



# Testimony to the Senate Industry, Business and Labor Committee on HB 1314

© Gerald Blank

[www.jerryblank.us](http://www.jerryblank.us)

Kevin Ford – Chief Information Security Officer NDIT  
3/08/2021

NORTH  
**Dakota**  
Be Legendary.™



# The Threat is Huge

North Dakota receives over **2.1 Billion detected attacks per year**<sup>1</sup> from external threats including:

- Nation States,
  - China,
  - Russia,
  - Iran, &
  - North Korea;
- Corporate Espionage, and;
- Organized Crime Syndicates.

1. Based on ¼ Sampling of 2020 Firewall logs from June 2020, August 2020, October 2020, and Last 30 days (as of December 20, 2020)



# We Have Low Visibility Around Security Events

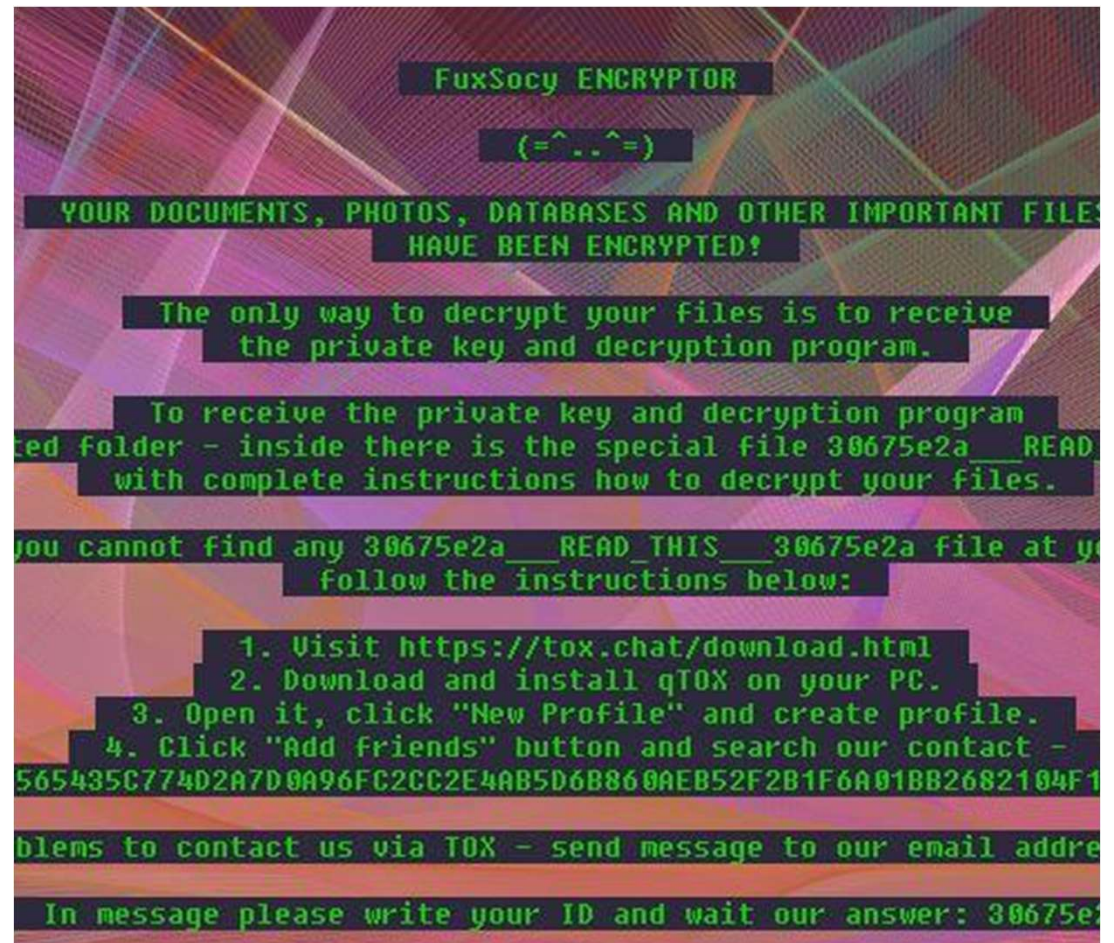
We see traffic associated with security events on STAGENet but can't attribute them

- No coordination
- No requests to centrally block
- No protection for network "neighbors"

FIRST SEEN	WILDFIRE VERDICT	SHA256	FILE SIZE (BYTES)	FILE TYPE	TAGS
01/29/2021 8:15:38am	Malware	53972df62b7d1e2640cda96981728292408f8f75c9a978eb34cf8c4262f1643	1,019,392	PE	ProcessInjection
01/29/2021 2:59:59am	Malware	f2731ba50c5293b82a919e930988459e99ee60ce1b0d71c4e4062c0b9cf5d279	1,112,064	PE	IPAddressLookup, ProcessInjection, UsesDynamicDNS
01/28/2021 4:46:06pm	Malware	548793c58adcbdf8b0dc9c0c1a5f433d049909df81f5e5de659b0d89f55a50d	1,053,184	PE	AccessesWindowsVaultPasswords, ProcessInjection
01/28/2021 11:48:40am	Malware	5859339c78607a62a4a7556ecb1c155c67d4e7c23af87a9a708a2e07f10da646	88,443	PDF	GenericPhishingDocs
01/27/2021 9:18:28am	Malware	b13b959632bf32aebf8d1b1106d6bf35afb374c7bfeff2aa3fa5b7d20593b3f1f	59,674	Microsoft Excel Document	
01/27/2021 1:41:24am	Malware	bd0a70575336c7c295d763de9b56f4c7f4e5a8ccccf7dc65798fcd0ab71d129d0	59,157	Microsoft Excel Document	
01/27/2021 1:21:35am	Malware	7da580ba488cb0e0edff56217e34e745a2a6723f32819a0de41b2cf63533a0b	395,302	PDF	
01/26/2021 11:18:18pm	Malware	b9ece958582c9cd5ee96f523167da22f54e6acde01fc08202944c7723f572b8	516,960	RAR Archive	
01/26/2021 6:42:26pm	Malware	004b9a0f1989dc7150b922620623a8c3a625004b39fa3057f33b07054a981926	463,194	RAR Archive	
01/26/2021 5:39:47pm	Malware	5ad47b104936310fa504040e7f9f262b40d6bcd28396bf803f14ff4f035c163	28,334	RAR Archive	IPAddressLookup, ProcessInjection
01/26/2021 11:45:42am	Malware	1fd406033789aa59b4efbfb061e39e44a0cbe55319589f72535791a6d1016a	156,704	Microsoft Excel 97 - 2003 Document	
01/26/2021 11:20:41am	Malware	5a4c36eb074f626d6b8464037097c77628c0fa67d5440dcf98d80c771d354a	156,714	Microsoft Excel 97 - 2003 Document	
01/26/2021 11:13:51am	Malware	2035598bef0e7bec000870d4c0b071c023df326c77ab271e409a1049644d22	156,704	Microsoft Excel 97 - 2003 Document	
01/26/2021 11:08:56am	Malware	b65c0fdcc16a5e25b788672c1258d213ca59e6b4eaa24a119cffe69ce471a89	156,704	Microsoft Excel 97 - 2003 Document	
01/26/2021 10:04:48am	Malware	0aa69997ae763732534917d2ed66c84d3c604aa5f7f43b5da5104a6006ef716	9,467,392	PE	
01/26/2021 9:45:49am	Malware	83461a9b9979c908622f5ddad3e8aa03eabcfa5065697e7d722db0accfc0bfb	156,704	Microsoft Excel 97 - 2003 Document	

# We Have Little Information to Provide

“Presentation by representatives of the Information Technology Department (ITD) regarding North Dakota's cybersecurity status, including[...] a list of North Dakota state and local government ransomware attacks known to the public.” - LITC Agenda 3/13/2020



# HB 1314 - How it Works

HB 1314 will improve oversight and coordination of the state network by:

- Increases central visibility of cybersecurity events on the state network;
- Provides central network coordination to remediate impacted entity; and
- Stops the spread of cybersecurity events to other entities.

STAGENet  
Entity

- Identifies initial event
- Reports event information to ITD on ongoing basis
- Requests state cooperation as required

ITD

- Coordinate w/ Entity to provide needed service
- Establishes and maintains secure communications
- Provides report to Legislative management

Legislative  
Management

- Receives reports
- Has increased awareness of STAGENet security