gocyber

COLLECTIVE

October Announcements

- GoCyber Collective Board has been formed.
  - Shawn Waldman - President
  - Kyle Jones – Vice President
  - Gary Estes – Secretary
  - Randy Miller – Treasurer

- Signal App
  - GoCyber Collective will be using Signal to distribute real-time threat intelligence. Signups are available on the tables.

Special Interest Groups

- Special Interest Groups (SIGs)
  - Defense Industrial Base – Led by Dr. Thomas Autry
    - Dr. Autry's presentation will be following this morning's speaker and is open to the entire Collective.
  - Local Government – Led by Darren Davey
    - Meeting for a few minutes in between sessions.
  - Public Safety – Led by Gary Estes
    - Will meet in November following the presentation.

November Presentation

- November 15th the Secure Cyber Defense SOC Team will present on playbooks and how to utilize them. Attendees will also receive playbooks you can use immediately.

SECURECYBER
DEFENSE

Information

Feel free to email us at Admin@gocybercollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

You can register and download past presentations from the website.

- GoCyberCollective.org

Event Sponsors

SECURECYBER DEFENSE

FORTINET®

MY CYBERSECURITY NIGHTMARE

GoCyber Collective | October 2023

SHOOK
CONSTRUCTION

DEFINITIONS

CYBER-CRIME = Any criminal activity that involves a computer, networked device or network whereby one party is harmed or damaged by the intentional, malicious actions of a threat actor.

CYBER-SECURITY = Art of protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity and availability of information.

CYBER-THREAT-ACTOR = A single criminal or group of criminals who orchestrate and execute malicious acts against victims specific to technology-related infrastructures. This is done with the intent to hold the victim ransom for the inequitable return of intellectual assets.

CYBER-VICTIM = Me.

80 – 19 – 1

RULE

shook =YOU

TIME MACHINE

1) HOPE
2) INSURANCE
3) COMMUNICATIONS
4) PLAN
5) FUNDING

TOP 5

1) CLOUD
2) SEXY
3) BACKUPS
4) OUTSOURCE
5) INSURANCE

GRIZZLY BEAR APPROACH

1) Password aging
2) Password complexity
3) Multifactor authentication
4) Separation of duty
5) Ingress-Egress DIA monitoring
6) Mimecast email gateway
7) SIEM
8) Next generation AI-based EDR
9) Manual airgap
10) AWS-Ohio replication
11) AWS-Oregon double replication
12) Cold site
13) Increased staffing
14) Increased Cybersecurity budget
15) Splashtop remote support
16) 1Password credential mgt.
17) CallMultiplier
18) Apple-Microsoft separation
19) Wi-Fi access schedules
20) Wi-Fi segmentation
21) Next-Gen datacenter firewall
22) Next-Gen project firewalls
23) Cybersecurity awareness training
24) Whitecoat phishing campaigns
25) URL filtering

26) MDM
27) Monthly network audits
28) ERP SOC-II hosting
29) Increased Cybersecurity budget
30) Business continuity planning
31) Business communications planning
32) USB device restrictions
33) Zero trust methodology
34) Heavy machine inventories
35) Cyber insurance deep-dive
36) Self-insurance options
37) Turned down Microsoft RDP
38) Eliminated local admin rights
39) Retired traditional Antivirus
40) Offloaded internally hosted websites
41) Poor performing platforms
42) Disable unused ports
43) Phantom networks
44) MAC address filtering
45) Country killer
46) Microsoft AD cloud replication
47) Penetration testing
48) 3rd party Cybersecurity assessment
49) Security-minded culture
50) Dark web roleplay
51) Principle of least privilege
52) Network documentation project
53) Cybersecurity continuing education
54) Cato Networks

QUESTIONS?

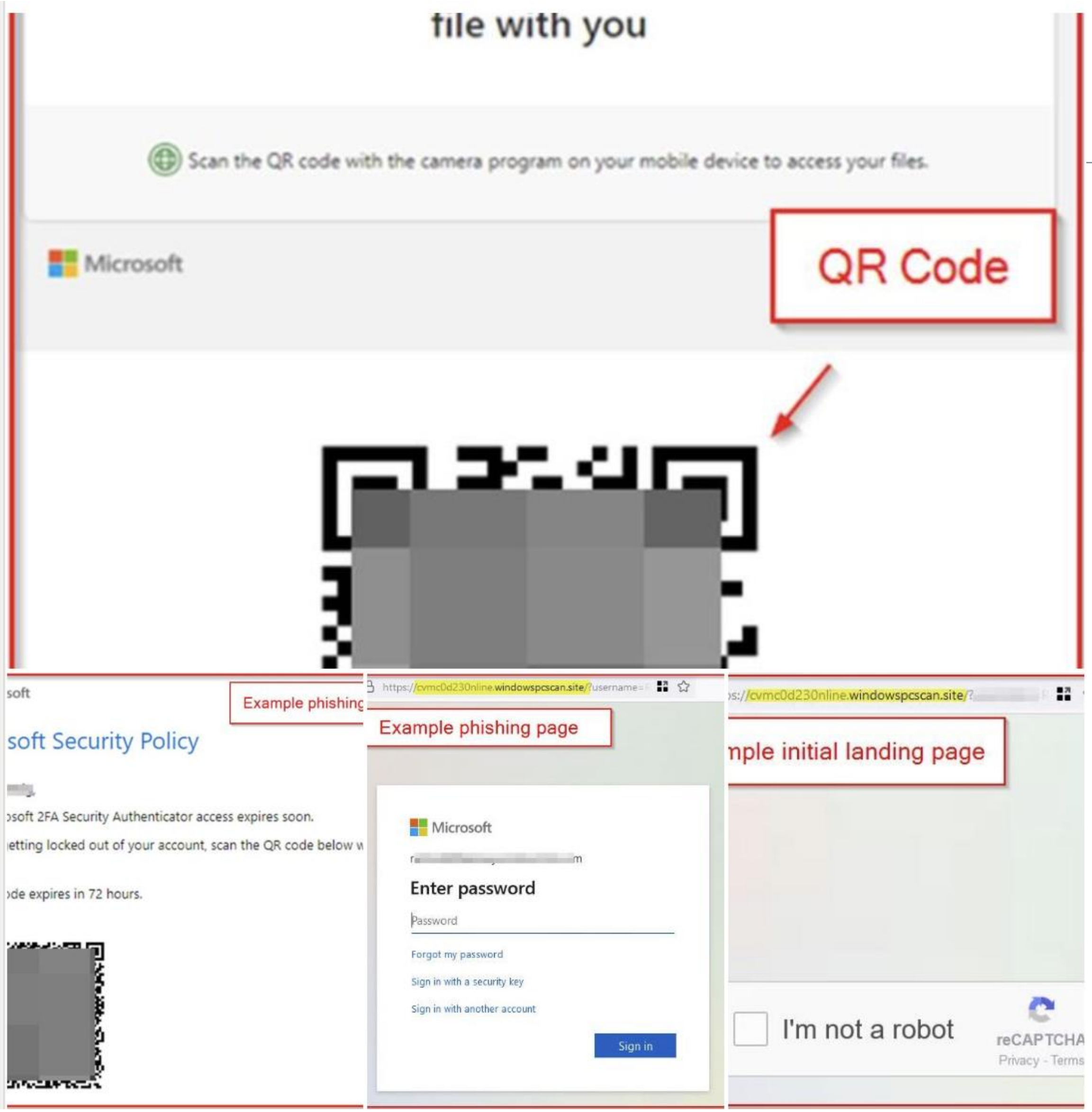
THANK YOU

The Last 2 Weeks In Cyber

THE LAST 2 WEEKS IN CYBER

- Cisco - IOS Vulnerability - ACTIVE Exploit
- Confluence Vulnerability – ACTIVE Exploit
- Multiple Fortinet Vulnerabilities
- Citrix Netscaler - Again
- Apple Security Updates
- NSA-CISA – Top 10 Cyber Misconfigurations
- Microsoft Patches

QR CODE PROBLEMS



file with you

Scan the QR code with the camera program on your mobile device to access your files.

Microsoft

QR Code

soft

Example phishing

soft Security Policy

›soft 2FA Security Authenticator access expires soon.

ıetting locked out of your account, scan the QR code below w

›de expires in 72 hours.

https://cvmc0d230nline.windowspcscan.site/?username=

Example phishing page

Microsoft

Enter password

Password

Forgot my password

Sign in with a security key

Sign in with another account

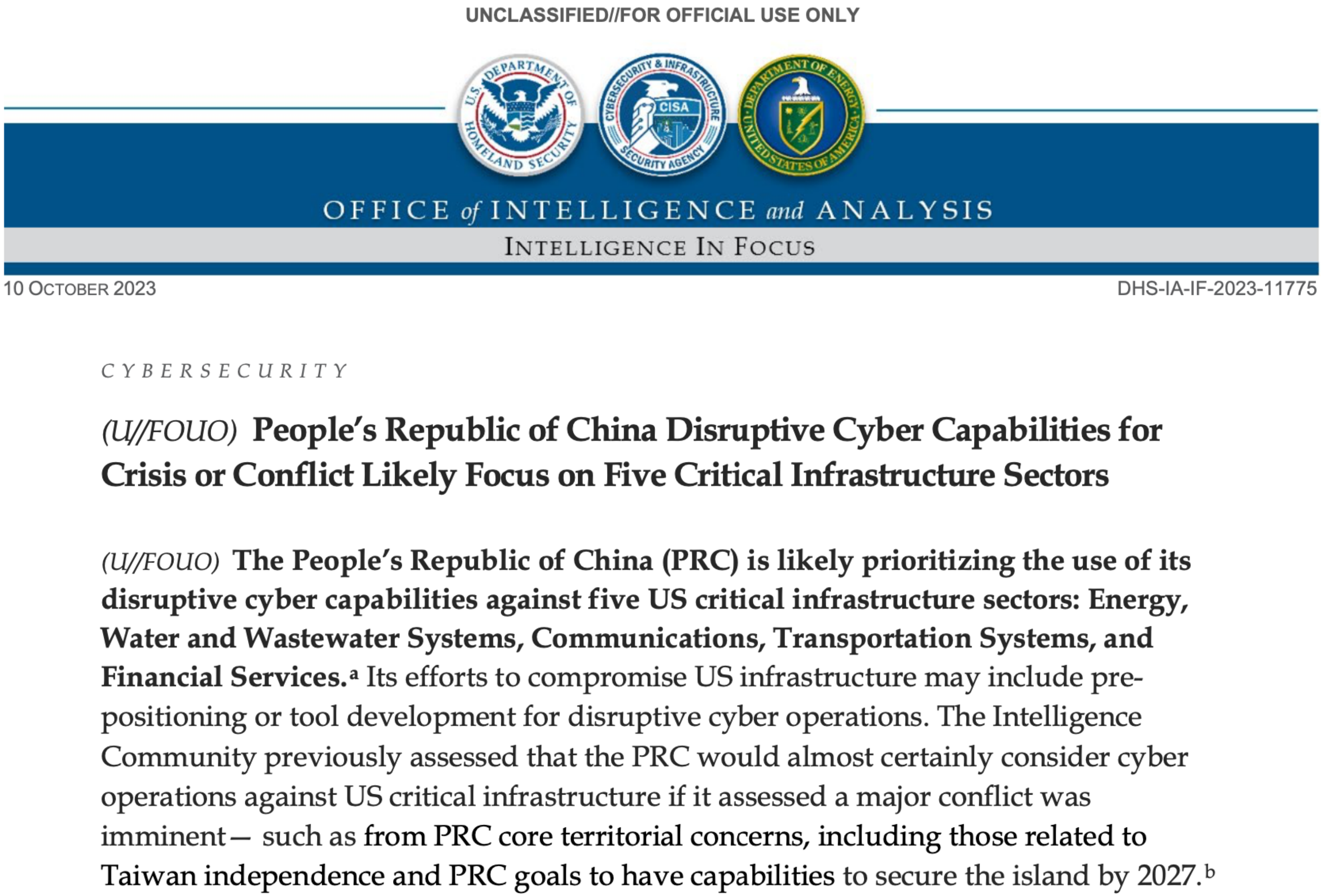
Sign in

s://cvmc0d230nline.windowspcscan.site/?

ıple initial landing page

□ I'm not a robot

reCAPTCHA
Privacy - Terms



UNCLASSIFIED//FOR OFFICIAL USE ONLY

OFFICE *of* INTELLIGENCE *and* ANALYSIS

INTELLIGENCE IN FOCUS

10 OCTOBER 2023

DHS-IA-IF-2023-11775

CYBERSECURITY

(U//FOUO) People's Republic of China Disruptive Cyber Capabilities for Crisis or Conflict Likely Focus on Five Critical Infrastructure Sectors

(U//FOUO) **The People's Republic of China (PRC) is likely prioritizing the use of its disruptive cyber capabilities against five US critical infrastructure sectors: Energy, Water and Wastewater Systems, Communications, Transportation Systems, and Financial Services.**[a] Its efforts to compromise US infrastructure may include pre-positioning or tool development for disruptive cyber operations. The Intelligence Community previously assessed that the PRC would almost certainly consider cyber operations against US critical infrastructure if it assessed a major conflict was imminent— such as from PRC core territorial concerns, including those related to Taiwan independence and PRC goals to have capabilities to secure the island by 2027.[b]

THREATS FROM CHINA / CRITICAL INFRASTRUCTURE

- » Energy
- » Water and Wastewater
- » Communications
- » Transportation
- » Finance

CISCO IOS VULNERABILITY

» DON'T ENABLE ADMIN ACCESS REMOTELY

» THERE IS NO PATCH AVAILABLE YET

» **SHOW RUNNING-CONFIG | INCLUDE IP HTTP SERVER|SECURE|ACTIVE**

» **LOOK FOR IP HTTP SERVER RUNNING**

» **LOOK FOR IP HTTP SECURE-SERVER**

NSA TOP 10 RECOMMENDATIONS

1. DEFAULT CONFIGURATIONS OF SOFTWARE AND APPLICATIONS
2. IMPROPER SEPARATION OF USER/ADMINISTRATOR PRIVILEGE
3. INSUFFICIENT INTERNAL NETWORK MONITORING
4. LACK OF NETWORK SEGMENTATION
5. POOR PATCH MANAGEMENT
6. BYPASS OF SYSTEM ACCESS CONTROLS
7. WEAK OR MISCONFIGURED MULTIFACTOR AUTHENTICATION (MFA) METHODS
8. INSUFFICIENT ACCESS CONTROL LISTS (ACLS) ON NETWORK SHARES AND SERVICES
9. POOR CREDENTIAL HYGIENE
10. UNRESTRICTED CODE EXECUTION