SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION
Cyber Alert
PHOENIX DIVISION

Approved for Release: 15 October 2018

SIR Number: SIR-00324139521

(U//FOUO) PHOENIX BI-WEEKLY CYBER REPORT FROM 14 SEPTEMBER 2018 TO 27 SEPTEMBER 2018

SOURCE: (U) A documentary source.

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 14 September 2018 to 27 September 2018. 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) On 14 September 2018, the FBI provided a MS-ISAC computer security advisory titled, "Multiple Vulnerabilities in PHP Could Allow for Arbitrary Code Execution." Successfully exploiting the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the affected application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition. There are currently no reports of these vulnerabilities being exploited in the wild. Systems affected: PHP 7.2 prior to 7.2.10; PHP 7.1 prior to 7.1.22; PHP 7.0 prior to 7.0.32; and PHP 5.6 prior to 5.6.38. For additional information, see MS-ISAC advisory 2018-101 at the InfraGard Portal.

(U) Warning: This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted or analyzed. Receiving agencies are requested not to take action based on this raw reporting without prior coordination with the FBI.

(U) Note: This product reflects the views of the PHOENIX Division.

(U//FOUO) On 18 September 2018, the FBI disseminated a Public Service Announcement (PSA) titled, "Cybercriminals Utilize Social Engineering Techniques to Obtain Employee Credentials to Conduct Payroll Diversion." IC3 has received complaints reporting cybercriminals are targeting the online payroll accounts of employees in a variety of industries. Institutions most affected are education, healthcare, and commercial airway transportation. Cybercriminals target employees through phishing emails designed to capture an employee's login credentials. Once the cybercriminal has obtained an employee's credentials, the credentials are used to access the employee's payroll account in order to change their bank account information. Rules are added by the cybercriminal to the employee's account preventing the employee from receiving alerts regarding direct deposit changes. Direct deposits are then changed and redirected to an account controlled by the cybercriminal, which is often a prepaid card. For additional information, see FBI I-091818-PSA at the InfraGard Portal.

(U) On 18 September 2018, the FBI provided a MS-ISAC computer security advisory titled, "Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution." Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. 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. There are currently no reports of these vulnerabilities being exploited in the wild. Systems affected: Apple Support for iOS versions prior to 2.4. For additional information, see MS-ISAC advisory 2018-102 at the InfraGard Portal.

(U) On 19 September 2018, the FBI provided a MS-ISAC computer security advisory titled, "Multiple Vulnerabilities in Adobe Acrobat and Reader Could Allow for Arbitrary Code Execution (APSB18-34)." Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system. 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: Acrobat DC (Continuous Track) for Windows and macOS version 2018.011.20058 and prior. For additional information, see MS-ISAC advisory 2018-103 at the InfraGard Portal.

(U) On 20 September 2018, the FBI provided a MS-ISAC computer security advisory titled, "Multiple Vulnerabilities in Cisco WebEx Network Recording Player for Advanced Recording Format Files Could Allow for Arbitrary Code Execution." The WebEx meeting service is a hosted multimedia conferencing solution that is managed and maintained by Cisco WebEx. The ARF player is an application that is used to play back and edit ARF recording files. 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 this vulnerability being actively exploited in the wild. Systems affected: Cisco Webex Meetings Suite (WBS32) versions prior to WBS32.15.10. For additional information, see MS-ISAC advisory 2018-104 at the InfraGard Portal.

(U) On 24 September 2018, the FBI provided a MS-ISAC computer security advisory titled, "A Vulnerability in Microsoft Windows JET Database Engine Could Allow for Remote Code Execution." The JET Database Engine provides data access to various applications such as Microsoft Access, Microsoft Visual Basic, and third-party applications. Successful exploitation of

this vulnerability could allow for a remote attacker to execute code in the context of the current process. Depending on the privileges associated with this process, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Processes that 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: Only Windows 7 has been confirmed vulnerable but the exploited component is included in all supported versions of Windows, including server editions. For additional information, see MS-ISAC advisory 2018-105 at the InfraGard Portal.

(U//FOUO) On 26 September 2018, the FBI disseminated a Situational Information Report (SIR) titled, "Indicators of Hidden Cobra Cyber Attack at an Identified Medical Center, as of 14 August 2018." On 14 August 2018, a medical center in El Paso, Texas, experienced several attacks against its firewall, including the following IP addresses associated with the North Korean state-sponsored cyber unit Hidden Cobra: 59.90.93.97, 80.91.118.45, 81.0.213.173, 98.101.211.162, 111.207.78.204, 181.119.19.56, 184.107.209.2 and coinpot.co. Several e-mails successfully bypassed the firewall with executable attachments. The attack raised concerns that malicious cyber actors could attack smaller clinics attached to the targeted medical center and gain access to personally identifiable information. For additional information, see FBI SIR-00323815942 at the InfraGard Portal.

(U//FOUO) On 27 September 2018, the FBI disseminated a PSA titled, "Cyber Actors Increasingly Exploit The Remote Desktop Protocol to Conduct Malicious Activity." Remote administration tools, such as Remote Desktop Protocol (RDP), as an attack vector has been on the rise since mid-late 2016 with the rise of dark markets selling RDP Access. Malicious cyber actors have developed methods of identifying and exploiting vulnerable RDP sessions over the Internet to compromise identities, steal login credentials, and ransom other sensitive information. The Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) recommend businesses and private citizens review and understand what remote accesses their networks allow and take steps to reduce the likelihood of compromise, which may include disabling RDP if it is not needed. For additional information, see FBI I-092718-PSA at the InfraGard Portal.

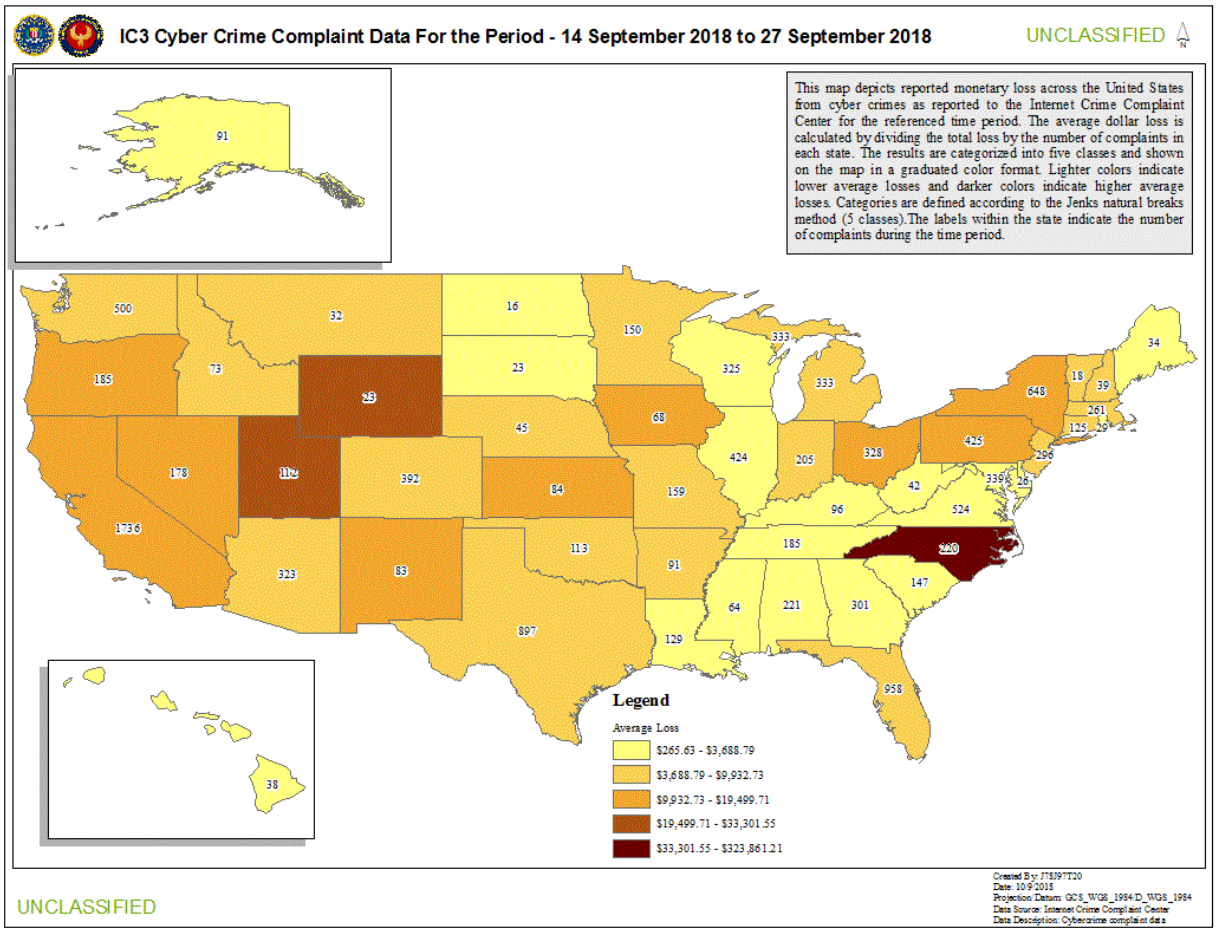
(U) CYBER GUARDIAN

(U//FOUO) A review of Cyber Guardian incidents from 14 September 2018 to 27 September 2018 revealed 92 total incidents nationwide, with two Arizona entities targeted. A government school's student information system was the target of a network intrusion and Personal Identifiable Information (PII) was accessed; and a real estate company was the target of an insider who after being fired stole PII on prospective, current and former employees. The sector targeted was Government Facilities - Education (1) and Commercial Facilities - Real Estate (1). Additionally, attribution for the targeted entity was detailed as Unattributed (1) and Cyber Criminal (1).

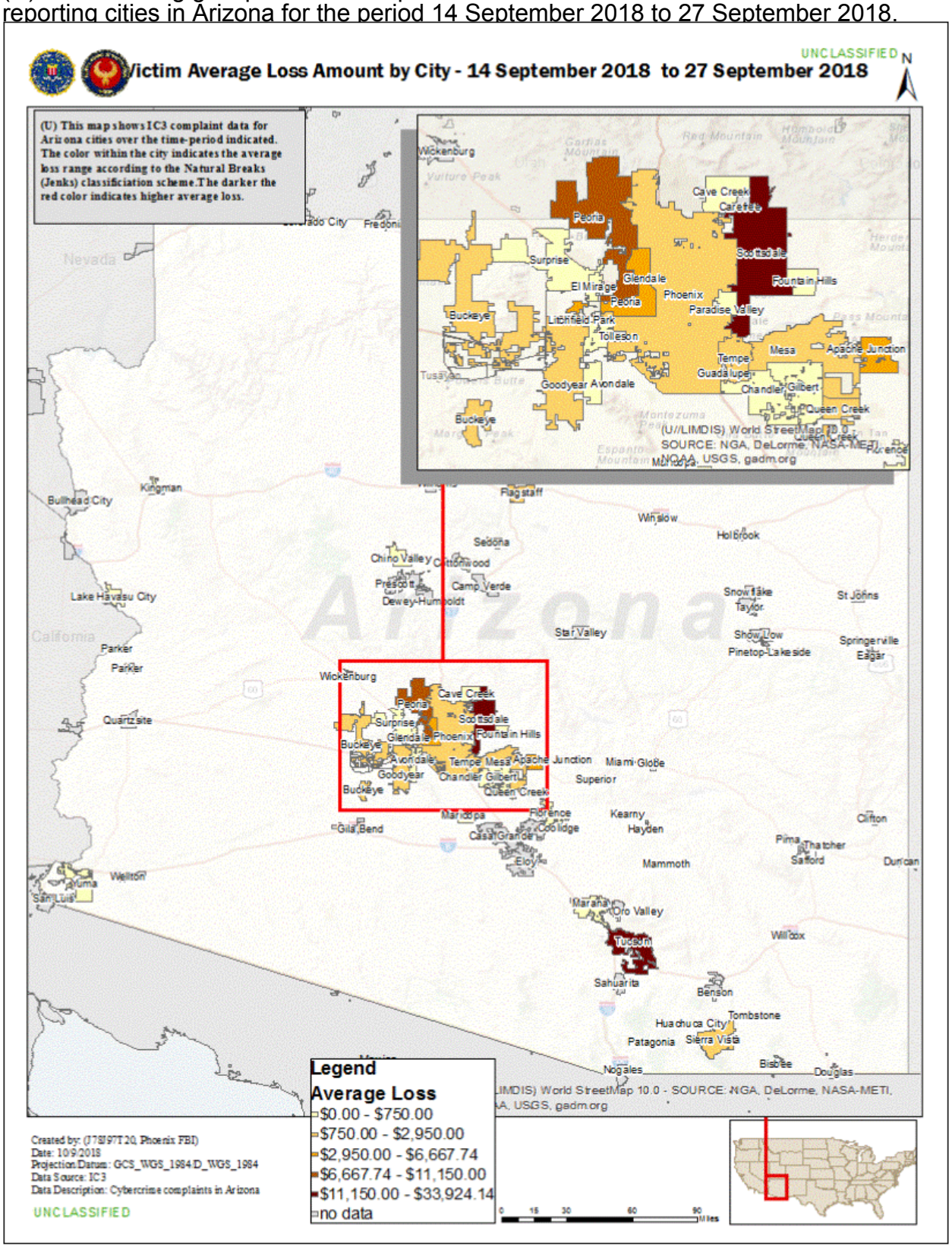
(U) INTERNET CRIME COMPLAINT CENTER (IC3)

(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 14 September 2018 to 27 September 2018, Arizona ranked 14th in total victim count and 14th in

total victim losses when compared against the other states. The following geospatial chart depicts the total number of victims and victim losses for the United States.



(U) The following geospatial chart depicts the total number of victims and victim losses for the reporting cities in Arizona for the period 14 September 2018 to 27 September 2018.



(U) The following chart compares the United States and the state of Arizona regarding specific types of cyber crimes.

CRIME TYPE	U.S. VICTIM COUNT	U.S. VICTIM LOSS	AZ VICTIM COUNT	AZ VICTIM LOSS
Non-payment/Non-Delivery	2,008	$6,241,586.27	41	$119,549.37
Extortion	1,909	$3,685,371.74	54	$13,790.00
Personal Data Breach	1,857	$3,238,851.22	43	$36,425.23
Social Media	1,602	$3,272,454.02	40	$211,666.80
No Lead Value	1,297	$0.00	51	$0.00
Virtual Currency	1,293	$2,291,137.42	33	$38,000.00
Phishing/Vishing/Smishing/Pharming	860	$2,028,646.91	24	$82,469.00
BEC/EAC	856	$41,466,370.91	22	$939,822.41
Harassment/Threats of Violence	679	$608,230.19	24	$0.00
Confidence Fraud/Romance	670	$14,817,232.62	23	$551,922.79
Tech Support	627	$1,158,367.81	15	$7,834.99
Overpayment	589	$1,604,222.39	12	$5,375.00
Spoofing	580	$2,286,574.78	10	$7,300.00
Advanced Fee	561	$2,346,090.65	10	$78,050.00
Credit Card Fraud	529	$9,814,194.24	17	$45,101.41
Employment	519	$1,690,085.50	7	$1,900.02
Identity Theft	497	$2,876,102.66	17	$67,389.42
Government Impersonation	471	$3,849,541.65	9	$6,690.00
Real Estate/Rental	390	$2,558,399.73	9	$3,274.00
Other	290	$2,156,030.30	5	$0.00
Lottery/Sweepstakes/Inheritance	270	$2,946,989.18	7	$67,595.23
Misrepresentation	209	$1,092,197.43	6	$2,722.79
Malware/Scareware/Virus	93	$62,763.63	0	$0.00
Corporate Data Breach	87	$1,893,855.95	4	$0.00
Investment	83	$74,856,303.70	3	$63,500.00
Crimes Against Children	58	$9,816.00	2	$0.00
IPR/Copyright and Counterfeit	58	$65,401.91	4	$0.00
Ransomware	57	$60,774.52	0	$0.00
Charity	30	$16,075.00	2	$0.00
Re-shipping	27	$186,455.70	1	$0.00
Civil Matter	24	$407,833.53	2	$344,300.00
Denial of Service/TDos	18	$60,047.00	0	$0.00
Health Care Related	18	$101,226.55	0	$0.00
Gambling	6	$35,828.47	0	$0.00
Hacktivist	6	$0.00	0	$0.00
Terrorism	1	$0.00	0	$0.00
Total	**19,129**	**$189,785,059.58**	**497**	**$2,694,678.46**

(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-00324139521
Product Title: (U//FOUO) PHOENIX BI-WEEKLY CYBER REPORT FROM 14 SEPTEMBER 2018 TO 27 SEPTEMBER 2018
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):