

DIR Network Security Operations Center Overview/ 2016 NSOC Annual Threat Report

April 12th, 2017



Agenda

- Intro
- NSOC background
- People
- Technology (Tools, Services)
- Process
- 2016 Threat Report
- Contact Info
- Heat Map
- Panel Discussion



SUBCHAPTER C. NETWORK SECURITY CENTER

Sec. 2059.101. NETWORK SECURITY CENTER. The department shall establish a network security center to provide network security services to state agencies.

- NSOC was authorized by the Texas Legislature in 2007

- Texas Government Code 2059 – DIR will provide perimeter security
- DIR is the Internet Service Provider (ISP) for its internet customers
 - Maintain Internet availability for customers 24X7X365
 - Uptime is crucial therefore the NSOC provides DDoS monitoring and mitigation to its customers through its' ISPs
- High Volume....Everything is bigger in Texas!
 - Blocking in excess of 3 billion unauthorized or malicious communication attempts against our shared network per month! 4 billion in March
 - Protecting over 2.8 million public facing IP addresses
 - 25TB of data each day passes through our security tools
- As the Internet Service Provider (ISP) and without endpoints we have limitations on how aggressive our security posture may be
 - Customers own their data and have ISOs/CISOs that manage their risk

- SOC is staffed with high quality security professionals
 - This includes leaders and highly trained engineers and analysts that can respond appropriately to the threats facing the NSOC
 - We can make large investments in tools but if the Security Team is not enabled to perform their job duties either through a failure in process or governance then the program will not be successful
- Current Staff expertise includes:
 - Network Security architect
 - Senior Analysts
 - Security Engineers
 - IT Governance
 - Ethical Hackers
 - Project Management

Panel Discussion Members

Moderator:

Jeremy Wilson, CISSP, CISM, Security+

-DIR NSOC Security Manager

Panel Members:

Joe Poole, CISSP

-DIR Lead Security Analyst DIR

Mac Cole, MSCIS, CISSP, CEH

- DIR Security Analyst

Dan Lyons, CCNA, CCNA: Security, CCNP:SITCS

- Senior Security Analyst – AT&T

Juan Reyes, MSCIS, CISSP, CISA, CISM, GCIH, GCIA

- Senior Security Analyst – AT&T

Richard Overfield, CISSP-ISSEP, CISA, MBA

-NSOC Operations Director – AT&T

Security Operation Center (SOC): The benefit of running multiple tools is that they all have strengths and weaknesses and some are better at catching certain types of events. Having multiple tools and partners watching similar traffic from different perspectives has enabled us to provide better protection and alerting to our customers

- Intrusion Prevention System (IPS)
- Network Forensics Tool (NFT)
- Malware detection System (MDS)
- Intrusion Detection System (IDS) open source

- **Intrusion Detection System (IDS) Albert** -is an IDS monitoring service that is being provided to the NSOC at no cost through an Inter-Agency Agreement with the Multi-State Information Sharing and Analysis Center (MS-ISAC)
- **Intrusion Detection System (IDS) Panopticon** is a low cost IDS service that is being provided to the NSOC through an Inter-Agency agreement with the University of Texas
- **DDOS 24X7 monitoring and mitigation service**
 - Being provided by DIR's Internet Service Providers (AT&T, Century Link)
 - 150mb threshold on 10gbps pipes although smaller events can be mitigated
 - DDOS service is bandwidth focused not resource exhaustion focused

- Aggressive blocking
 - We have taken an aggressive blocking stance
 - We block any known bad IPs or domains
 - We block IPs we catch scanning or attempting brute force logins
- Monitor outbound traffic
 - Last layer of protection
 - Watching for call-outs and beaconing
 - Unusual connections
- Alerting the agencies to suspicious activity
 - Send the alert with a summary of the suspicious activity, evidence, research, and remediation to the affected agency and
 - All Indicators Of Compromise (IOCs) are added to our statewide GRC tool for incident tracking purposes

Alerting Process

- Analysts review data from IPS, IDS, NFT, MDS outside parties etc.
- They gather collaborating evidence of the suspected malicious activity from the other tools
- They send the agency security team an alert via email and GRC Archer
 - Summary of the suspected malicious behavior
 - The believed culprit or malware variant
 - Indicators of compromise are identified
 - Console screenshots and/or tool logs as evidence of the traffic
 - Information/Research links on that malware
 - Recommended remediation procedures for that malware

- Information Sharing, DIR actively participates in cyber security information sharing with:
 - FBI
 - US Cert
 - MS-ISAC
 - DIR Vendor partners
 - NSOC Security Tools
 - Security Industry researchers
 - Our Customers
- This Cyber intelligence is added back into our tools to better protect our customers and our networks

2016 NSOC Threat Report

- DIR NSOC is providing it's 3rd Annual NSOC Threat report
- Part of an ongoing effort to increase our communications and to provide an update on the security activity NSOC has seen over the past year.
- The Report discusses current security posture of the state's shared network and threats we have observed in 2016
- Report provides additional details about lessons learned, vendor research, trends, and some emerging threats in our shared environment.
- How to get it? DIR website, or take a copy today....

2016 NSOC Threat Report/What's in it?

2016 Threat Report
Network Security Operations Center

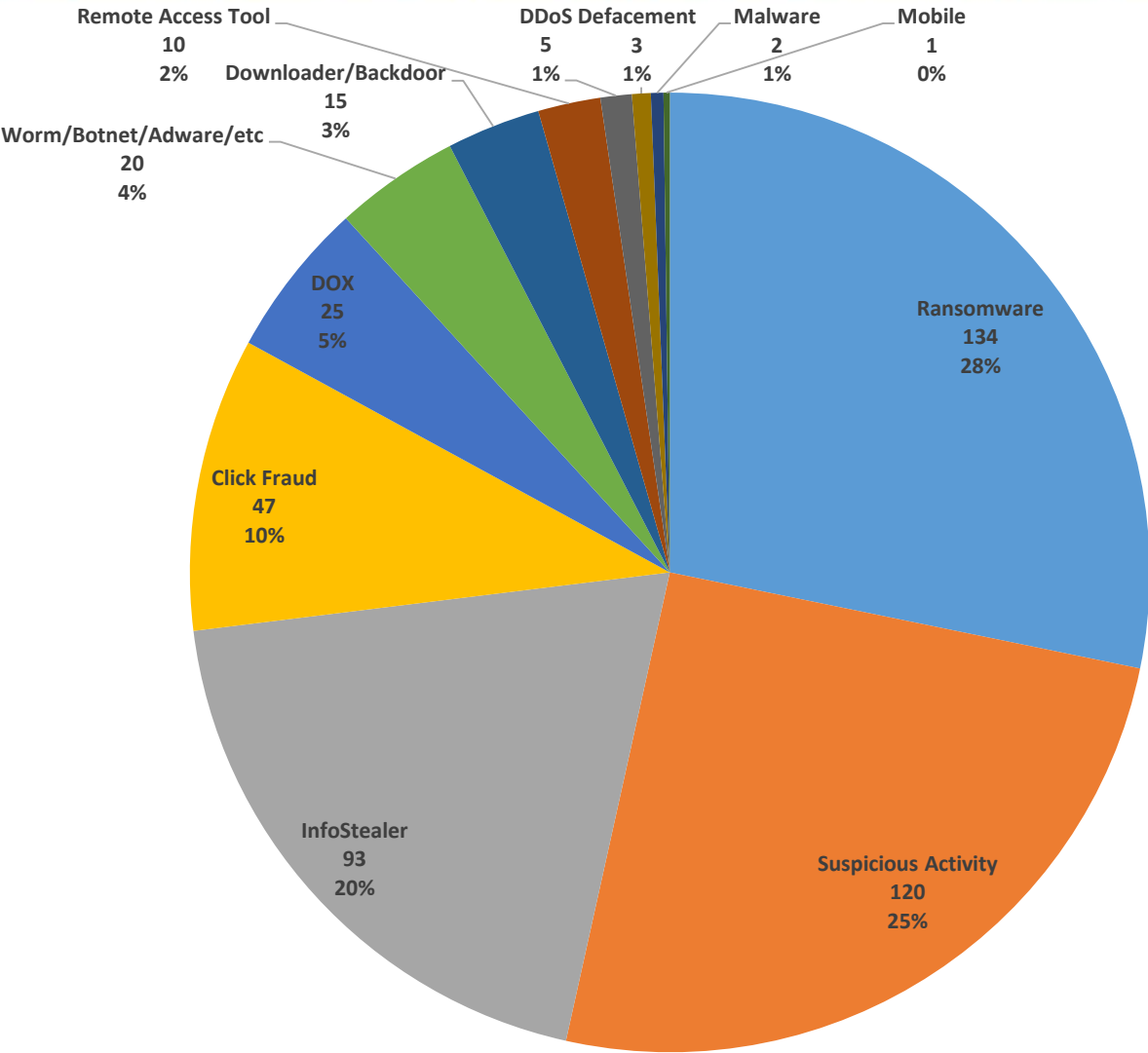


Texas Department of Information Resources

Contents

1. A Letter from the Executive Director.....	1
2. Introduction by Mac Cole and Jeremy Wilson.....	2
3. Hacktivism and DDoS for Hire.....	4
4. Phishing: The Attack Vector of Choice.....	6
5. Spear Phishing – Avoid the Harpoon.....	8
6. TOR and You: The Basics.....	10
7. A Scanner So Darkly.....	12
8. Conclusion.....	14
9. Contributors.....	15

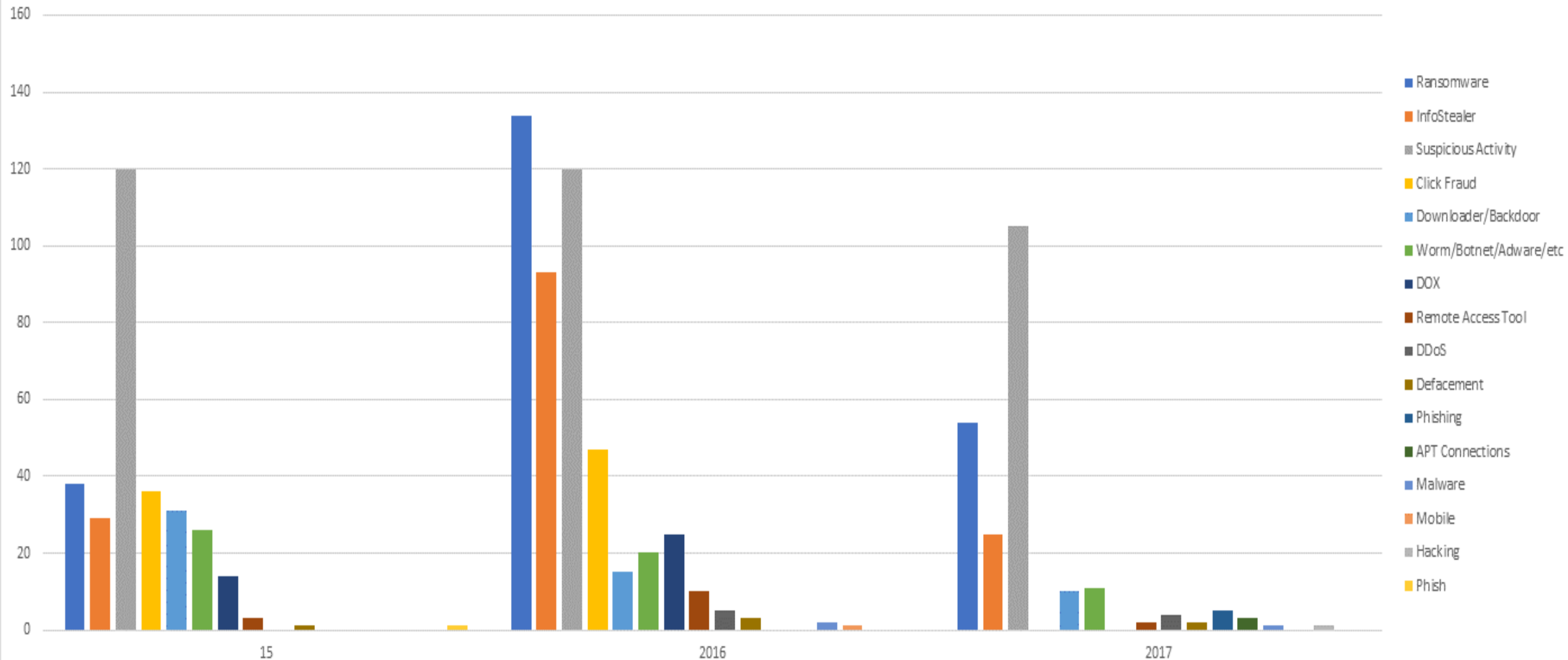
NSOC Alerts FY-2016



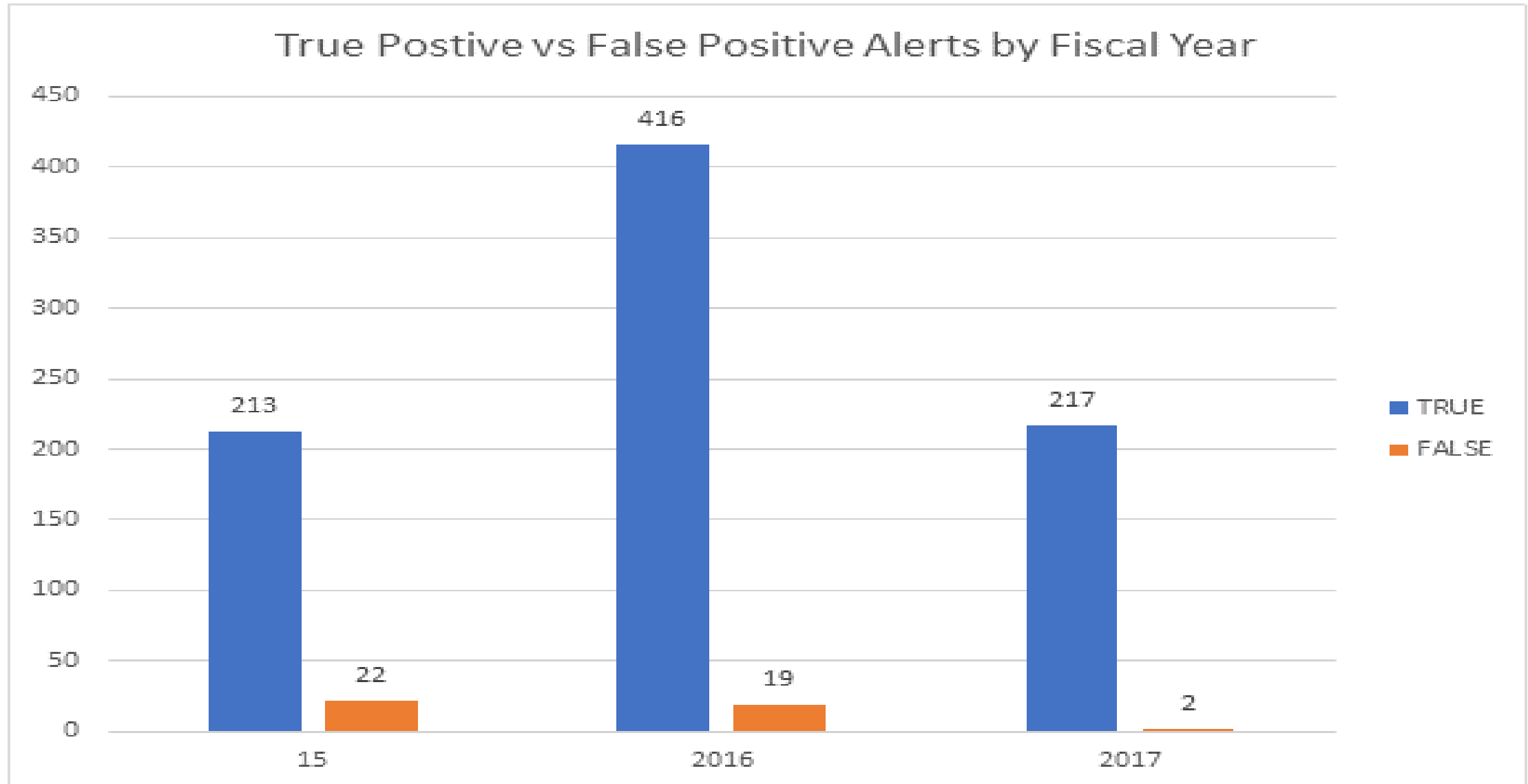
FY	2016
month	(All)
Row Labels	Count NSOC AI
Ransomware	134
Suspicious Activity	120
InfoStealer	93
Click Fraud	47
DOX	25
Worm/Botnet/Adware/etc	20
Downloader/Backdoor	15
Remote Access Tool	10
DDoS	5
Defacement	3
Malware	2
Mobile	1
Grand Total	475

NSOC Alerts by FY

Alerts by Threat Category by Fiscal Year



True False Positive Rate



NSOC Contact Information

- Who ya gonna call?....NSOC!
- 24x7 NSOC On call
 - 888-839-6762
 - Option 1 network
 - Option 2 Security
- Security-alerts@dir.texas.gov
 - Goes to the entire NSOC security team if you have questions or need support
- Jeremy Wilson – NSOC Security Manager
512-475-0602 jeremy.wilson@dir.texas.gov