



MCP

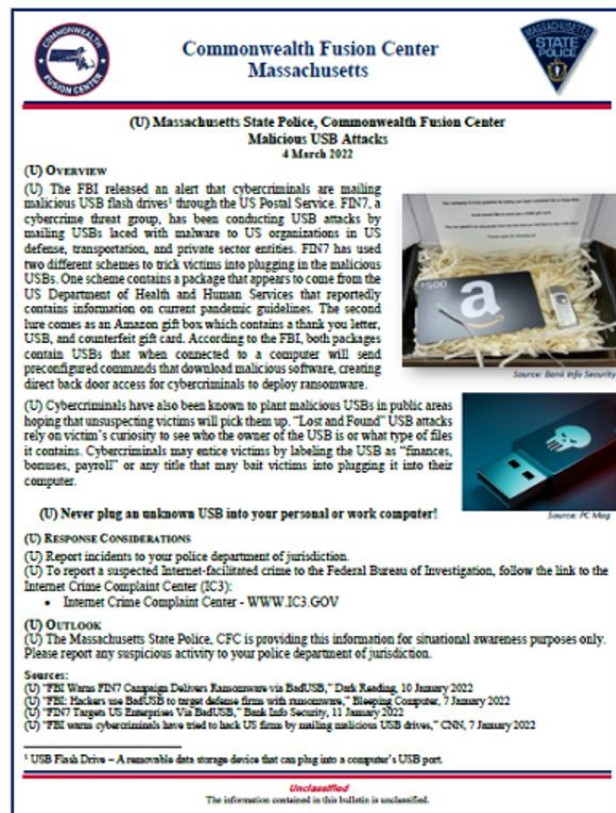
Massachusetts
Cybersecurity Program

Unclassified//For Official Use Only



Commonwealth Fusion Center Massachusetts Cybersecurity Program

- Established in 2016 to address increasing cyber threats to Critical Infrastructure
- Information Sharing, Awareness Bulletins, Trainings, Pass-through Alerts, Threat Briefings
- MCP distro
- Partnerships



Executive Overview

- Attack response windows have collapsed as adversaries operate at machine speed.
- Modern intrusions increasingly prioritize “logging in” with stolen identities rather than breaking in with malware.
- Cloud, edge, identity, and AI-enabled social engineering are now central attack surfaces.
- Defensive priorities: automation, phishing-resistant authentication, and an assume-breach mindset.



Velocity: The “Minutes” Window

Based on data collected by CrowdStrike:

- **Average eCrime breakout time:** 29 minutes—65% faster.
- **Fastest documented breakout:** 27 seconds.
- **Vulnerability exploitation:** The disclosure-to-exploitation window has fallen from weeks or days to hours.
- **Ransomware handoff:** Initial access brokers have transferred access to operators in as little as 22 seconds.



Weaponization of Artificial Intelligence

- Generative AI scales phishing, vishing and voice cloning, deepfake social engineering, and rapid code reconnaissance.
- Criminal forums recorded a 550% increase in ChatGPT mentions.
- Attackers use AI to generate malicious commands across many organizations simultaneously.
- Adaptive techniques help bypass basic behavioral detection.



Identity and Malware-Free Intrusions

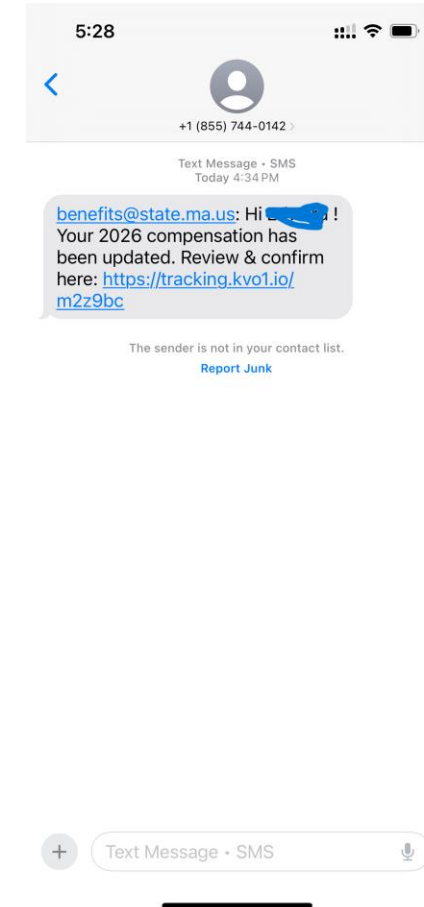
- **79%–82% of detections are malware-free.**
- Threat actors use valid credentials, stolen session tokens, and compromised SaaS configurations to appear legitimate.
- Common entry points include third-party vendor gaps, OAuth token abuse, and helpdesk impersonation.
- The goal is to infiltrate systems without deploying malicious files.





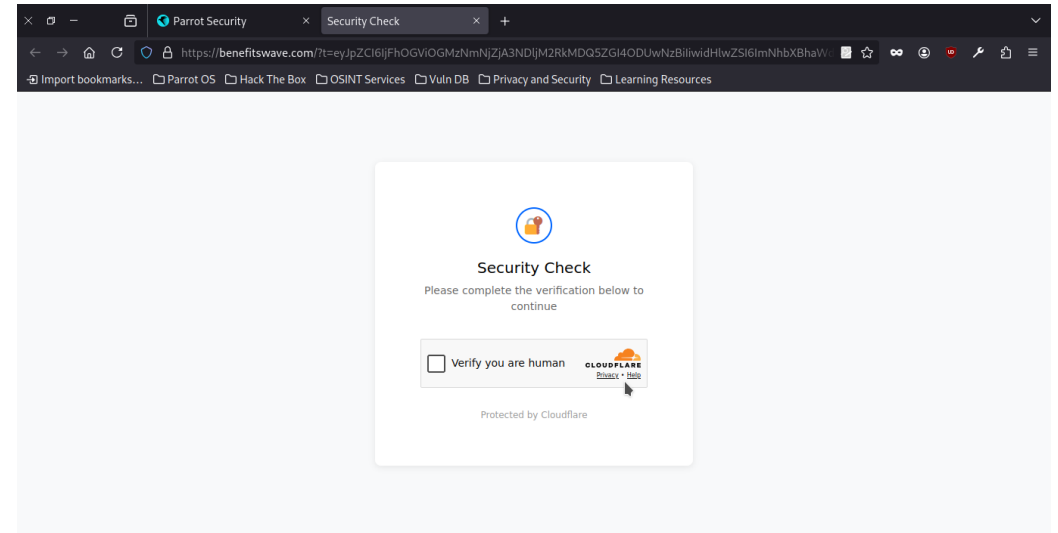
SMS Phishing Campaign

- Received a text from entity claiming to be Commonwealth of Massachusetts HR Benefits.
- Email : [benefits @state.ma.us](mailto:benefits@state.ma.us) (legitimate)
- Phone Number search does not come back to any entity .



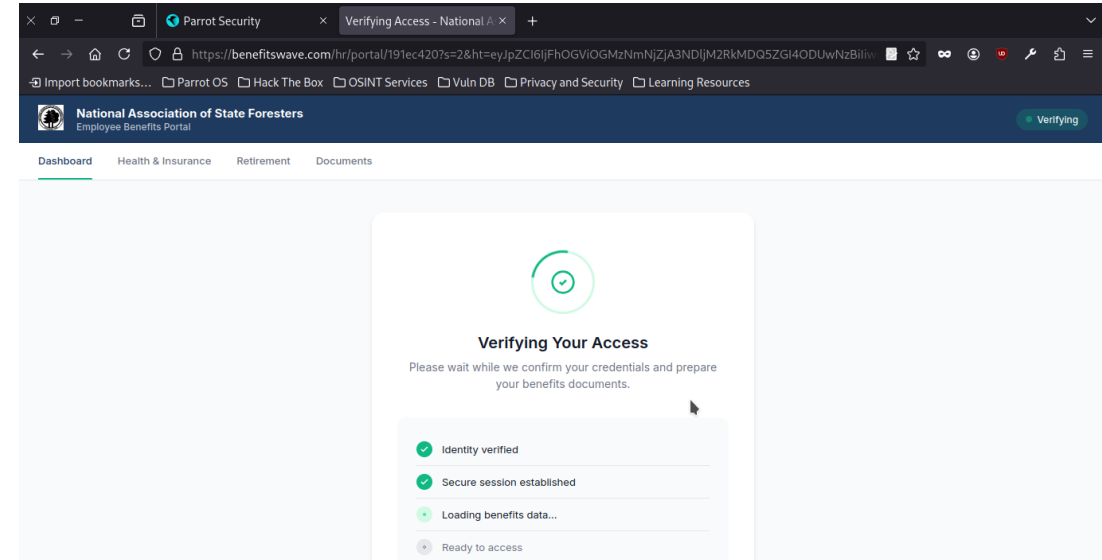
SMS Phishing Campaign

- The URL Link was opened in a sandboxed virtual Machine
- The embedded link redirects to a URL: benefitswave.com
- This website is hosted by Routerhostng LLC and points back to Cloudzy virtual private servers.
- The IP associated with the benefitswave.com site is 172.86.105.195
- The screen on the right requires you to check the box to move forward.



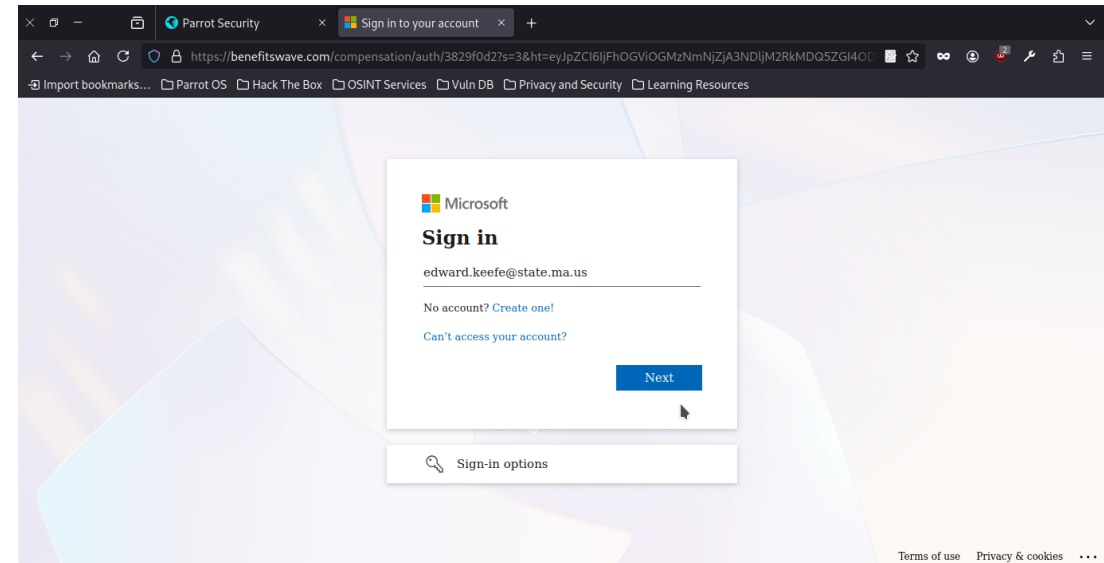
SMS Phishing Campaign

- After the box is checked it automatically opens to a new window within the site that is titled “The National Association of State Foresters”
- Screen appears to go through some type of verification process.
- The legitimate website for stateforesters.org is hosted on IBM cloud.
- I could not find a benefits page for The National Association of State Foresters.



SMS Phishing Campaign

- After the fake verification process, it redirects to a Microsoft login screen where it wants you to enter credentials.
- Most concerning of this was I put the link from the text message into a VM that has never logged into Microsoft Office before, and it popped up with my work email.
- At this point I did not proceed any further.



Attacks on Critical Infrastructure

Ababil of Minab

- Ababil of Minab claimed to have attacked LA County Metro IT systems including administrative access to VMware vCenter Server environment. Open-source reporting stated this cyber-attack required LA Metro Transit to take down internal systems which caused delays to patrons adding funds to their metro cards. Message boards showing departure and arrival times for trains and buses were not operational.



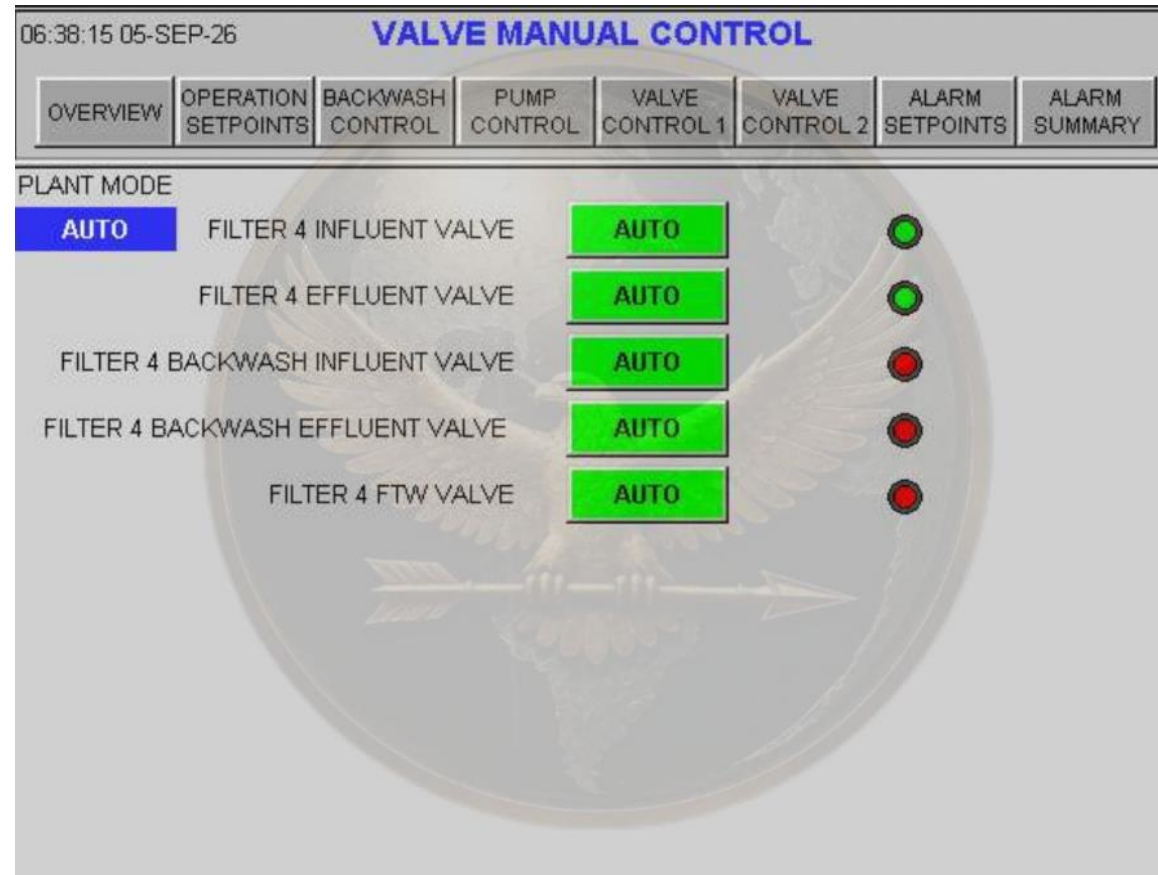
Attacks on Critical Infrastructure

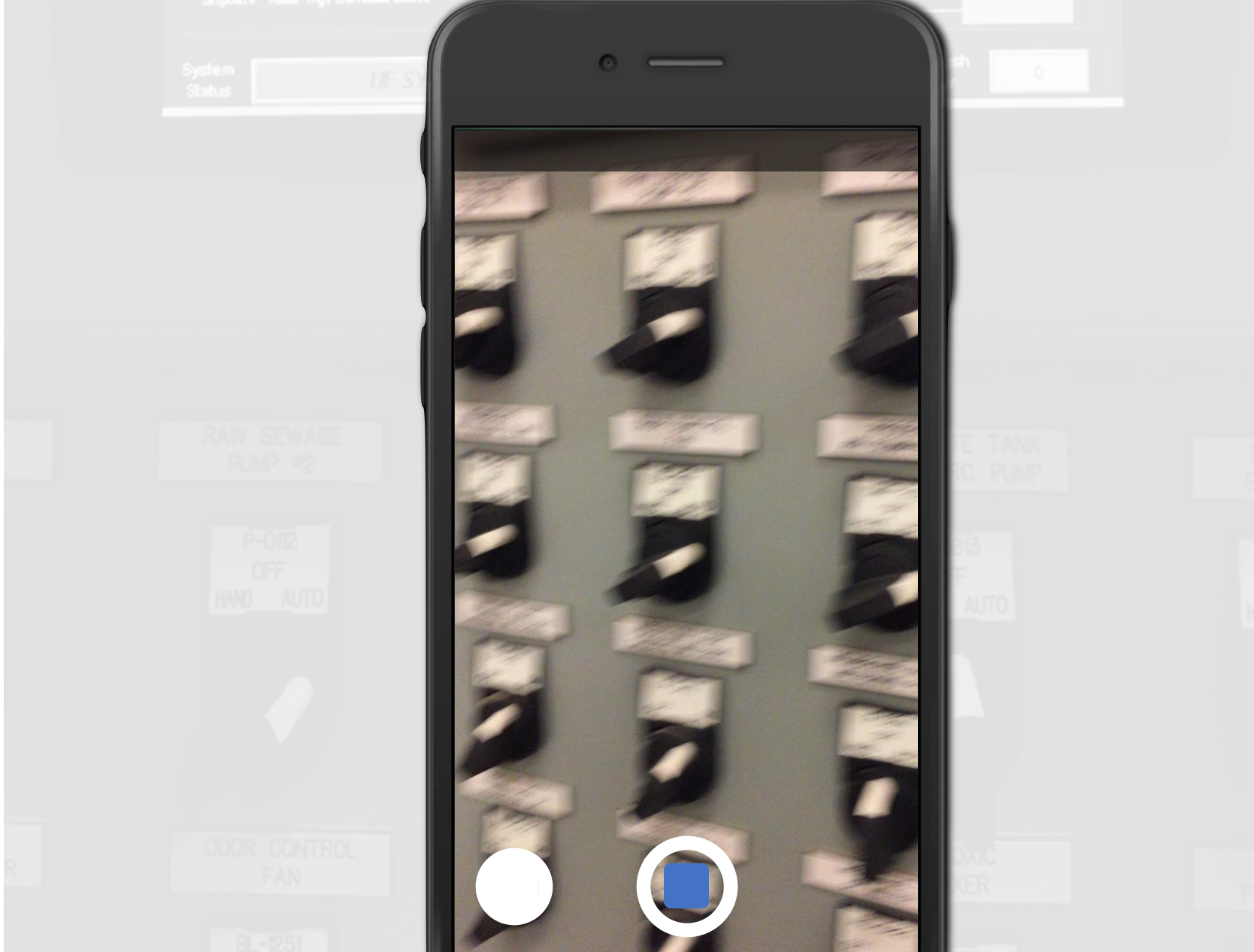
- The Commonwealth Fusion Center has reported on attacks to critical infrastructure (specifically the water sector) for the past several months.
- This month The Commonwealth Fusion Center has observed a Russian speaking group, identified as Golden Falcon.
- This group is sympathetic to Iran. Golden Falcon is leveraging public facing appliances to expose publicly exposed industrial control systems.
- Golden Falcon has published screenshots of the human machine interface(HMI) of these systems.



Attacks on Critical Infrastructure

Golden Falcon





What can be done to help protect my Organization

- Cybersecurity Incidents often lead to information silos.
- Common challenges that hinder Information sharing:
 1. Proprietary information
 2. Legal restrictions (Cyber Insurance)
 3. Legal exposure
 4. Potential embarrassment
 5. Suspicion of outside help (Law Enforcement)



What can be done to help protect my Organization

- Taking a neighborhood watch approach may help
- We need to be better neighbors when things affect our community.
- We need to share information with our peers
 1. Professional Organizations
 2. Work colleagues and peers
 3. Other agencies and departments in our community.
- We need to report incidents to Law Enforcement and take advantage of their information sharing networks.



Reporting

- You are our best source of Cyber Threat Intelligence!
- Reporting entity will not be identified when sharing out information
- “a municipality in Massachusetts” , “a K-12 organization in Massachusetts”, “a public safety agency in Massachusetts”
- Shared information passed on to larger community for situational awareness and as actionable, timely, relevant CTI via MCP Distro



Reporting



Homeland Security



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY



MS-ISAC®
Multi-State Information
Sharing & Analysis Center®



(U/FOUO) CFC Massachusetts Cybersecurity Program Bulletin: Phishing Attacks
November 25, 2019

(U) OVERVIEW

(U/FOUO) Phishing is a cybercrime in which the unsuspecting victim willingly gives sensitive information (personal, financial, business) to who they believe is an official/legitimate institution in which they have a preconceived relationship with.

(U/FOUO) Phishing has consistently been the main tool in most cybercrimes since the rise of the internet. Outcomes of successful phishing attacks may include but are not limited to financial loss, malware infiltration, ransomware attack, data breach, compromise, and other security incidents. There are many forms of phishing but this bulletin will focus on six popular types.

(U) COMMON TYPES OF PHISHING

(U) Spear Phishing

Spear phishing attacks are designed to target a specific person or organization. In this type of attack, suspects try to steal data from the victims via email or electronic communication. Hoaxing is on a specific target allows the suspects to use social engineering, open source, or other research to personalize the information and appear to be more credible to the victim. The more believable the scam, the more likely the victim is to believe the attack to be true and reveal sensitive information.

(U) Whaling

Whaling, like spear phishing, also attacks a specific target, however, whaling attacks are aimed at high profile employees, such as a CEO or another senior official in an organization. These targets are selected as they typically have more access and influence in the company than other employees. Whaling attacks create trust between the attacker and victim through social engineering and other digital means. The possible goals of a whaling attack could be to manipulate the victim into authorizing financial transactions, releasing sensitive information, or approving authorization to the organization's database. The result of releasing sensitive information might not be exploited immediately, but could lead to future attacks.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

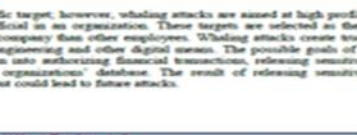
Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.

Declassified//For Official Use Only
The information contained in this bulletin is For Official Use Only. No portion of this bulletin should be released, copied or reproduced or re-disseminated without prior approval of the Commonwealth Fusion Center.



Booba Project: Profile

Financially motivated ransomware and cyber-extortion group; emerged in June 2026.

Assessed as a possible rebrand of Frag ransomware.

Uses double extortion: data theft followed by encryption and leak threats.

Targets public sector, education, manufacturing, professional services, healthcare, and technology.



SonicWall CVE-2026-102255

- Severity: Critical; CVSS 10.0.
- Type: Pre-authentication server-side request forgery.
- Impact: Unauthenticated takeover of an exposed SMA1000 appliance.
- Target: Workplace interface on SonicWall SMA1000 gateways.
- Status: Reported active exploitation shortly after disclosure.
- Affected: SonicWall SMA 6210, SMA 7210, and SMA 8200v
- Successful exploitation may provide backend control and enable lateral movement



Continuity of Operations

A cybersecurity incident is not just an IT Problem

- Financial Issues
 1. People need to be paid
 2. Things need to be ordered
 3. Services need to be performed
- Service Issues
 1. School Lunch
 2. Access to communications
 3. Access to medical records



Next Steps

- Work with all departments of your community to develop a cyber incident response plan.
- Hold a tabletop exercise to at a regular cadence to talk through who an event would be handled.
 1. Who will be in charge of the incident.
 2. What resources do I need.
 3. Will I need outside resources.
- From your cyber incident response plan build that into a Continuity of Operations Plan (COOP)



Resources Available

- CISA - Cross-Sector Cybersecurity Performance Goals - A common set of protections that all critical infrastructure entities - from large to small - should implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques.
- <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>
- <https://www.cisa.gov/resources-tools/resources/no-cost-cybersecurity-services-and-tools>



Resources Available

- Mass Cyber Center - Municipal Cybersecurity Toolkit

<https://masscybercenter.org/municipal-toolkit>

- Utah Cyber Center – Local Government Cybersecurity Playbook.

<https://cybercenter.utah.gov/knowledgebase/category/?id=CAT-01004>



Local Government Cybersecurity Playbook

Best-practice guidance and example products
to support common cybersecurity

Disclaimer (Important)

This playbook is intended as practical guidance for local governments. Example products are provided for planning and procurement discussions and are not endorsement s. All security decisions should be based on local risk, legal requirements , budgets, and operational needs.

MCP Resources

- Commonwealth Fusion Center MA Joint Cyber Threat Briefing
 - Last Thursday of every month
- Commonwealth Fusion Center MCP distro list.
- Commonwealth Fusion Center MCP VTIP program.



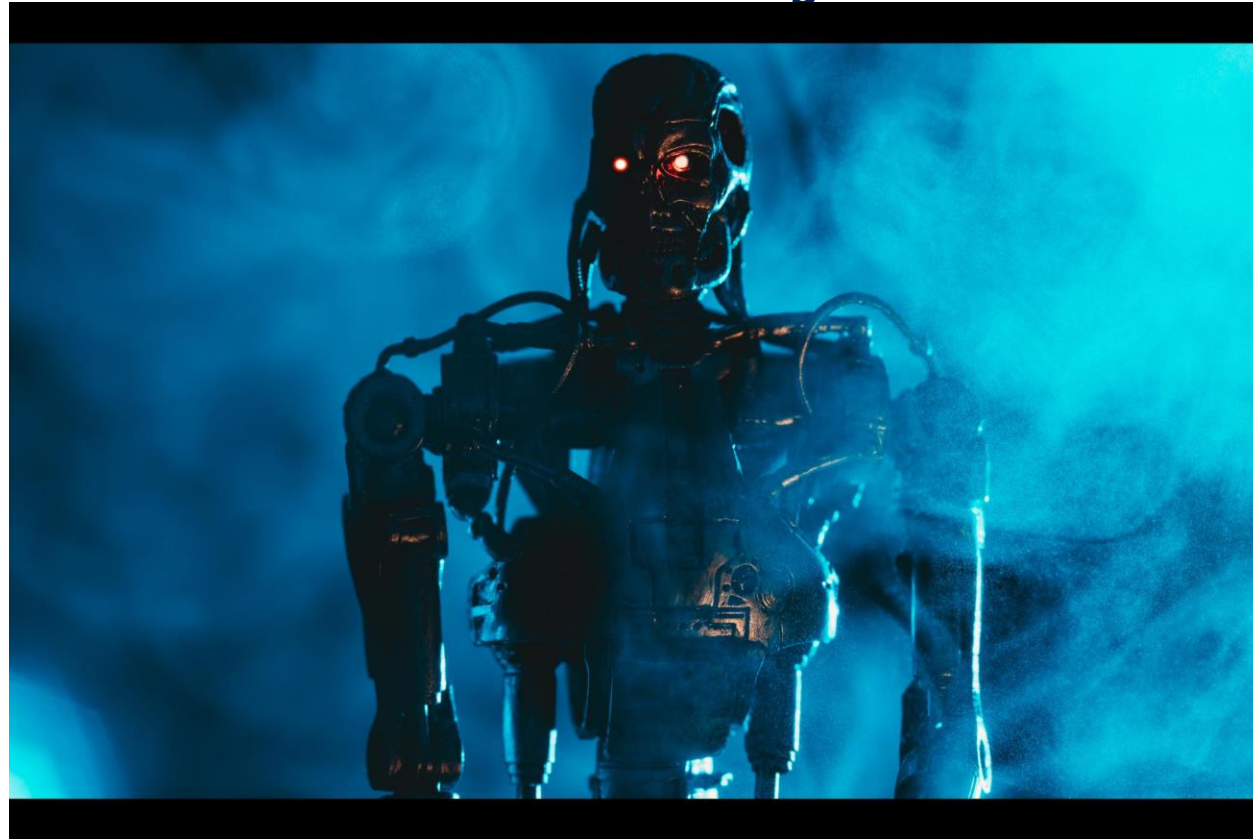
Key Takeaways

- These incidents are not going away and are occurring at an increased operational tempo.
- We need to be vigilant to know what is normal in our day-to-day work and report those things that are not normal.
- Cybersecurity is a team sport. The more resources available make bigger events more manageable.
- You do not need to be in trouble to ask for assistance and resources.



Days to July 11, 2029

993 Days



Thank you!



MCP
Massachusetts
Cybersecurity Program



General Inquiries: mcppol.state.ma.us

Report an Incident: 508-820-2233

