State of Cybersecurity

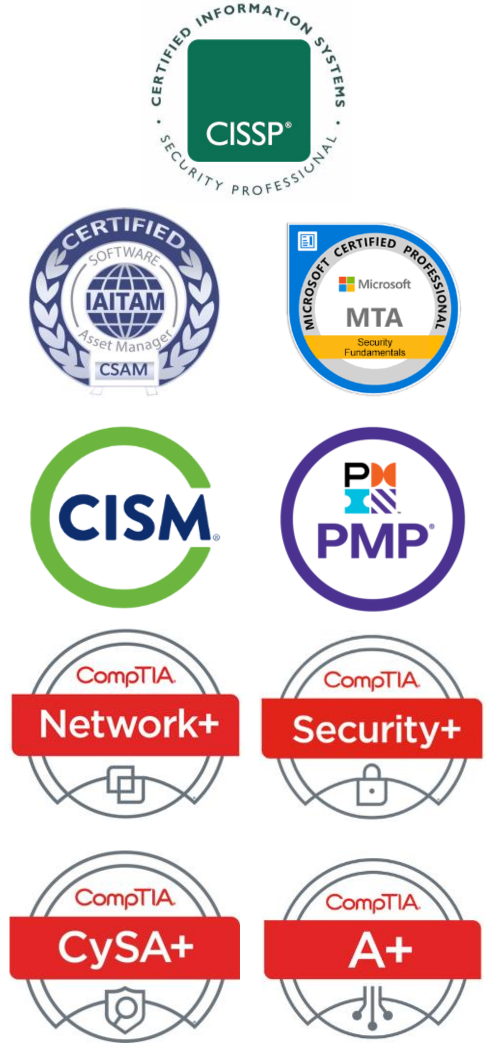
Supporting the Orange County Transportation Authority's (OCTA) mission by protecting OCTA networks, systems, and the confidentiality of data through effective Identification, Protection, and Response.

Cybersecurity Team Members

Well-qualified cybersecurity team, comprised of 6 employees

Third-party 24x7 managed security operations center (SOC) monitor and escalate cyber alerts to the core team

Collective Employee Certifications


CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®
CERTIFIED SOFTWARE IAITAM Asset Manager
CSAM
MICROSOFT CERTIFIED PROFESSIONAL
Microsoft
MTA
Security Fundamentals
CISM
PMI
PMP®
CompTIA
Network+
CompTIA
Security+
CompTIA
CySA+
CompTIA
A+

Top 2024 Cybersecurity Threat Themes

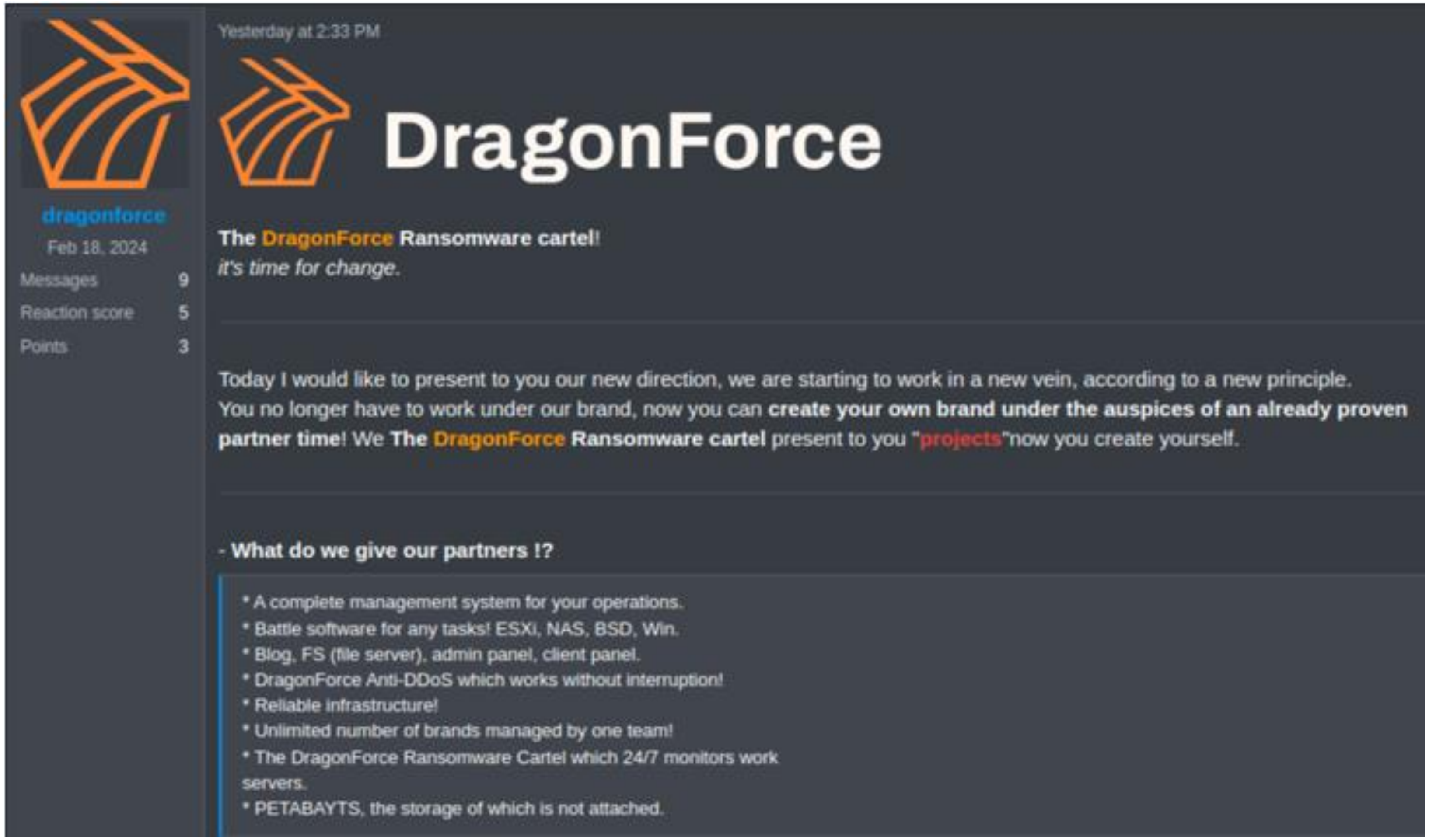
- Ransomware-as-a-Service (RaaS)
- Supply Chain Attacks
- Identity Attacks & MFA Gaps
- Cloud Environment Exploitation
- Exploitation of Zero-Day Vulnerabilities
- AI-Enhanced Threats
- Cybersecurity Workforce & Talent
- Critical Infrastructure

Organized Crime, Cartels, Terrorism, Nation-State, and Geopolitical Adversaries

Increased Executive and Board Focus on Resilience and Recovery

AI – Artificial Intelligence
MFA – Multi-Factor Authentication

Ransomware-as-a-Service (example)



dragonforce

Feb 18, 2024

Messages	9
Reaction score	5
Points	3

Yesterday at 2:33 PM

The DragonForce Ransomware cartel!

it's time for change.

Today I would like to present to you our new direction, we are starting to work in a new vein, according to a new principle. You no longer have to work under our brand, now you can **create your own brand under the auspices of an already proven partner time**! We **The DragonForce Ransomware cartel** present to you "projects"now you create yourself.

- What do we give our partners !?

* A complete management system for your operations.
* Battle software for any tasks! ESXi, NAS, BSD, Win.
* Blog, FS (file server), admin panel, client panel.
* DragonForce Anti-DDoS which works without interruption!
* Reliable infrastructure!
* Unlimited number of brands managed by one team!
* The DragonForce Ransomware Cartel which 24/7 monitors work servers.
* PETABAYTS, the storage of which is not attached.

(literal text)

"Today I would like to present to you our new direction, we are starting to work in a new vein, according to a new principle. You no longer have to work under our brand, now you can **create your own brand under the auspices of an already proven partner time**! We **The DragonForce Ransomware cartel** present to you "**projects**" now you create yourself.

2024 Cybersecurity Department Achievements

Incident Response

- Improved technical disaster recovery documentation
- Implemented many new real-time behavioral alerts and triggers
- Performed an External Pen-Test
- Enforced password resets and replaced laptop / desktops if users were duped by phishing attacks

Vulnerability Management

- Consolidated IT inventory into two primary repositories allowing faster access to asset data
- Accelerated vulnerability patching
- Enhanced our patching exception documentation and included mitigating control analysis

Identity & Access Management

- Performed several types of user access reviews
- Removed administrative access as much as possible

Risk & Governance

- Performed automated breach attack simulations
- Conducted third-party risk assessments
- Aligned IT controls with NIST CSF industry framework

Security Awareness

- Conducted live AI trainings / webinars
- New user licenses are provisioned with pre-recorded user trainings
- Created an AI acceptable use policy
- Increased company-wide security newsletter

IT – Information Technology
National Institute of Standards and Technology (NIST)
Cybersecurity Framework (CSF)

2025 Anticipated Adversarial Tactics

More of the same, plus…

- Destructive Ransomware
- Advanced Exploit Chaining
- Abuse of Legitimate Software Features
- More Malware-less Attacks
- Increased SaaS Exploitations
- Cloud Infrastructure Exploitation
- Data Warehouse Campaigns
- Continued Network Perimeter Targeting

Abuse of valid user accounts is still the primary preferred entry method across all tactics

2025 Cybersecurity Department Focus

Data Privacy & Data Protection Program

- Reduce our sensitive data attack surface; reduce liability
- Automated sensitive data scanning across the enterprise
- Implement Privacy-by-Design processes for new projects
- Privacy Steering Committee to help identify potential privacy risks before projects start

Enhanced Identity Protection

- AI-based system automation to detect:
  - Unauthorized privilege escalation
  - Compromised user passwords
  - Suspicious lateral movement
- Improve identity hygiene
- Proactive Threat Hunting

Advanced Anti-Phishing Features

- AI-based phishing and Business Email Compromise (BEC) attack detection and prevention
- AI-based end user phishing simulation tests that adapt to end user testing behaviors

Consolidated Cyber Ecosystem

- Eliminate complexity of supporting multiple security tools
- Shared intelligence to improve threat detection
- Built-in AI-based threat prevention