the global economy. For addtional information, see INSA Report at the InfraGard Portal.

(U) On 19 June 2019, the FBI provided a MS-ISAC cybersecurity advisory titled, "A vulnerability in Mozilla Firefox Could Allow for Arbitrary Code Execution." Successful exploitation of the this vulnerability could allow for arbitrary code execution through an exploitable crash. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user

rights. Mozilla is currently aware of targeted attacks in the wild abusing this flaw. Systems affected: Mozilla Firefox versions prior to 67.0.3. For additional information, see MS-ISAC advisory 2019-067 at the InfraGard Portal.

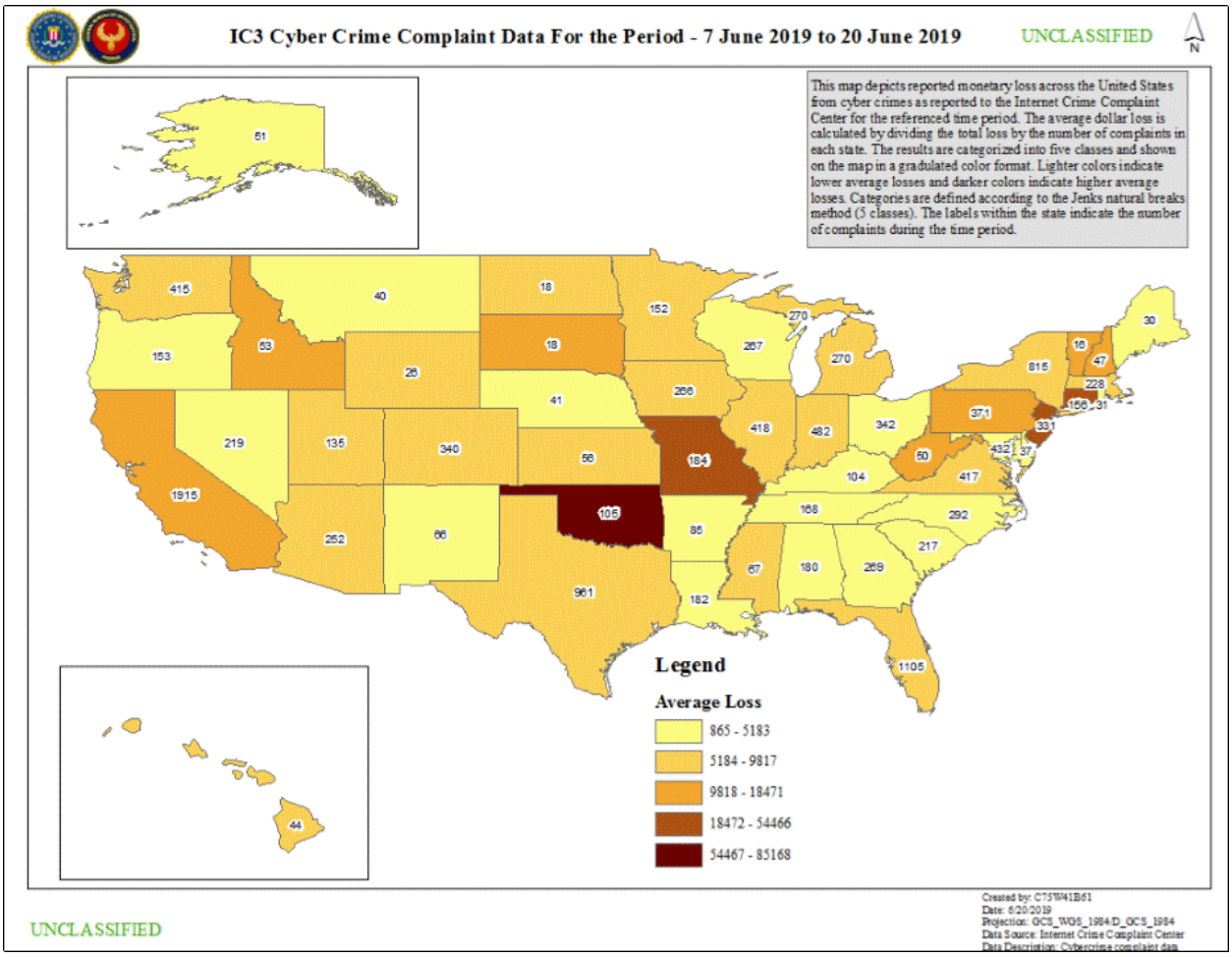
(U) On 20 June 2019, the FBI provided a MS-ISAC cybersecurity advisory titled, "A Vulnerability in Oracle WebLogic Could Allow for Remote Code Execution." Oracle WebLogic is an application server used for building and hosting Java-EE applications. Successful exploitation of this vulnerability could result in remote code execution within the context of the application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. There are reports of this vulnerability being actively exploited in the wild. Systems affected: Oracle WebLogic versions 10.3.6.0.0, 12.1.3.0.0, and 12.2.1.3.0. For additional information, see MS-ISAC advisory 2019-068 at the InfraGard Portal.

(U) CYBER GUARDIAN

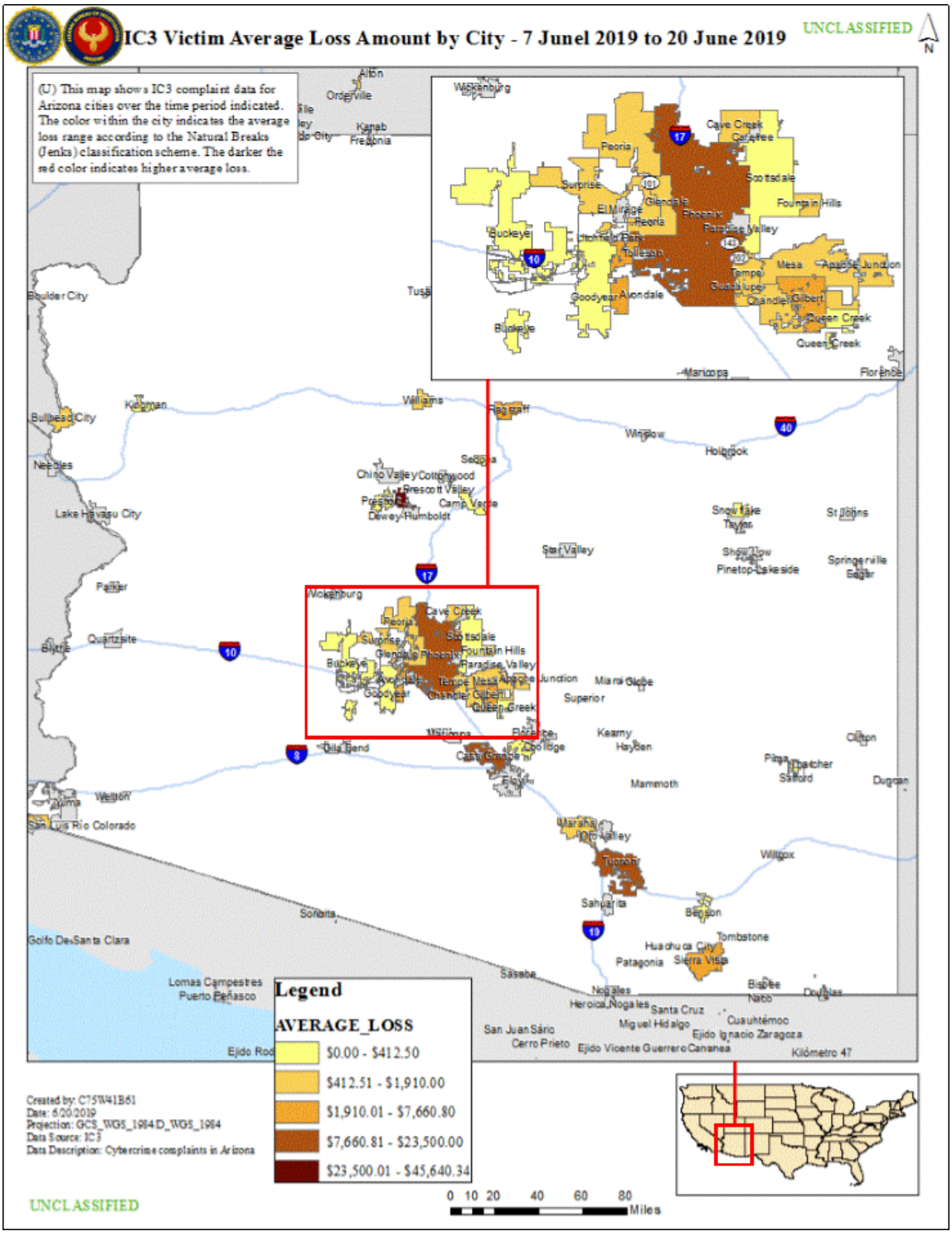
(U//FOUO) A review of Cyber Guardian incidents from 7 June 2019 to 20 June 2019 revealed 123 total incidents nationwide, with four Arizona entities targeted. An Arizona resident had their SnapChat account hacked and taken over for extortion purposes; An employee of a Cleared Contractor was the target of a spoofed email which invited potential recruits to add the employee's email to conduct an interview; The Point-of-Sale (POS) system for a commercial retail business was targeted by the hacking group FIN6 to install Trinity malware to obtain payment card data; and a Cleared Contractor was being targeted by a spoofed email address attemtping to scam the company for unpaid purchases. The sectors targeted were Other - Individual (1); Cleared Contractor (2); and Commerical Facilities - Retail (1). Additionally, attribution for the targeted entities were detailed as Criminal (2); and Unattributed (2).

(U) INTERNET CRIME COMPLAINT CENTER (IC3)

(U) The following information was compiled from statistical data maintained by the FBI IC3 and provides InfraGard and Strategic Partners with comparative data to show how Arizona ranks against the rest of the nation in cyber crime. Upon reviewing the IC3 statistical data for the period 7 June 2019 to 20 June 2019, Arizona ranked 19th in total victim count and 19th in total victim losses when compared against the other states. The following chart depicts the total number of victims and victim losses for the United States.



(U) The following chart depicts the total number of victims and victim losses for the reporting cities in Arizona for the period 7 June 2019 to 20 June 2019.



(U) The following chart compares the United States and the state of Arizona regarding specific types of cyber crimes for the period 7 June 2019 to 20 June 2019.

CRIME TYPE	U.S. VICTIM COUNT	U.S. VICTIM LOSS	AZ VICTIM COUNT	AZ VICTIM LOSS
BEC/EAC	842	$57,210,759.03	16	$683,420.20
Confidence Fraud/Romance	634	$29,059,911.79	10	$499,342.52
Investment	99	$9,060,220.77	2	$600.00
Extortion	1,641	$8,747,140.94	29	$5,143.00
Spoofing	867	$7,083,462.51	20	$350,425.00
Government Impersonation	505	$6,625,498.87	12	$501.00
Real Estate/Rental	550	$5,805,350.76	0	$0.00
Personal Data Breach	1,495	$5,454,956.53	36	$5,484.35
Non-payment/Non-Delivery	2,113	$4,766,963.35	47	$112,791.56
Credit Card Fraud	470	$4,745,640.44	13	$29,240.25
Identity Theft	546	$4,696,631.05	17	$34,436.45
Advanced Fee	514	$3,167,170.87	18	$31,923.78
Social Media	1,189	$2,921,804.51	21	$59,078.43
Virtual Currency	1,025	$2,601,987.01	24	$0.00
Overpayment	654	$2,156,444.54	14	$38,300.57
Phishing/Vishing/Smishing/Pharming	838	$2,077,478.58	18	$5,450.00
Civil Matter	23	$1,902,875.03	0	$0.00
Tech Support	412	$1,654,356.92	24	$5,431.68
Employment	591	$1,644,639.74	13	$22,790.00
Other	274	$926,434.84	4	$414.39
Lottery/Sweepstakes/Inheritance	257	$901,998.09	5	$0.00
Corporate Data Breach	57	$816,592.76	1	$0.00
Harassment/Threats of Violence	686	$680,888.09	24	$2,358.00
Ransomware	73	$594,268.28	1	$0.00
IPR/Copyright and Counterfeit	83	$497,376.36	1	$0.00
Misrepresentation	202	$434,118.95	6	$8,039.44
Health Care Related	11	$136,920.00	0	$0.00
Malware/Scareware/Virus	326	$114,479.96	4	$300.00
Charity	16	$102,793.73	1	$0.00
Re-shipping	40	$65,201.47	2	$0.00
Gambling	4	$16,450.00	0	$0.00
Denial of Service/TDos	40	$8,000.00	1	$0.00
Crimes Against Children	37	$5,816.27	1	$0.00
Terrorism	2	$950.00	6	$2,890.00
No Lead Value	2,147	$600.00	6	$0.00
Total	**19,263**	**$166,686,182.04**	**397**	**$1,898,360.62**

(U) This report has been prepared by the PHOENIX Division of the FBI. Comments and queries may be addressed to the PHOENIX Division at 623-466-1999.

Distribution

ACTIC (Arizona Fusion Center)
FBI Cyber Strategic Partners Phoenix
FBI InfraGard Phoenix
FBI Intranet

FBI Customer Satisfaction Survey

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of our product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance. Please return to:
Federal Bureau of Investigation
PHOENIX DIVISION
21711 N. 7th St.
Phoenix AZ 85024
Fax: 623-466-1770

Customer and Product Information

SIR Tracking ID: SIR-00328362177
Product Title: (U//FOUO) PHOENIX BI-WEEKLY CYBER REPORT FROM 7 JUNE 2019 TO 20 JUNE 2019
Dated: _____
Customer Agency: _____

Relevance to Your Intelligence Needs

1. The product increased my knowledge of an issue or topic. (Check one)
   ___5. Strongly Agree
   ___4. Somewhat Agree
   ___3. Neither Agree or Disagree
   ___2. Somewhat Disagree
   ___1. Strongly Disagree

Actionable Value

2. The product helped me decide on a course of action. (Check one)
   ___5. Strongly Agree
   ___4. Somewhat Agree
   ___3. Neither Agree or Disagree
   ___2. Somewhat Disagree
   ___1. Strongly Disagree

Timeliness Value

3. The product was timely to my needs. (Check one)
   ___5. Strongly Agree
   ___4. Somewhat Agree

___3. Neither Agree or Disagree

___2. Somewhat Disagree

___1. Strongly Disagree

Comments (please use reverse or attach separate page if needed):