In the Cross-Hairs:
Protecting the Public’s Data

Public Sector Threat Brief - Q3 2023
Matt Singleton, CrowdStrike
MATT SINGLETON
Executive Strategist

- **25+ years**: Innovating at the intersection of security, education & digital transformation
- **State Government**: Former Chief Information Security Officer for the State of Oklahoma; Chief Operations Officer for the state’s IT division; State Chief Information Officer for Education
- **Higher Education**: Developed cybersecurity strategy and program for the University of Oklahoma system; Led innovation arm of OU IT; Professor of Cybersecurity
- **Education**: M.PS. - Applied Intelligence, specializing in Cyber Intel, Homeland Security & Counterterrorism from Georgetown University; B.A. - Administrative Leadership from the University Of Oklahoma
- **Thought Leadership**: Momentum, National Association of State Technology Directors; Hunt, Bourne and Ryan are Amateurs, Threatday
AGENDA

The Global Threat Landscape
Public Sector Specific Threats
The Way Forward
GLOBAL THREAT LANDSCAPE

- Volume/Speed/Sophistication of Attacks
- Adversaries
- Top Current Threats
  - Third-Party Software
  - Cloud Exploitation
  - Access Brokers/Identity
THREE PRIMARY METRICS FOR MEASURING THE ADVERSARY

Volume

Speed

Sophistication
CROWDSTRIKE DISTINCT & SOPHISTICATED INTRUSION TELEMETRY

Two-Year Timespan – 300% increase

Less than two-year Timespan – 500% increase

Volume
Speed
Sophistication


Nation-State  Unassigned  eCrime
Every Second Counts

Adversaries are getting faster, defenders must accelerate

Breakout time has dropped from 9 hours and 42 min in 2018 to only 79 min in 2023
THE NECESSITY OF SPEED
Survival of the Fastest

TO STAY AHEAD YOU MUST:

DETECT IN: 1 min
INVESTIGATE IN: 10 min
RESPOND IN: 60 min

BREAKOUT TIME

MITRE ATT&CK PHASE
Complexity: Malware versus Malware-Free Attacks

29% Malware Threat Sophistication - Non-Malware Attacks

YOU NEED COMPLETE BREACH PREVENTION

71% Malware-Free

https://www.crowdstrike.com/resources/reports/overwatch-threat-hunting-report/
ACCELERATING THREAT LANDSCAPE

1990

THE FIRST THREATS

2000

EVOLUTION OF
CAPABILITIES

2010

MATURING CYBER
THREAT ECOSYSTEM

2020

THE MODERN ATTACK

OPPORTUNISTIC
THREATS

ATTACK VOLUME
AND VELOCITY

VIRUSES
TROJANS
DDOS
PHISHING

AUTOMATED
THREATS

INDIVIDUAL
RANSOMWARE

HYBRID
THREATS

ATTACK
TOOLKITS

UBIQUITOUS
TARGETED THREATS

SUPPLY
CHAIN
THREATS

THREATS AS
A SERVICE

BIG GAME
HUNTING

CLOUD
THREATS

ACCESS
BROKERS
ADVERSARIES TRACKED BY CROWDSTRIKE

CRIMINAL
Cryptonym: Spider
Motive: Financial gain
Method: Fraud, data theft, extortion, etc.

STATE-SPONSORED
Cryptonym: Panda, Bear, Kitten, Chollima...
Motive: Geopolitical or financial gain
Method: disruption, espionage, or manipulation

HACKTIVIST / TERRORIST
Cryptonym: Jackal
Motive: Attention
Method: disruption or disclosure
Cloud exploitation is on the rise

95% increase in cloud exploitation

3x increase in cases involving cloud-conscious adversaries

Adversaries sharpening cloud TTPs

- **COZY BEAR**: uses malicious tools to modify cloud services
- **SCATTERED SPIDER**: deployed ransomware from a cloud staging env.
- **LABYRINTH CHOLLIMA**: uses cloud resources to deliver documents with malicious macros
- **COSMIC WOLF**: Targets victim data stored within cloud environments

Identity is a key cloud access point

Valid accounts are used to gain initial access in 43% of cloud-based intrusions.

In 67% of cloud security instances, roles have elevated privileges beyond what was required.
A Growing Threat: Insecure Configurations

Human error drives cloud risk

99%
Of cloud security failures are the customer’s fault - Gartner

60%
of workloads lack properly configured security protections

28%
of workloads run as root or allow escalating to root

26%
of workloads have Kubernetes Service Account Token automounted

24%
of workloads have root-like capabilities
IDENTITY IS A PRIMARY ACCESS MECHANISM FOR THE ADVERSARY

80% of data breaches have a connection to compromised privileged credentials - Forrester Research

Breaches from stolen/compromised credentials took the longest to detect:

250 days - Cost of a Breach Report, 2021
Access Broker Boom

Acceleration of demand
Population of services increasing with more than 2,500 advertisements – a 112% increase from 2021

Buy a la carte or in bulk
Several brokers will sell in bulk as others will use a “one-access, one-auction” technique.

Access methods remain consistent
Abuse of compromised credentials obtained by information stealers or purchased in log shops on the dark web

80% of all breaches use compromised identities and 50% of organizations have experienced an Active Directory (AD) attack in the last two years.
DARK WEB ADVERTISEMENT

Northeastern State University

Northeastern State University is a public university with its main campus in Tahlequah, Oklahoma.

Get ready for a week-long online auction extravaganza! With just 7 days on the clock, seize the opportunity to bid on exclusive, unique and impressive data. Let the thrill of timed bidding ignite your competitive spirit! Leave your email, price and interested item, we will contact you soon.

email, necessary data, your price

ObMuOWqVi

Captcha

Send

Northeastern State University is a public university with its main campus in Tahlequah, Oklahoma. The university also has two other campuses in Muskogee and Broken Arrow as well as online. Northeastern is the oldest institution of higher learning in the state of Oklahoma as well as one of the oldest institutions of higher learning west of the Mississippi River. Tahlequah is home to the capital of the Cherokee Nation of Oklahoma and about 25 percent of the students at NSU identify themselves as American Indian. The university has many courses focused on Native American linguistics, and offers Cherokee language Education as a major. Cherokee can be studied as a second language, and some classes are taught in Cherokee for first language speakers as well.
PUBLIC SECTOR SPECIFIC THREATS

- Why Public Sector?
- The Growing Cyber Threat
- Denial of Service
- Ransomware & Data Extortion
- Third-Party Tools
WHY PUBLIC SECTOR?

- Large user base
- Public Safety implications
- Diverse end points
- High-profile
- Numerous stakeholders
- Federated IT/Cybersecurity models
- Under-resourced
PUBLIC SECTOR - ADVERSARY MOTIVATIONS

Nation State

eCrime

Hacktivist

14
17
4
PUBLIC SECTOR - NATION STATE TRENDS

CHINA

DPRK (North Korea)

RUSSIA

IRAN

3 3 4 4
POTENTIAL DISRUPTIVE IMPACTS

TARGET: OPERATIONAL TECHNOLOGY
INDUSTRY-SPECIFIC TOOLS

TARGET: PHYSICAL SAFETY/SECURITY SYSTEMS

TARGET: PERSONALY IDENTIFIABLE INFORMATION (PII)

TARGET: MISSION CRITICAL APPLICATIONS

TARGET: MISSION CRITICAL RESOURCES

TARGET: WEAPONIZABLE RESOURCES

TARGET: INTELLECTUAL PROPERTY
CURRENT TREND: RANSOMWARE + DATA EXTORTION

Data extortion forces you to choose between the consequences of data leaks or the consequences of ransomware.

**RECONNAISSANCE**
Targeting domain controllers and valuable data

**EXFILTRATION**
Sensitive data moved to adversary controlled storage

**RANSOMWARE**
Deployed enterprise-wide (endpoints, network drives, shares, etc.)

**EXTORTION**
When ransom deadline expires, actor threatens to release data

**CONSEQUENCES**
Refusal to pay ransom leads actor to fulfill their promise
THE WAY FORWARD

- Where We Need to Be
- CrowdStrike Recommendations
- Call to Action
WHERE WE NEED TO BE

- Dedicated 24 x 7 coverage to Prevent, Predict, Detect, Respond
- Complete visibility of our environment and risks
- Complementing state-provided security controls
- Reduced risk and increased productivity
CrowdStrike Recommendations

- Join the MS-ISAC.
- Leverage free MS-ISAC services.*
- Engage in regional ISACs/ISAOs.
- Work with state organizations on the SLCGP.
- Participate in Whole-of-State strategies.
- Engage CrowdStrike RSM.
  - Conduct a free AD Assessment.
  - Conduct a free Cloud Security Assessment.

*https://www.cisecurity.org/ms-isac/services