ZEROFOX®

#SaveBaltimore | #BaltimoreRiots

CRISIS MANAGEMENT

THE FOLLOWING INFORMATION IS PROPRIETARY AND CONFIDENTIAL

ZEROFOX CRISIS MANAGEMENT

WHAT WE DO? ZeroFOX identifies threats and protects key assets during emergency crises. The ZeroFOX platform identifies and monitors public and private global communication channels and distills the signal from the noise to ensure that the proper resources are focused on responding to high-confidence threats.

Threat Identification

- Threat Actors: Physical & digital actors are identified and prioritized based upon context, threat impact, and actor attributes. Immediate Response is Recommended.
- Influencing Actors: Physical & digital influencers are creating or influencing eco-systems that could spread propaganda, misinformation, or actual information.

Asset Protection

- People: Key individuals that are actively being targeted physically or digitally to include the attack type, risk, and actionable recommendations.
- Organizations: Key organizations that are actively being targeted physically or digitally to include the attack type, risk, and actionable recommendations.
- Systems: Key technical systems that are actively being targeted digitally to include the attack type, risk, and actionable recommendations.

Emergency Contact Info

Email: asap@zerofox.com
Phone: 844-FOX-7259

EXECUTIVE SUMMARY

4/28 - 2:32PM

THREATS MITIGATED	19
Actors Monitored	62
Influencers Monitored	187
Fraud Accounts Monitored	91

ASSETS PROTECTED	
People Monitored	11
Systems Monitored	56
Organizations Monitored	6

1. Apply additional security resources to PROTECTED SYSTEMS immediately in the form of DDOS mitigation services, system patching, two-factor administrator authentication, and DR backups. Coordinated attacks began at 2330 2/27 and are expected to increase in volume around 1500-1700 2/28

2. Monitor and secure all digital personal and professional accounts for PROTECTED PEOPLE. This includes but is not limited to Social Accounts, Email, Bank Accounts, and Gov Accounts. Alerts should immediately be sent to all PROTECTED PEOPLE to ensure that they are informed of their personal and professional risks by being targeted and sensitive information being disclosed.

3. Organization-wide emails should be sent to all PROTECTED ORGANIZATIONS to alert them of the pending and in-process attacks. Additional caution should be used when opening emails and social communication given the increase in targeted phishing attacks.

4. Alert Governor Hogan that his social and email addresses may have been compromised as of 1130 EST 2/28.

5. Alert Baltimore PD on all monitoring threat actors and influencers.

ZEROFOX®

THREAT ACTORS: #MOSTWANTED

CRISIS MANAGEMENT

THREAT ACTORS

@AnonOlympus

Geo: **Unknown**
Severity: **MEDIUM**
Threat Type: **CYBER, DOX**

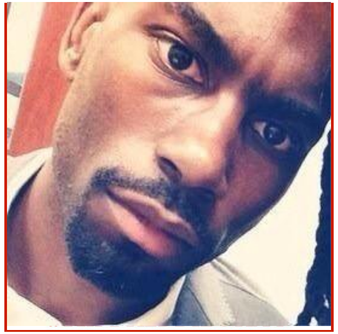
REACH	HIGH
ENGAGEMENT	MEDIUM
ACTION	CONTINUOUS MONITORING, TAKEDOWN DOX POSTS
NOTES	General Anonymous account publishing PII about protected assets, inciting protestors

@OpBaltimore

Geo: **Baltimore City**
Severity: **HIGH**
Threat Type: **CYBER**

REACH	MEDIUM
ENGAGEMENT	MEDIUM
ACTION	BOLSTER CYBER DEFENSE, CONTINUOUS MONITORING
NOTES	Dedicated #OpBaltimore account, spreading IRC channel login and inciting protests. Following relatively small (under 1K), but growing rapidly.

THREAT ACTORS



DeRay McKesson @deray

Geo: **St. Louis**
(Currently Baltimore)
Severity: **HIGH**
Threat Type: **PHYSICAL**

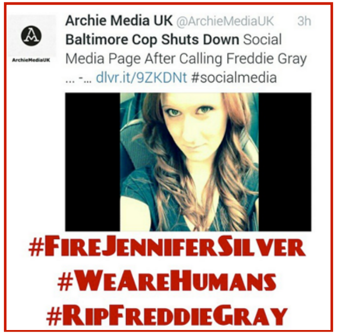
REACH	HIGH
ENGAGEMENT	HIGH
ACTION	CONTINUOUS MONITORING
NOTES	One of the main coordinators of the protests -- affiliated with nowisthemovement.org, wetheprotestors.org and baltimoreuprising.org. Massive following. Facebook Email Instagram LinkedIn Personal Vine

Johnetta “Netta” Elzie @nettaaaaaaaa

Geo: **St. Louis**
Severity: **HIGH**
Threat Type: **PHYSICAL**

REACH	HIGH
ENGAGEMENT	HIGH
ACTION	CONTINUOUS MONITORING
NOTES	One of the main coordinators of the protests -- affiliated with nowisthemovement.org, #ferguson and baltimoreuprising.org. Massive following. Facebook Email Instagram

THREAT ACTORS



Archie Media UK @ArchieMediaUK 3h
Baltimore Cop Shuts Down Social Media Page After Calling Freddie Gray ... -... dlvr.it/9ZKDNt #socialmedia

#FireJenniferSilver
#WeAreHumans
#RipFreddieGray

terminateofficerjennifersilver

Geo: **Unknown**
Severity: **HIGH**
Threat Type: **DOX**

REACH	MEDIUM
ENGAGEMENT	MEDIUM
ACTION	PROFILE TAKEDOWN
NOTES	Instagram account slandering Officer Jennifer Silver and publishing PII.

@KINGDACEO

Geo: **Baltimore City**
Severity: **MEDIUM**
Threat Type: **PHYSICAL**

REACH	HIGH
ENGAGEMENT	HIGH
ACTION	CONTINUOUS MONITORING
NOTES	Threat actor is coordinating supplies for protesters -- appears to be one of the main local protest organizers

THREAT ACTORS

@poLicedoX

Geo: **Unknown**
Severity: **HIGH**
Threat Type: **DOX**

REACH	LOW
ENGAGEMENT	HIGH
ACTION	PROFILE TAKEDOWN
NOTES	Twitter account DOXing protected entities associated with the protests.

@BmoreBloc

Geo: **Baltimore City**
Severity: **MEDIUM**
Threat Type: **PHYSICAL**

REACH	HIGH
ENGAGEMENT	HIGH
ACTION	CONTINUOUS MONITORING
NOTES	Main Twitter account for protest coordination

INFLUENCERS

Handle	Severity	Geo	Reach	Engagement	Notes
@xpuppydogx	Medium	N/A	High	Low	
@monstaX	Medium	N/A	High	Low	
@AjCool16	Low	N/A	High	Medium	
@LatinaAnarchist	Medium	N/A	High	Medium	Sending supplies from NJ
@Slangincrack	Medium	Local	High	High	Death threats, possible troll

ZEROFOX

ASSET PROTECTION: #DEFENDBALTIMORE

CRISIS MANAGEMENT

PROTECTED PEOPLE

Name	Attack	Physical PII	Digital PII	Credit Info	SSN	Family PII	Associate PII	Impersonation
Larry Hogan	Cyber							YES
Stephanie Rawlings-Blake	DOX	YES	YES			YES	YES	YES
Officer Jennifer Silver	DOX	YES				YES		
Matt Martino	DOX							
Lt. Brian Rice	NA							
Officer Caesar Goodson	NA							
Sgt. Alicia White	NA							
Officer William Porter	NA							
Officer Garrett Miller	NA							
Officer Edward Nero	NA							
Captain Eric Kowalczyk	NA							

IMPERSONATION ATTACK DETAILS

Name	Impersonator	Profile URL	Social Network
Stephanie Rawlings-Blake	Stephanie.rawlingsblake.1	https://www.facebook.com/stephanie.rawlingsblake.1?ref=br_rs	Facebook
	@srbforbaltimore	https://twitter.com/srbforbaltimore	Twitter
	@bizarrosrb	https://twitter.com/BizarroSRB	Twitter
	@MajorSRB	https://twitter.com/MajorSRB	Twitter
Baltimore City Police	@BaltimorePolice	https://twitter.com/BaltimorePolice	Twitter
	@baltimorepolice	https://twitter.com/baltimorepolice	Twitter
	Baltimore-City-Police-Department	https://www.facebook.com/pages/Baltimore-City-Police-Department/153395264698498	Facebook
	@BaltimorePolice	https://twitter.com/BaltimorePolice	Twitter
	@baltimorecitypolice	https://instagram.com/baltimorecitypolice/	Instagram
	@baltimorecitypolicedept	https://instagram.com/baltimorecitypolicedept/	Instagram
	@cebaltimore8eea	instagram.com/cebaltimore8eea	Instagram
Governor Larry Hogan	@GovernorHogan	https://twitter.com/GovernorHogan	Twitter
	@LarryHogan	https://twitter.com/LarryHogan	Twitter
Maryland National Guard	@mdnationalguard	https://twitter.com/mdnationalguard	Twitter

**ZeroFOX can mitigate / takedown with approval*

PROTECTED ORGANIZATIONS

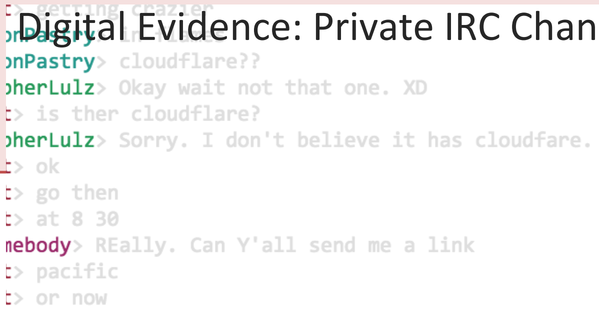
Organization Name	Coordinated Cyber Attack	Coordinated Physical Attack	Key Individuals Targeted	Impersonation Attacks	Identifiable Aggressors	Notes
Baltimore City Police	Yes	Yes	Yes	Yes	Yes	ZeroFOX Monitoring
Baltimore City Government	Yes	Yes	Yes	Yes	Yes	ZeroFOX Monitoring
Maryland State Government			Yes		Yes	ZeroFOX Monitoring
Maryland State Troopers		Yes	Yes		Yes	ZeroFOX Monitoring
National Guard				Yes		ZeroFOX Monitoring
Baltimore Fire Department		Yes				ZeroFOX Monitoring

Protected Systems

[redacted]

PROTECTED SYSTEMS

Findings / Techniques	Recommendations
ZeroFOX Assessment: • Probability of a coordinated attack is high • Limited number of participants prior to Tuesday afternoon EST • First designated start time was 11:30pm EST 8/27 • Future wave of start time is roughly 3-5pm EST 8/28 • No public endorsement on the #ddos channel or anonops IRC; however private endorsement is active Observed Techniques: • DDoS Tools in use to target PROTECTED ORGANIZATIONS: • LOIC, VDOS, Anonware, Str3ssed	• Migrate sites to cloud (ex: AWS, Inherent protections) • Establish DDoS Mitigation Service • As seen below via a direct IRC conversation from the attackers: likelihood to drop it off if protected via DDoS mitigation services (CloudFlare, Akamai, etc...).



Digital Evidence: Private IRC Channel

```
t> getting crazier
onPastry> in flames
onPastry> cloudflare??
pherLulz> Okay wait not that one. XD
t> is ther cloudflare?
pherLulz> Sorry. I don't believe it has cloudfare.
t> ok
t> go then
t> at 8 30
mebody> REally. Can Y'all send me a link
t> pacific
t> or now
```

ZEROFOX®

COVERT RENDERINGS OF TECHNICAL SYSTEM ATTACK PLANS

CRISIS MANAGEMENT

[redacted]

[redacted]

ZEROFOX®