
go
cyber
COLLECTIVE

April Announcements

Serving Our Communities

Thank you, William Cornett!

Law enforcement served well – 101 and 201 a success!

SparkSprints: Spoofing – May 20th (after Monthly Meeting)

Inside SOC: Critical Blue Team Operations

Cyber for Local Gov't Exec. Leadership – July 21

Incident Response plan is LAW! Get your action plan and playbook

gocyber COLLECTIVE

Digital Transformation Center

gocyber COLLECTIVE

SPOOFING

May 20, 2026
9:45 AM to Noon

Signal Domain Threat Role Play

Scenario 1

Aviation

Flight path manipulation

HIGH RISK

Scenario 2

Maritime

Position deception

ACTIVE

CRITICAL

GPS

Position Alteration

Scenario 3

ELEVATED

Power Grid

Infrastructure Targeting

Scenario 4

GoCyber Collective 201 Tyler Way Moraine 45439

SparkSprints: Spoofing

GEOIntel exercise → Wednesday, May 20th, 2026 → 9:45 AM – 12:00 PM (right after GoCyber meeting)

FREE!!! → Great team-building exercise → Lunch provided

Register today!

gocyber COLLECTIVE

Inside the SOC: Critical Blue Team Operations

- Wednesday July 8th, 2026
- 9 AM – 3:30 PM
- Identify: How attacker gained access, moved through environment, explored systems
- $999

Cyber for Local Government Executive Leadership - One-Day Workshop Registration

Cyber for Local Government Executive Leadership

- Tuesday July 21st
- 8:00 AM – 4:30 PM
- Take Aways:

  -Recognize significance of cybersecurity

  -Role of leadership to maintain security

  -Understand/implement cyber hygiene

  -Importance of audits/regular training

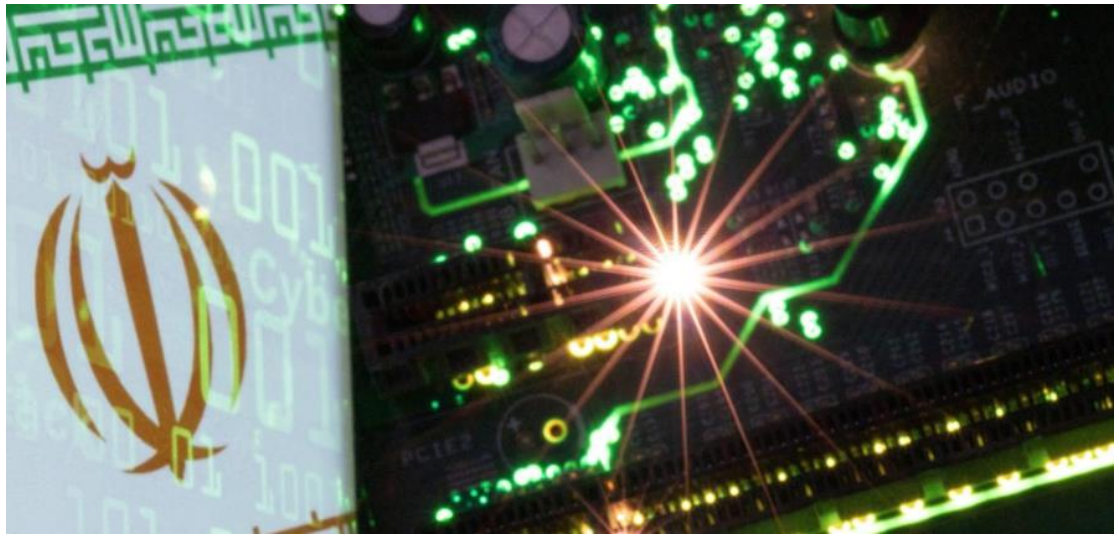
  -Comprehensive role of insurance roles

  -Requirements under new state law
- Donuts, coffee, & lunch provided
- $499

April Threat Briefing

- James Fisher
  - -SecureCyber
  - -Director of Security Ops

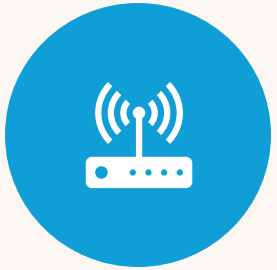
Iran Threat Briefing



Potential Targets

US MILITARY ASSETS

US TECHNOLOGY COMPANIES



ENERGY AND CIVILIAN INFRASTRUCTURE

CYBER AND DIGITAL INFRASTRUCTURE

Recent Stories

Stryker

US medical tech firm

Microsoft Intune management console

Personal Email

FBI Director

Lockheed Martin

Staff information

State-Sponsored APT Groups

MuddyWater
Alias Earth Vetala, Mango Sandstorm, Seedworm, Static Kitten, MERCURY, and TA450

APT34 (OilRig/Helix Kitten)

APT33 (Elfin / Refined Kitten)

APT35 (Charming Kitten / Phosphorus / Magic Hound)

Hacktivist Proxy Groups

Handala
CyberAv3ngers
Cyber Islamic Resistance

https://attack.mitre.org/groups/

Top Vulnerabilities and Attack Vectors Exploited

Microsoft Exchange / ProxyShell
APT35 primarily targets Microsoft Exchange servers through ProxyShell exploitation chains combined with Autodiscover and EWS services to extract Global Address Lists, which then become the foundation for targeted phishing campaigns that harvest credentials.

Edge Infrastructure (VPNs, Citrix, ManageEngine, PaperCut)
Internet-facing infrastructure including Exchange, VPNs, Citrix, ManageEngine, and PaperCut are repeatedly exploited, as Iranian actors target newly disclosed edge vulnerabilities rapidly after disclosure.

Password Spraying against Cloud Identity (Entra ID / M365)
APT33 has shifted heavily toward large-scale Microsoft 365 and Entra ID password spraying, while APT34 continues to stand out for DNS tunneling and Exchange- or cloud-based C2.

Vulnerable Cameras and ICS/OT Devices
Marshtreader (Agrius) was observed scanning for vulnerable cameras using CVE-2023-6895 and CVE-2017-7921 across Israel, using infrastructure associated with Iranian actors.

Social Engineering and Credential Phishing
Iranian threat actors have demonstrated strong social engineering capabilities, including spear-phishing campaigns and "honeytrap" operations used to build relationships with targets of interest to gain access to accounts or sensitive information.

ClickFix / PowerShell Lures
A password-spraying attack conducted from Nord VPN infrastructure against Israeli municipal government entities was followed by spear-phishing attacks containing links to a ClickFix page designed to trick users into executing malicious PowerShell to deliver a remote access tool.

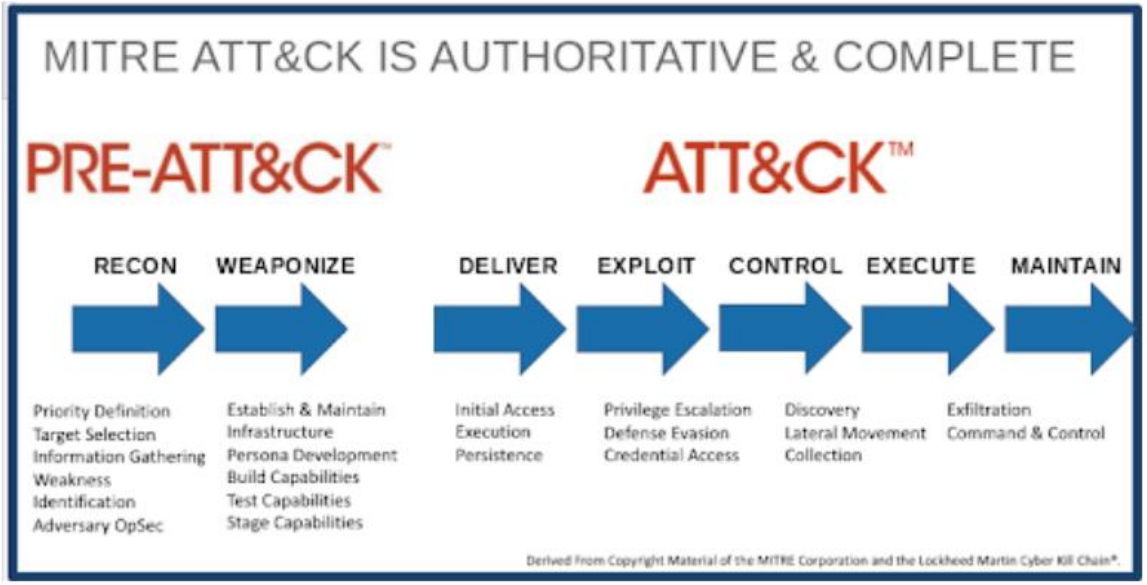
Initial Access

T1566 – Phishing / Spearphishing: Shamoon variants used spearphishing to gain initial access, eventually relying on the Eldos RawDisk driver to bypass Windows APIs and overwrite the master boot record (MBR).

T1190 – Exploit Public-Facing Application: Agonizing Serpens frequently exploited publicly available one-day vulnerabilities in public-facing web applications to drop custom web shells.

T1078 – Valid Accounts / Default Credential Abuse: Early-stage tactics observed include default credential abuse, valid account exploitation, brute force attacks, and network reconnaissance, signaling that adversaries are mapping environments to identify high-value assets.

T1110.003 – Password Spraying: Groups demonstrate increased centralized planning through the establishment of an "Electronic Operations Room," using brute force style social-engineering and spear-phishing tactics. Specific TTPs include password spraying and multifactor authentication "push bombing" to compromise user accounts.



Fog of War

“Fog of war" is the uncertainty, confusion, and limited situational awareness experienced by commanders and soldiers during military operations, often caused by inaccurate, incomplete, or misleading information. Coined in the 1830s by Carl von Clausewitz, it highlights the chaotic nature of battle, where accurate decision-making is inhibited.

Cybercrime has skyrocketed 245% since the start of the Iran war

Iran's False Flag Operation Claims

What can we do?

Technical

Audit environments for weak credentials
Audit credentials for access (least privileged)
Limit scope and permissions of admin accounts
Ensure your edge devices are updated
Enroll in vendor security release notifications
Application and vendor audit
Immutable backups
Limit unattended access
Review security tools directly for alerts
Block all unapproved remote support tools (RMM)
    Anydesk,Screen Connnect
Verify logging
Verify logging retention time
Eyes on security tools

Non- Technical

See Something Say something

Tabletop exercises
    Comprised edge device
    Loss of admin control

April GoCyber Collective Keynote Speaker

-Marc Ricker – iVALT

-The Identity Verification Game Changes Now

iVALT

Provable Human Authority

Closing the Execution Gap in Zero Trust

Patents:
8 Granted | 10+ Pending

April 2026

iVALT

Attackers Don’t Break In. They Log In.

HUMAN AUTHORITY is Never Proven Before Execution

80-90% of Attacks Start with Stolen Credentials

iVALT

A Broken Model → AI Scales Risk Exponentially

Why It Fails

→ Credential-Based Identity is Broken Everywhere

→ IAM Was Not Designed for AI or Autonomous Execution

→ Authority is Never Verified at Execution

A Human Authority Control Plane is Required

iVALT

Provable Human Authority

Cryptographic Proof Before Execution

The Human Proof Model

Biometrics → **Identity**

PKI (Mobile) → **Device Binding**

GPS + Time → **Context**

Eliminates the Risk of Inherited Authority

iVALT

Human Authority Checkpoints

No Changes to IAM or AI Infrastructure

Enforce Human Authority at Execution — Ends Stolen Credential Fraud

On-Demand ID™

Verified Identity at Both Ends of the Conversation

Employees & Customers

Trusted Help Desk &

Customer Interactions

iVALT

Representatives and ChatBots

Stops Social Engineering and AI Deepfakes

Unverified Actors Blocked

DocuID®

Ultimate Document Security

Enterprise • SaaS • AI Sources

Originator Defines Recipients & Access

iVALT

Human-Bound Identity Embedded in Every Document

(At Save / Encryption)

Inside & Outside the Enterprise

Access Enforced Everywhere

Originator Controls Access Forever

iVALT

Provable Human Authority — Key Takeaways

- Control Risk at the Only Place It Matters — Execution
- Prove Human Authority Before Every Critical Action
- **No Infrastructure Changes → Immediate Control**
- Enterprise-Ready Today

Closes IAM Identity Gaps → Secures AI Execution at Scale

iVALT

The Future of Identity

Thank you!

Marc Ricker
EVP Business Development
Marc.ricker@ivalt.com
+1 216.570.7411

Brian Stout
Co-Founder and CPO
brian@ivalt.com
+1 719.964.9650

Download Our App and Test On-Demand ID

Download on the App Store

GET IT ON Google Play

www.iVALT.com
info@ivalt.com

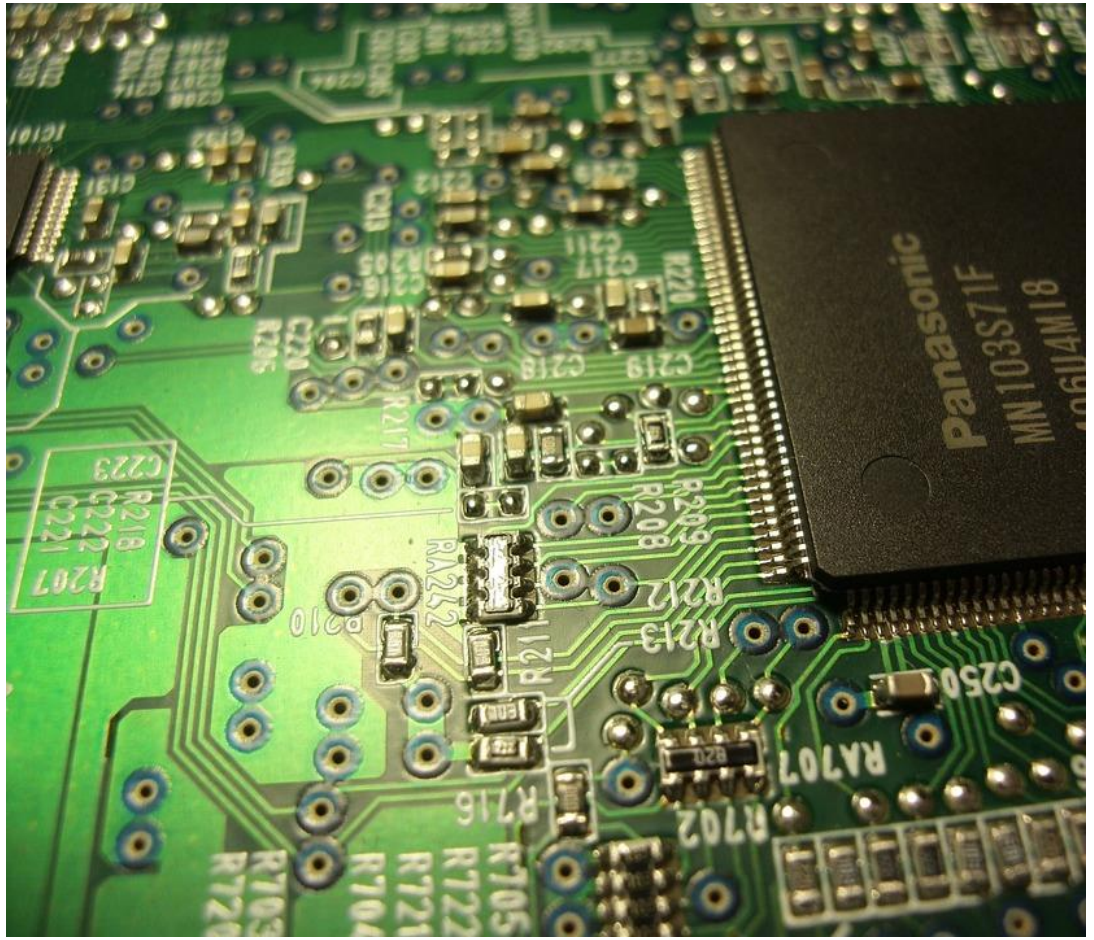
May Meeting:

- Netta Squires – Open District Solutions
- President of Gov't Affairs, Cybersecurity & Resilience
- Exec. Director: Center for Critical Infrastructure Security
- Securing Infrastructure

gocyber COLLECTIVE

April Parting Shots

- Local Gov't/Public Safety SIG – Sun Watch Room
- Education SIG – Wright Patt Room
- Defense Contractor SIG – Hawthorn Room
- Register for Workshop, Monthly Meetings
- Turn in your lanyards at the desk



gocyber COLLECTIVE

Information

Email me at john@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 for future breakfast meetings from the website.

- GoCyberCollective.org

Event Sponsors