SOUTHWEST TEXAS FUSION CENTER (SWTFC)

NSCC Collaboration Day:
04/02/20

1300-1400hrs

Presenter:
SWTFC IA: Daniel McKee
SWTFC SPM: Aric Jimenez

(U) Overview

COVID-19 in San Antonio

COVID-19 Calls for Service in San Antonio

Cyber Threats Involving COVID-19

- Including San Antonio-Related Scam/Malware Sites

(U) Enforcement of Public Health Emergency Declaration

Enforcement of Public Health Emergency Declaration

Summary Report

	Total - 3/30/2020 Only					Total - Declaration Period				
	DSD	CCDO	Health	SAPD	Total	DSD	CCDO	Health	SAPD	Total
Number of Calls Received	62	24	28	28	142	403	182	162	233	980
Violations Observed (total locations)	39	13	25	3	80	274	123	139	103	639
Warnings Issued	39	13	25	3	80	274	123	139	103	639
No Violation Observed	23	11	3	25	62	129	59	23	130	341

NOTE: Report summarizes activities related to enforcement of the Fourth Declaration of Public Health Emergency regarding COVID-19 issued on March 18, 2020. Code Enforcement (Development Services Department), Parking Enforcement (Center City Development & Operations), Metropolitan Health District, and San Antonio Police Department have been charged with the enforcement of this declaration. The results in this report include enforcement activities conducted by teams covering 24 hours a day, seven days a week. The Fourth Declaration of Public Health Emergency was effective until 11:59, Tuesday, March 24, 2020. The Fifth Declaration of Public Health Emergency was issued on March 23, 2020 to take effect on March 24, 2020 at 11:59 p.m. and will continue through 11:59 p.m. on April 9, 2020, subject to San Antonio City Council approval.

(U) Calls for Service Referencing COVID-19

- Multiple Chain Businesses experiencing large crowding, lack of social distancing. Results in calls for service, altercations between patrons, higher assaults at these locations

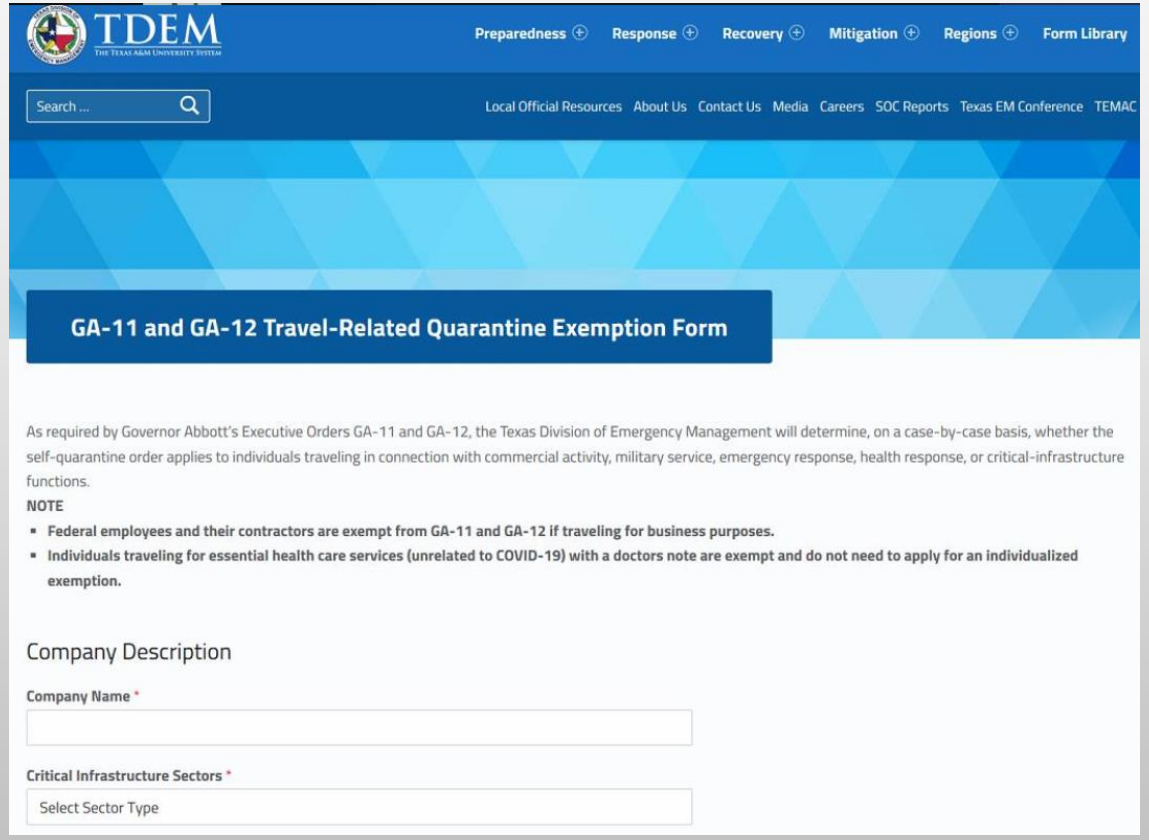
(U) Calls for Service Referencing COVID-19 (cont.)

Small Businesses Still Operating Despite the city ordinance:

- Locally owned diners/restaurants: Taquerias, Asian Restaurants, Seafood Restaurants
- Privately owned gyms
- Flea Markets
- Bars
- Nail Shops

(U) New Travel Restrictions for Gov. Employees

- New travel restrictions requiring approval by the state of Texas for critical infrastructure and government employees or contractors with a need for travel



(U) Calls for Service Referencing COVID-19

SAPD Dispatch Calls for COVID-19 Ordinance Violations by Substation for March 20 – April 1:

SAPD Dispatch Calls for C-Ordinance Viol^ - Most Recent to Oldest Order

20 March - 1 April 2020

PD Responded Call Notes Added - Far Right Column

Substation	Totals
CENTRAL	171
EAST	163
NORTH	267
PRUE	219
SAPD Outside Area	2
SOUTH	225
WEST	257
Grand Total	**1,304**

(U) COVID-19 Indicators of Compromise (IOCs)

- Currently around 24,000+ COVID-19 related characteristics related to malicious cyber activity
  - Includes IP addresses, domain registrations, prior black listing, prior incident history, etc.

- Using the following themes to attract victims:

  Vaccination locations, unemployment benefits, insurance claims, antiviral products for sale, covid19 lawyers, city ordinance covid information

anticovid19supply.com
jacarandascovid.com
uniteagainstcovid19.org
coronavirusmain.com
covid-19chronicles.com
covid19news.work
coronavirussenator.com
privatecovid19testing.com
covid19lawclaim.com
coronavirusleague.com
covid19drycleaners.com
brg-coronavirus-covid.com
coronavirusonlinecounselling.com
coronavirusflowers.com
qqcovid.com
fukcovid19.shop
covid-19pause.com
yourcovid.com
endthecovid19.org
185.104.29.12
covid19maroc.com
lbgadvisorscovid19.com
oraclenovelcoronavirus.com
arcoronavirusbankruptcy.com
covid19cmap.com
coronavirusbankruptcylawyers.com
coronavirusaktuell.com
coronavirusnoticias.online
208.113.181.84
covid19specialdeals.com
cvscovid-19.com
covid19employerliability.com
corona-virus-cases.com

(U) Last 24HRS Domain Registrations

- 2125 newly created suspicious web domains related to covid-19
- 1394 (72%) located in the US, 82 (4.22%) in RU, 69 (3.55%) in DE
- Majority registered with GoDaddy.com (35%, 685), followed by NameCheap Inc. (7.37%, 143)

(U) Malicious San Antonio + Texas Domain Registrations

Element	Type	Element TIC	Threat	T
sanantoniocovid.info	fqdn	31	Newly Registered Domain	
coronavirusprevention sanantonio.com	fqdn	18	Newly Registered Domain	
sanantoniocovid19.com	fqdn	31	Newly Registered Domain	
covid-19preventionsanantonio.com	fqdn	18	Newly Registered Domain	
sanantoniocovid.com	fqdn	31	Newly Registered Domain	
texascovid19attorneys.com	fqdn	25	Newly Registered Domain	
texascoronavirusloans.com	fqdn	27	Newly Registered Domain	
texascoronaviruslawyers.com	fqdn	20	Newly Registered Domain	
texasbackcovid19.com	fqdn	21	Newly Registered Domain	
texascovid19lawyers.com	fqdn	20	Newly Registered Domain	
texascoronavirusdisinfection.com	fqdn	21	Newly Registered Domain	
covid19intexas.com	fqdn	26	Newly Registered Domain	
coronavirusintexas.org	fqdn	19	Newly Registered Domain	
covid19testingtexas.com	fqdn	23	Newly Registered Domain	
texascoronaviruslawyer.com	fqdn	20	Newly Registered Domain	
coronavirusinformationcenteroftexas.com				

(U) Ex. sanantoniocovid.info

Analysis Report

ID	af3bce6ad5222b79c784420aeaa70d42	Filename	cd1b1a6ab5752316dd8ea2444ba52a4f.html
OS	Windows 7 64-bit	Magic Type	HTML document, ASCII text, with no line terminators
Started	3/31/20 16:36:14	File Type	html
Ended	3/31/20 16:42:15	SHA256	888fb3e2a0e046c88bc2dcfa679e6801e9a7a21429ae67c6e2feaf0edca84d31
Duration	0:06:01	SHA1	4d528ae8b6e0e270057cd62841c5442778ec669c
Sandbox	mtv-work-061 (pilot-d)	MD5	d58ea04ed74044f81c7ef4e1b93eeb70

Behavioral Indicators

Submitted HTML Minimal Code With Redirect	Severity: 70	Confidence: 90
HTML File Uses Redirect By Refresh	Severity: 60	Confidence: 90
HTML Contains Only Redirection Code	Severity: 55	Confidence: 95
Static Analysis Flagged Artifact As Anomalous	Severity: 60	Confidence: 80

```
PING sanantoniocovid.info (184.168.221.50) 56(84) bytes of data.
64 bytes from ip-184-168-221-50.ip.secureserver.net (184.168.221.50)
64 bytes from ip-184-168-221-50.ip.secureserver.net (184.168.221.50)
64 bytes from ip-184-168-221-50.ip.secureserver.net (184.168.221.50)
64 bytes from ip-184-168-221-50.ip.secureserver.net (184.168.221.50)
64 bytes from ip-184-168-221-50.ip.secureserver.net (184.168.221.50)
^C
--- sanantoniocovid.info ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
```

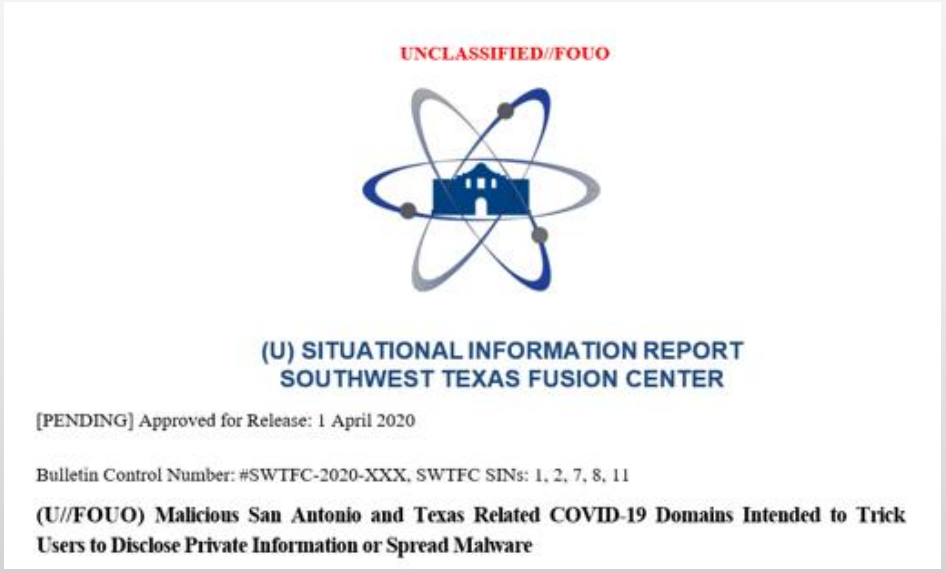
Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2010-1899	Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability."
CVE-2010-2730	Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability."
CVE-2010-3972	Heap-based buffer overflow in the TELNET_STREAM_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information.
CVE-2012-2531	Microsoft Internet Information Services (IIS) 7.5 uses weak permissions for the Operational log, which allows local users to discover credentials by reading this file, aka "Password Disclosure Vulnerability."
CVE-2012-2532	Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) processes unspecified commands before TLS is enabled for a session, which allows remote attackers to obtain sensitive information by reading the replies to these commands, aka "FTP Command Injection Vulnerability."
CVE-2010-1256	Unspecified vulnerability in Microsoft IIS 6.0, 7.0, and 7.5, when Extended Protection for Authentication is enabled, allows remote authenticated users to execute arbitrary code via unknown vectors related to "token checking" that trigger memory corruption, aka "IIS Authentication Memory Corruption Vulnerability."

(U) SWTFC Situational Information Report

- Discusses San Antonio-related IOCs
- Trends of links being spread via text messages, email, and social media
- Must work for recognized government entity with a need to know to be placed on distribution list



UNCLASSIFIED//FOUO

(U) SITUATIONAL INFORMATION REPORT
SOUTHWEST TEXAS FUSION CENTER

[PENDING] Approved for Release: 1 April 2020

Bulletin Control Number: #SWTFC-2020-XXX, SWTFC SINs: 1, 2, 7, 8, 11

(U//FOUO) Malicious San Antonio and Texas Related COVID-19 Domains Intended to Trick Users to Disclose Private Information or Spread Malware

(U) SWTFC Weekly Threat Brief

- Summary of suspicious activity reporting within the San Antonio Region
- Includes significant threats related to national narratives (COVID-19)
- Also includes relevant Cyber Threats related to COVID-19 in last release
- Must work for recognized government entity to be placed on distribution list

(U) SWTFC Judgements

- Main takeaways:
  - San Antonio still experiencing non-compliance in San Antonio by smaller businesses within the West, South and North sides of town
  - San Antonio Law Enforcement may get legal authority to penalize ordinance violations via citations, removal of patrons, etc.
  - Many newly registered sites are not malicious yet, but are predicted to be operational soon
  - More San Antonio and Texas related COVID scam sites expected to go up as infections and public fear increase in Texas
  - Majority of scam sites focused on financial motivation or misinformation