Stranger Threats: Navigating the Upside Down of Higher Ed Cyber Threats

Higher Education 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.P.S. - 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
Higher Ed Specific Threats
The Way Forward
GLOBAL THREAT LANDSCAPE

- Volume/Speed/Sophistication of Attacks
- Adversaries
- Top Current Threats
- Access Brokers
THREE PRIMARY METRICS FOR MEASURING THE ADVERSARY

Volume  Speed  Sophistication
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

MITRE ATT&CK PHASE
Every Second Counts

Adversaries are getting faster, defenders must accelerate

eCrime Breakout Time
79 min

Breakout time has dropped from 9 hours and 42 min in 2018 to only 79 min in 2023
Complexity: Malware versus Malware-Free Attacks

YOU NEED COMPLETE BREACH PREVENTION

MALWARE
29%

MALWARE-FREE
71%

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

OPPORTUNISTIC THREATS

ATTACK VOLUME AND VELOCITY

VIRUSES
TROJANS
WORMS
BOTNETS
DDOS
APTS
PHISHING

AUTOMATED THREATS

1990
THE FIRST THREATS
2000
EVOLUTION OF CAPABILITIES
2010
MATURING CYBER THREAT ECOSYSTEM
2020
THE MODERN ATTACK

UBIQUITOUS TARGETED THREATS

HYBRID THREATS
THREATS AS A SERVICE
BIG GAME HUNTING
ATTACK TOOLKITS
CLOUD THREATS
INDIVIDUAL RANSOMWARE
ACCESS BROKERS
SUPPLY CHAIN THREATS
ADVERSARIES TRACKED BY CROWDSTRIKE

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

HACKTIVIST / TERRORIST
Cryptonym: Jackal
Motive: Attention
Method: disruption or disclosure

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

Access operations
How Adversaries gain access
- VALID CREDENTIALS
- SUPPLY CHAIN
- COMPROMISE
- O-DAY EXPLOITATION
- MFA BYPASS

Post Exploitation
How Adversaries remain stealthy
- RECONNAISSANCE
- LATERAL MOVEMENT
- PRIVILEGE ESCALATION

Impact
How the Adversary achieves their objective
- RANSOMWARE
- DATA LEAK
- DATA EXTORTION
- DATA EXFILTRATION
China-nexus adversaries significantly increased 2022 operational scale

Exploits to gain initial access
China-Nexus Adversaries continued shifting toward exploitation of web-facing services

Increase in use of zero-day exploits
Enterprise software continued to be a high-priority target. Additional zero-day exploits include weaponized MSFT Office documents.

Zero-day exploits were most commonly observed in intrusions targeting North American organizations in 2022; China-nexus adversaries used zero-day exploits to compromise entities in the aerospace, legal and academic sectors.

China-nexus adversaries were observed targeting nearly all 39 global industry sectors and 20 geographic regions CrowdStrike Intelligence tracks.
TOP CURRENT TRENDS

- 3rd PARTY SOFTWARE VULNERABILITIES
- CLOUD-BASED ATTACKS
- IDENTITY-BASED BYPASS
CrowdStrike 2023 Cloud Risk Report

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

- **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

**Human error drives cloud risk**

99%

Of cloud security failures are the customer’s fault - Gartner
CYBERSECURITYDIVE
Deep Dive Library Press Releases Topics

MOVEIt vulnerability ensnares more victims
Some organizations have been impacted due to their direct use of MOVEIt while others have been exposed by third-party vendors.
Published June 27, 2023

CYBERSECURITYDIVE

MOVEIt Hack: Number of Impacted Organizations Exceeds 340
The number of entities impacted by the MOVEIt hack — either directly or indirectly — reportedly exceeds 340 organizations and 18 million individuals.

DATA BREACHES

2023-06-01 // SITUATIONAL AWARENESS // Active Intrusion Campaigns Targeting MOVEIt File Transfer Software

What Happened?
Yesterday, Progress Software announced a vulnerability in its MOVEIt file transfer software. The vulnerability, which has yet to be issued a CVE value, facilitates the use of web shells and remote code execution (RCE). Exploitation has been acknowledged in public forums with dates as early as May 27, 2023.
Patches are available from the vendor at the link above.

Recommendations
Without mincing words: MOVEIt needs to be ruthlessly and efficiently hunted and patched in impacted environments. Shodan shows over 2,500 public-facing MOVEIt servers.
Progress Software is recommending that HTTP and HTTPS traffic on ports TCP/80 and TCP/443 be restricted on MOVEIt systems until patching can be completed. Falcon Firewall, or any host-based/network firewall, can be used to implement this control.
As there are active campaigns in the wild, mitigating the threat to MOVEIt software should be given the highest priority.

Intelligence
Falcon Intelligence customers can use the following links to read technical reporting on MOVEIt exploitation [ US-1 | US-2 | EU | Gov ].
TrustedSec also has a good writeup [here].
China-based hackers breached US government email accounts, Microsoft and White House say

By Sean Lyngeas, CNN
Updated 9:51 PM EDT, Wed July 12, 2023

Microsoft takes pains to obscure role in 0-days that caused email breach

Critics also decry Microsoft's "pay-to-play" monitoring that detected intrusions.

DAN GOODIN - 7/14/2023, 5:19 PM

Microsoft Security Breach: A Wake-Up Call For Board Of Directors

Betsy Atkins Contributor

I'm a board vet writing about corporate governance & business trends

Jul 18, 2023, 02:26pm EDT

CISA and Microsoft Partnership Expands Access to Logging Capabilities Broadly

Released: July 19, 2023

Microsoft 365 Breach Risk Widens to Millions of Azure AD Apps

July 21, 2023

China-linked APT actors could have single-hop access to the gamut of Microsoft cloud services and apps, including SharePoint, Teams, and OneDrive, among many others.
ACCESS BROKERS: VITAL ROLE IN THE E-CRIME ECOSYSTEM

ACCESS BROKERS ARE THREAT ACTORS WITH A SIGNIFICANT HISTORY OF PROVIDING INITIAL ACCESS TO MULTIPLE ENTITIES

ACCESS BROKERS OFTEN PERFORM ADDITIONAL ROLES IN THE E-CRIME ECOSYSTEM
Access Broker Boom

Acceleration of demand
Popularity 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.
ACADEMIC CREDENTIAL ADVERTISEMENTS - Q2 2023
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

Uncontested ACCESS
Highly Federated LATERAL MOVEMENT
Faster BREAKOUT
HIGHER ED SPECIFIC THREATS

- Why Higher Ed?
- Adversary Trends
- Denial of Service
- Ransomware & Data Extortion
- Third-Party Tools
- Potential future C2
WHY HIGHER ED?

- Large user base
- Diverse end-points
- Powerful resources
- Intellectual property
- High-profile
- Federated IT/Cybersecurity models
- “Deep Pockets”
- Trusted access to other sectors:
  - Government (Civilian and Defense)
  - Manufacturing (Engineering, Chemical, Pharmaceutical, Telecom, etc.)
  - Technology
  - Healthcare
Education Sector - Adversary Motivations

- Nation State: 7
- eCrime: 13
- Hacktivist: 2
EDUCATION SECTOR - NATION STATE TRENDS

China: 1
DPRK (North Korea): 4
Russia: 2
Iran: 0
POTENTIAL DISRUPTIVE IMPACTS TO HIGHER ED

TARGET: INSTRUCTIONAL TECHNOLOGY AND TEACHING TOOLS

TARGET: INTELLECTUAL PROPERTY/RESEARCH INFORMATION

TARGET: STUDENT LIFE/FOOD & DINING SYSTEMS

TARGET: SAFETY SECURITY SYSTEMS, INCLUDING VIDEO AND DOOR ACCESS

TARGET: PROFESSOR AND STUDENT DATA AND PII

TARGET: ACADEMIC RECORDS AND GRADES
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
RECENT RANSOMWARE INCIDENTS

Mount Saint Mary College Reports Data Breach Affecting 17,924 Students and Employees, February 7, 2023

Possible cyber-security breach at five Louisiana schools, March 26, 2023

Ransomware Forces Shoreline Community College to Go Remote, March 27, 2023
REMOTE LEARNING IMPLICATIONS ON HIGHER ED STUDENT DATA SECURITY

- Remote learning expanded data at rest/in transit exponentially.
- While dissipating, ongoing evolution of the pandemic variants poses threat to in-person learning.
- 3rd party productivity and collaboration tool use exploded.
  - Zoom
  - Dropbox
  - Google Cloud
  - Etc.
THE WAY FORWARD

- CISA Recommendations
- CrowdStrike Recommendations
- 5 Steps to be Prepared
Recent CISA Report on Strengthening K-12 Cybersecurity May Help Institutes of Higher Ed

High Ed Institutions may find the key findings & recommendations useful:

- Develop Cyber IR plan leveraging the NIST CSF
- Build a relationship w/ CISA & FBI regional cybersecurity personnel
- Implement MFA
- Minimize the burden of security
- Training and awareness campaign
- Consider applying for cyber grants
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 Risk Assessment.
  - Conduct a free Cloud Risk Assessment.

*https://www.cisecurity.org/ms-isac/services
5 Steps To Be Prepared

1. Gain visibility into your security gaps
2. Prioritize identity protection
3. Prioritize cloud protection
4. Know your adversary
5. Practice makes perfect
CALL TO ACTION: PROTECT THE INFORMATION ENVIRONMENT FROM THE ADVERSARY THROUGH A COMPREHENSIVE CYBERSECURITY STRATEGY

Digital Risk Monitoring
Threat Intelligence
Malware Analysis & Search

OS & App Yuln Mgmt
Cloud Security Posture Mgmt
Attack Surface Monitoring

XDR
EDR
Log Mgmt
Asset Discovery
File Integrity Monitoring

Next-Gen Antivirus
Firewall Mgmt
Device Control
Cloud Workload Protection
Data Protection

Threat Hunting
MDR
Incident Response
Forensics

Hunting & Response

Threat Intel

Visibility & Orchestration

Attack Surface Mgmt

Identity Threat Detection
Identity Threat Protection

Identity & Access Mgmt

Workloads
Data
Networks

The Information Environment

Identities
CALL TO ACTION: PROTECT THE INFORMATION ENVIRONMENT FROM THE ADVERSARY THROUGH A COMPREHENSIVE CYBERSECURITY STRATEGY

The Information Environment

Identity & Access Mgmt

Hunting & Response

Data

WORKLOADS

Networks

Visibility & Orchestration

Attack Surface Mgmt

Threat Intel

Prevention & Protection

Falcon Recon
Falcon Intelligence
Falcon Sandbox & MalQuery

Falcon OverWatch
Falcon Complete
IR Services
Falcon Forensics

Falcon Spotlight
Falcon Horizon
Falcon Surface

Falcon XDR
Falcon Insight
Falcon LogScale
Falcon Discover
Falcon FileVantage

Falcon Prevent
Falcon Firewall Mgmt
Falcon Device Control
Falcon CWP
Falcon Data Protection