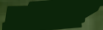


# The Anatomy of a Cyber Breach

There's nothing like breaking news of a healthcare data breach to create a chilling effect for health data interoperability. This fireside chat will cover various aspects of a cyber attack using real world examples.

Annual  
Meeting  
2024

DEC  
11-12

NASHVILLE  TENNESSEE



Featured Speaker

**Daniel Polk**

Special Agent, FBI Atlanta









Moderator

**Johnathan Coleman**

CISO, TECCA RCE

# Types of Threat Actors

THREATS	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
						
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.



# Recent Examples of security incidents

- Aug 13, 2024: OCR settlement for breach involving 2.4 million patients (Apr 2023). Sanctions included fines and mandatory implementation of MFA for all individual user accounts <sup>1</sup>
- May 3, 2024: U.S. House of Representatives report on the Feb 21, 2024 Change Health incident: The #1 thing learned was “the attack occurred because UnitedHealth wasn’t using multifactor authentication [MFA], which is an industry standard practice, to secure one of their most critical systems”. This incident affected approximately 1/3 of all Americans. See What We Learned: Change Healthcare Cyber Attack (house.gov) <sup>2</sup>
- Feb 21, 2024: OCR settles a ransomware investigation that affected over 14,000 individuals. OCR recommends all HIPAA entities utilize multi-factor authentication as a best practice to ensure only authorized users are accessing protected health information <sup>3</sup>

<sup>1</sup> <https://thecyberexpress.com/enzo-biochem-data-breach-cost-millions/>

<sup>2</sup> <https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack>

<sup>3</sup> <https://www.hhs.gov/about/news/2024/02/21/hhs-office-civil-rights-settles-second-ever-ransomware-cyber-attack.html>

# Physical & Digital Security



The Atlanta Journal-Constitution

News

Subscribe



Log In

Metro Atlanta

Georgia News

Legislature

National & World News

Business

2024 Election

The Trump Investigations

LOCAL NEWS

## IT professional pleads guilty in Gwinnett Medical Center hacking case

Patient information compromised



# #StopRansomware: Black Basta

- On 10 May, 2024, The FBI, CISA, HHS, and Multi-State Information Sharing and Analysis Center (MS-ISAC) released joint Cybersecurity Advisory AA24-131A<sup>1</sup> to provide information on Black Basta, a ransomware-as-a-service (RaaS) variant which was first identified in April 2022.
- Black Basta affiliates have impacted over 500 organizations globally and have encrypted and stolen data from at least 12 out of 16 critical infrastructure sectors.
- Healthcare organizations are attractive targets for cybercrime actors due to their size, technological dependence, access to personal health information, and unique impacts from patient care disruptions.



Note: Per CISA, Cybersecurity Advisory Alert Code AA24-131A is TLP:CLEAR  
Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

<sup>1</sup>[https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a?utm\\_source=SRWgov&utm\\_medium=page&utm\\_campaign=SRW](https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a?utm_source=SRWgov&utm_medium=page&utm_campaign=SRW)

# #StopRansomware: Black Basta – Initial Access

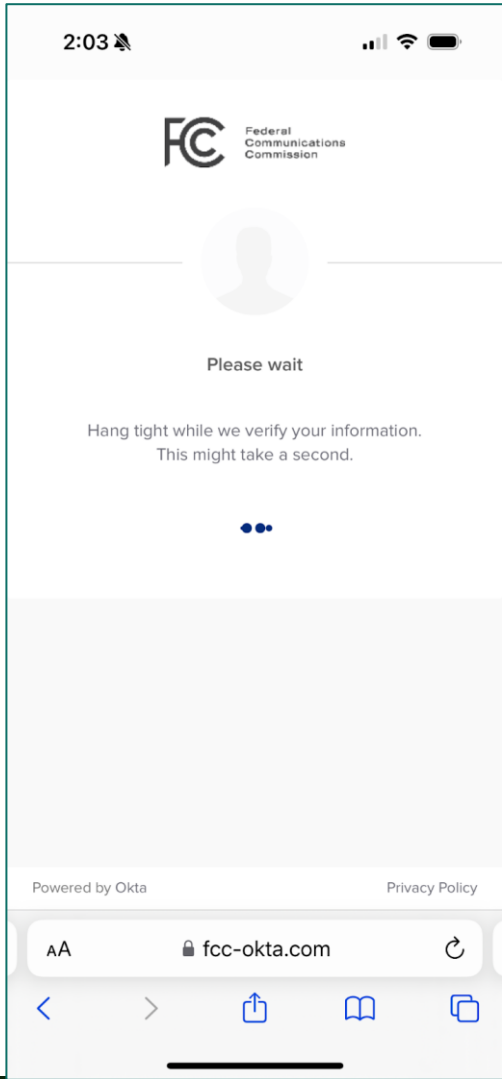
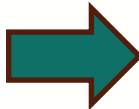
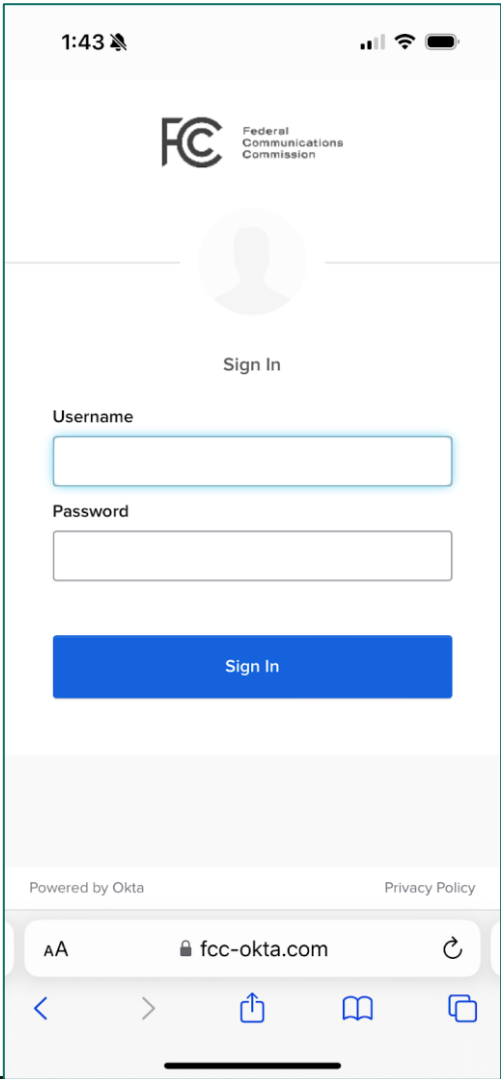
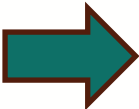
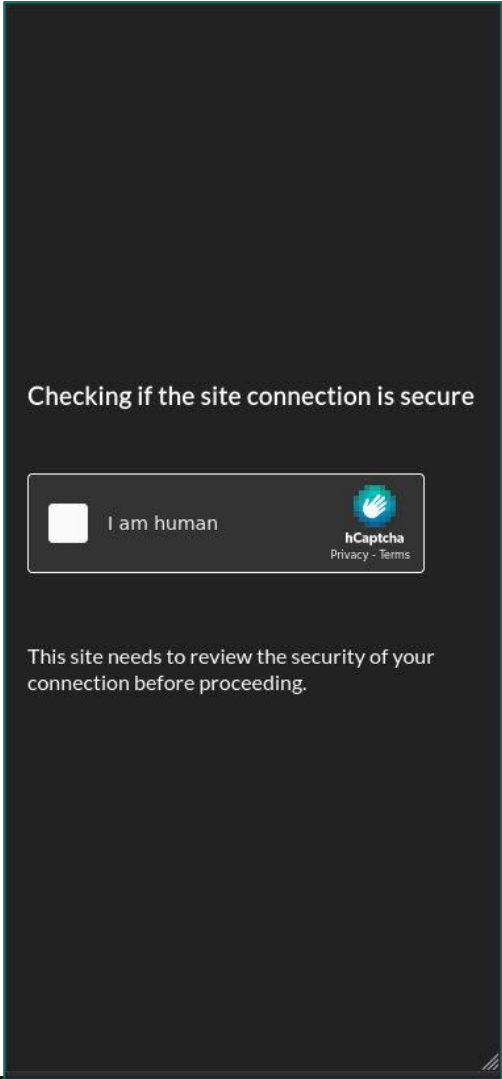
- Black Basta affiliates primarily use spearphishing to obtain initial access. Affiliates have also used Qakbot (AKA Qbot or Pinkslipbot), initially purposed as a credential stealer.
- Starting in February 2024, Black Basta affiliates began exploiting known vulnerabilities in COTS software to harvest and abuse valid credentials for initial access.
- **Update Nov 8, 2024:** Recent techniques include email bombing—a tactic used to send a large volume of spam emails—to aid social engineering over Microsoft Teams and trick victim end users into providing initial access via remote monitoring and management (RMM) tools.
  - Targeted users were sent a large volume of spam email, often from legitimate sources like website registrations, email subscriptions, and other marketing content.
  - Black Basta affiliates would subsequently call the victim, act as technical support, and offer to fix the issue.
  - In October 2024, this social engineering campaign incorporated the use of Microsoft Teams to contact victims. Black Basta affiliated operators would message the victims from legitimate Microsoft Teams accounts from external organizations, posing as technical support to resolve the email spam issues.
  - Black Basta affiliates requested victim users to download tools for allowing remote access.



# Contextual Campaigns

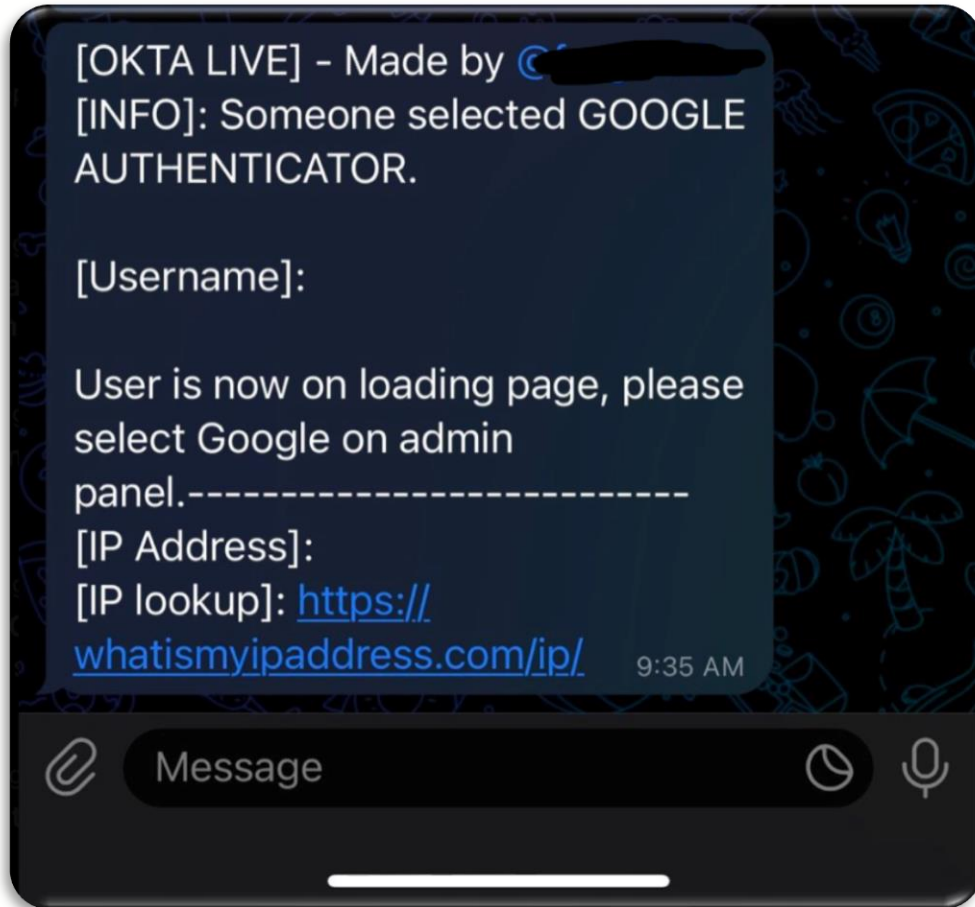
[REDACTED]  
[REDACTED]@[REDACTED]biotech.com)  
has invited you to join the  
private Zoom Meeting "Incident  
Response". Please tap [https://  
adaptivebiotech-zoom.com/  
meeting/incident](https://adaptivebiotech-zoom.com/meeting/incident) to join.

# Breaking MFA

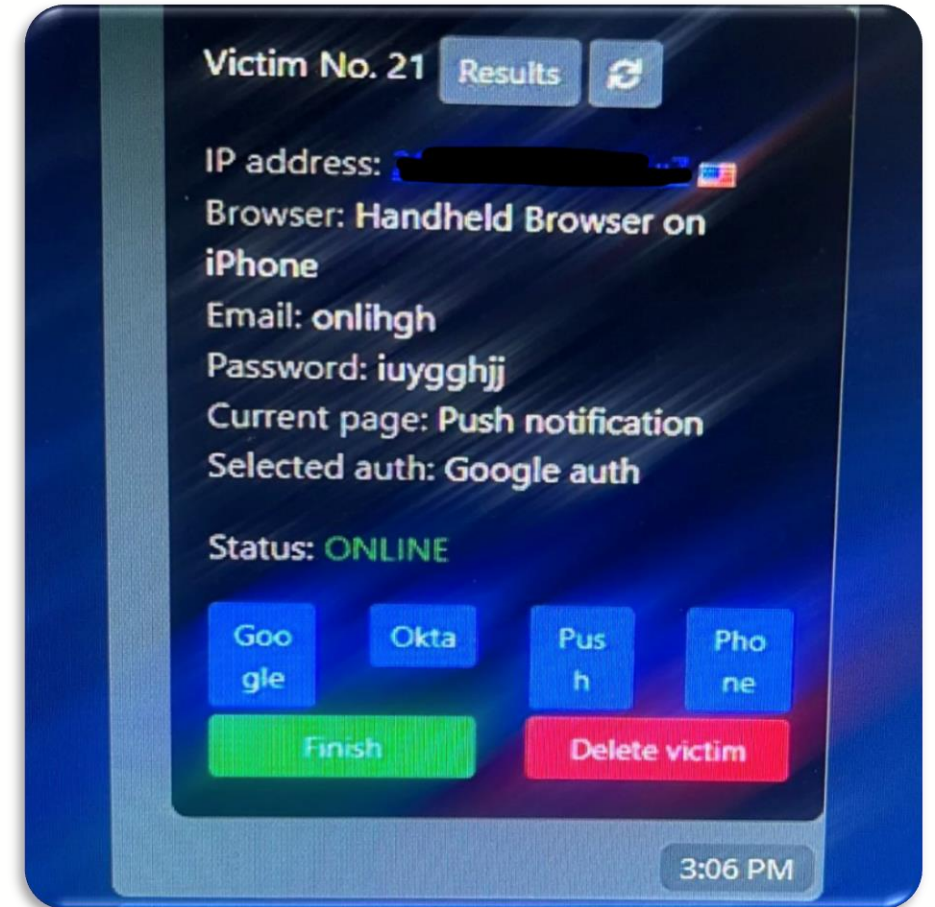
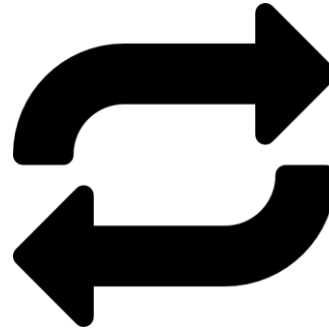




# Breaking MFA



*Telegram Bot Provides New Victim Alerts*



*Criminal Selects MFA on Admin Panel*

# #StopRansomware: Black Basta – Privilege Escalation and Lateral Movement

- **Privilege Escalation**

- Black Basta affiliates use credential scraping tools like Mimikatz for privilege escalation.
- According to cybersecurity researchers, Black Basta affiliates have also exploited other vulnerabilities for local and Windows Active Domain privilege escalation, including:
  - ZeroLogon (CVE-2020-1472 [CWE 330])
  - NoPac (CVE-2021-42278 [CWE-20] and CVE-2021-42287 [CWE-269])
  - PrintNightmare (CVE 2021-34527 [CWE-269])

- **Lateral Movement**

- Black Basta affiliates use tools such as BITSAdmin and PsExec, along with Remote Desktop Protocol (RDP), for lateral movement.
- Some affiliates also use tools like Splashtop, Screen Connect, and Cobalt Strike beacons to assist with remote access and lateral movement.

# #StopRansomware: Black Basta – Exfiltration and Encryption

- Black Basta affiliates use RClone to facilitate data exfiltration prior to encryption
- Prior to exfiltration, cybersecurity researchers have observed Black Basta affiliates using PowerShell to disable antivirus products, and in some instances, deploying a tool called Backstab, designed to disable endpoint detection and response (EDR) tooling
- Once antivirus programs are terminated, a ChaCha20 algorithm with an RSA-4096 public key fully encrypts files
- A **.basta** or otherwise random file extension is added to file names and a ransom note titled **readme.txt** is left on the compromised system
- To further inhibit system recovery, affiliates use the **vssadmin.exe** program to delete volume shadow copies



# #StopRansomware: Black Basta – Indicators of Compromise

- Network Indicators Disclaimer: The authoring organizations recommend network defenders investigate or vet IP addresses prior to taking action, such as blocking, as many cyber actors are known to change IP addresses, sometimes daily, and some IP addresses may host valid domains.
- **Update Nov 8, 2024:** The IOCs listed in the threat advisory were obtained from trusted third-party reporting

IP Address	First Seen	Description
170.130.165[.]73	October 14, 2024	Likely Cobalt Strike infrastructure
45.11.181[.]44	October 24, 2024	Likely Cobalt Strike infrastructure
66.42.118[.]54	October 15, 2024	Exfiltration server
79.132.130[.]211	October 24, 2024	Likely Cobalt Strike infrastructure

Domain	First Seen
Moereng[.]com	October 9, 2024
Exckicks[.]com	October 2, 2024

# #StopRansomware: Black Basta – Mitigation



## ACTIONS FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS TO TAKE TODAY TO MITIGATE CYBER THREATS FROM RANSOMWARE:

1. Install updates for operating systems, software, and firmware as soon as they are released.
2. Require phishing-resistant MFA for as many services as possible.
3. Train users to recognize and report phishing attempts.

[https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a?utm\\_source=SRWgov&utm\\_medium=page&utm\\_campaign=SRW](https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a?utm_source=SRWgov&utm_medium=page&utm_campaign=SRW)

# How can the FBI help?

- *Before an attack:*
  - Table-Top Exercises (TTX):
    - Identify Team Players
    - Comms (Out-of-band)
    - LE notification
    - Pay / Not Pay ransom
    - What to tell the board
- *After an attack:*
  - **From the moment a company knows the variant of ransomware, every minute spent not asking for a potential decryption key is business revenue lost.**
  - CAT – Cyber Action Team
  - Attribution, Recovery, and Restitution



# Reporting

- The Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3)  
<https://www.ic3.gov/>
- The Cybersecurity and Infrastructure Security Agency's (CISA's) online Incident Reporting System;  
<https://myservices.cisa.gov/irf>
- CISA's 24/7 Operations Center at [report@cisa.gov](mailto:report@cisa.gov) or (888) 282-0870
- The FBI encourages organizations to report information concerning suspicious or criminal activity to their local FBI Field Office



<https://www.fbi.gov/contact-us/field-offices>

[https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a?utm\\_source=SRWgov&utm\\_medium=page&utm\\_campaign=SRW](https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a?utm_source=SRWgov&utm_medium=page&utm_campaign=SRW)

# Annual Meeting 2024



NASHVILLE  TENNESSEE

the  
sequoia<sup>®</sup>  
project



carequality

• Thank you!