SECURECYBER
DEFENSE

July 2023 Threat Briefing – GoCyber Collective

ENGAGE
FORTINET ADVANCED PARTNER
Integrator

HOT
TOPICS

SCD Israel Winter Delegation
February 2024
Tel-Aviv Israel

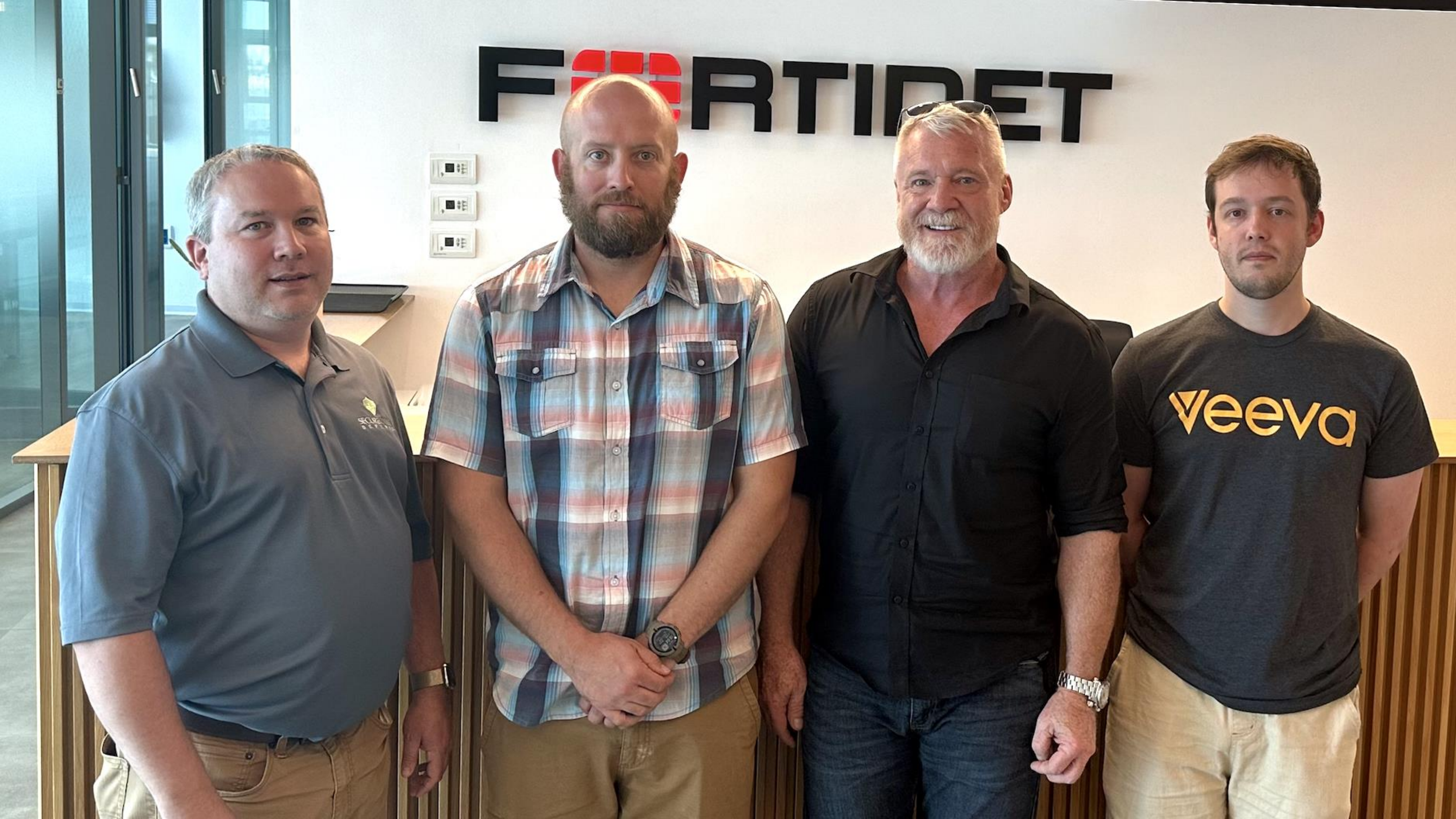
- Centered Around CyberTech 2024
- 1-2 Days of Israel Cyber Startups
- Custom Israel Gov't Site Visits
- International Cyber Discussions
- Family's welcome – Tours Available
- Delegation Site Seeing
- Network Internationally

Contact Shawn Waldman
swaldman@secdef.com
937-802-7521

Since 1954
Fender
STRATOCASTER
VIGAT

4,705,229
3,745
452,021
583
96,582
1995
5089
SYDNEY JERUSALEM NEW YORK
17:50 10:50 3:50
LUNDHALSEY

splunk>enterprise
Standard views
Apps
SOC Overview
Hunting
SOC Inbound Status 24h
IPS (FW) - External Attacks
IPS - External Attacks - Timeline by Category
FW Inbound traffic
WAF - Inbound Attacks High Severity over Time
Anti-DDOS
4,705,229
3,745
ATTACK ORIGINS
ORIGIN
China
Brazil
Israel
Argentina
Indonesia
Pakistan
Iran
Jordan
Albania
Japan
ATTACK VECTORS
DESCRIPTION
914
54
47
28
2
2
1
Check Point - Geo-locado.
Check Point - SSL Enforce
Check Point - Streaming
McAfee - DROP
Check Point - SSL and TL
McAfee - ICMP: Timestan
McAfee - P2P: QQLive Pr
ATTACK TARGETS
TARGET
LIVE ATTACK FEED
TIMESTAMP
SYDNEY JERUSALEM NEW YORK
17 50 10 50 3 50
LUNDHALSEY



FORTINET
veeva

IDE
Technologies
IDE

July - News Roundup

- Oracle Releases Critical Updates - Oracle Critical Patch Update Advisory - July 2023
- Citrix Releases Updates for ADC - Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467
- Multiple Critical Infrastructure Vulnerabilities
  - CISA Releases Seven Industrial Control Systems Advisories | CISA
  - CISA Releases Nine Industrial Control Systems Advisories | CISA
  - CISA Releases One Industrial Control Systems Advisory | CISA
  - CISA Releases Four Industrial Control Systems Advisories | CISA
- Adobe Cold Fusion Updates - Adobe Security Bulletin
- Cisco Vulnerabilities with SD-WAN API - Cisco SD-WAN vManage Unauthenticated REST API Access Vulnerability
- Juniper Fixes Vulnerabilities - Search (juniper.net)
- CISA Releases Guidance on Securing O365 - CISA and FBI Release Cybersecurity Advisory on Enhanced Monitoring to Detect APT Activity Targeting Outlook Online | CISA
- Microsoft Patch Updates July 2023 - July 2023 Security Updates - Release Notes - Security Update Guide - Microsoft

July - News Roundup

- Oracle Releases Critical Updates - Oracle Critical Patch Update Advisory - July 2023
- Citrix Releases Updates for ADC - Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467
- Mozilla Updates - Security Vulnerabilities fixed in Firefox 115.0.2 and Firefox ESR 115.0.2 — Mozilla
- Increased TruBot Activity - CISA and Partners Release Joint Cybersecurity Advisory on Newly Identified Truebot Malware Variants | CISA
- Apple Updates - Apple Releases Security Updates for Multiple Products | CISA
- VMWare Updates - VMSA-2023-0014 (vmware.com)
- Sierra Wireless – Victim of Ransomware Attack
- Priority Dispatch – Release of Ransomware Attack Data
- Trend – Endpoint Isolation and Containment

Questions?

Archive

Threat Briefing – What SCD is Seeing

- Office365
  - Mis-configurations
  - Wrong package level (need E5 for logging and advanced features)
  - No MFA (Not all accounts are getting covered)
  - Lack of use of compliance and auditing features

SCD Recommends

- ✓ Use O365 auditing tools like Secure Score
- ✓ Use CISA SCUBA Tool
- ✓ Use CIS O365 Baseline Doc
- ✓ Secure O365 (Under 300 Users)
- ✓ Secure O365 (Over 300 Users)
- ✓ How to setup MFA

February 2023 Intel

February - News Roundup

- ➢ PayPal Accounts Breached Due to Password Recycling
- ➢ US Government No Fly List Leaked
- ➢ Microsoft Patch Tuesday – February Edition
- ➢ Another Experian Glitch Exposes Credit Files for 47 Days
- ➢ New T-Mobile Breach Affects 37 Million Accounts
- ➢ OneNote Malicious Emails - .1 Files/Qakbot Ransomware
- ➢ CISA – A number of Critical Controls vulnerabilities
- ➢ Chick-fil-A Breach

February - News Roundup

- Apple ZeroDays
- Twitter MFA Change
- Clam AV Vulnerability (Cisco and many other products)
- Earthquake Phishing Scams (Turkey and Syria)
- Fortinet Vulnerabilities
- Stop Ransomware – DPRK Espionage Activities
- ESXiArgs Ransomware
- Gmail – Finland Server Issues

February - Fifteen Industrial Control System Advisories

- ICSA-23-047-01 Siemens Solid Edge
- ICSA-23-047-02 Siemens SCALANCE X-200 IRT
- ICSA-23-047-03 Siemens Brownfield Connectivity Client
- ICSA-23-047-04 Siemens Brownfield Connectivity Gateway
- ICSA-23-047-05 Siemens SiPass integrated AC5102/ACC-G2 and ACC-AP
- ICSA-23-047-06 Siemens Simcenter Femap
- ICSA-23-047-07 Siemens TIA Project Server
- ICSA-23-047-08 Siemens RUGGEDCOM APE1808
- ICSA-23-047-09 Siemens SIMATIC Industrial Products
- ICSA-23-047-10 Siemens COMOS
- ICSA-23-047-11 Siemens Mendix
- ICSA-23-047-12 Siemens JT Open, JT Utilities, and Parasolid
- ICSA-23-047-13 Sub-IoT DASH 7 Alliance Protocol
- ICSA-22-298-06 Delta Electronic DIAEnergie (Update B)
- ICSMA-23-047-01 BD Alaris Infusion Central

March 2023 Intel

March - News Roundup

- FBI chief details exactly how TikTok could threaten national security | Cybernews
- Ongoing - Ransom gang leaks trove of sensitive data from City of Oakland attack | Cybernews
- Cybersecurity Strategy Released Biden-Harris cybersecurity strategy explained | Cybernews
- Abandon LastPass - Why you should leave LastPass | Cybernews
- Sensitive US military emails exposed for two weeks in the wild | Cybernews
- Water ISAC DCOM Alert for SCADA WaterISAC Releases Advisory for Microsoft DCOM Patch | CISA
- CISA issues LockBit 3.0 Guidance #StopRansomware: LockBit 3.0 | CISA
- 8 new Industrial Controls vulnerabilities CISA Releases Eight Industrial Control Systems Advisories | CISA
- Bank Related SCAMS - Beware of Bank-Related Scams | CISA

March - News Roundup

- March Patching
- SANS Briefing InfoSec Handlers Diary Blog - SANS Internet Storm Center
- Patch Tuesday Dashboard - https://patchtuesdaydashboard.com
- Known Exploited Vulnerability Catalog - Known Exploited Vulnerabilities Catalog | CISA
- AskWoody - March madness here we come @ AskWoody
- SpaceX Ransomware - LockBit brags: We'll leak thousands of SpaceX blueprints stolen from supplier • The Register (ampproject.org)

March - Fifteen Industrial Control System Advisories

- ICSA-23-075-01 Siemens SCALANCE, RUGGEDCOM Third-Party
- ICSA-23-075-02 Siemens RUGGEDCOM CROSSBOW V5.3
- ICSA-23-075-03 Siemens RUGGEDCOM CROSSBOW V5.2
- ICSA-23-075-04 Siemens SCALANCE W1750D Devices
- ICSA-23-075-05 Siemens Mendix SMAL Module
- ICSA-23-075-06 Honeywell OneWireless Wireless Device Manager
- ICSA-23-075-07 Rockwell Automation Modbus TCP AOI Server
- ICSA-22-342-02 AVEVA InTouch Access Anywhere and Plant SCADA Access Anywhere (Update A)

April 2023 Intel

April - Fifteen Industrial Control System Advisories

- ICSA-23-108-01 Omron CSCJ Series
- ICSA-23-108-02 Schneider Electric Easy UPS Online Monitoring Software
- ICSA-23-017-02 Mitsubishi Electric MELSEC iQ-F, iQ-R Series (Update B)
- ICSA-19-346-02 Omron PLC CJ and CS Series (Update B)
- CVE-2019-8526 Apple macOS Use-After-Free Vulnerability
- CVE-2023-2033 Google Chromium V8 Engine Type Confusion Vulnerability

April - News Roundup

- ➢ Juice Jacking - FBI issues warning about "juice jacking" when using free cell phone charging kiosks (msn.com)
- ➢ Microsoft Patch Updates - Microsoft Patch Tuesday, March 2023 Edition – Krebs on Security
- ➢ IRS Tax Scams - IRS Warns of New Tax Scams | CISA
- ➢ CISA Added 2 new vulnerabilities to the Known Exploited Vulnerabilities - CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
- Apple MacOS
- Google Chrome
- ➢ FortiNet Advisories - April 2023 Vulnerability Advisories | FortiGuard
- ➢ March Ransomware Record Broken - March 2023 broke ransomware attack records with 459 incidents (bleepingcomputer.com)
- ➢ Lockbit seen targeting MAC's - LockBit ransomware encryptors found targeting Mac devices (bleepingcomputer.com)
- ➢ Update on FBI's Infragard

May 2023 Intel

May - News Roundup

- WhatsApp Encrypts Chats - WhatsApp now lets you lock chats with a password or fingerprint (bleepingcomputer.com)
- Microsoft Releases May 2023 Security Updates - Microsoft Releases May 2023 Security Updates | CISA
- Microsoft's May 2023 Release Notes - May 2023 Security Updates - Release Notes - Security Update Guide – Microsoft
- SANS Microsoft Patch Breakdown - InfoSec Handlers Diary Blog - SANS Internet Storm Center
- Krebs On Security Patch Breakdown - Microsoft Patch Tuesday, May 2023 Edition – Krebs on Security
- CISA Warns of critical Ruckus Wi-Fi Bug - CISA warns of critical Ruckus bug used to infect Wi-Fi access points (bleepingcomputer.com)
- Pharmercica Breach - Ransomware gang steals data of 5.8 million PharMerica patients (bleepingcomputer.com)

Current Threats

- BianLian Ransomware Group

• Strictly limit the use of RDP and other remote desktop services.
• Disable command-line and scripting activities and permissions.
• Restrict usage of PowerShell and update Windows PowerShell or PowerShell Core to the latest version.

Current Threats

- VMWare
- Babuk Leads the Way
- Lockbit 3.0
- Royal

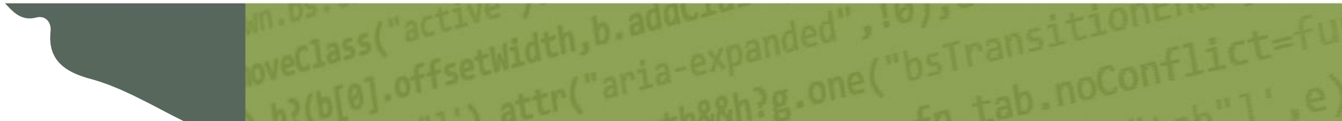
FCC’s Covered List

- Contains List of Banned Vendors
- Secure and Trusted Communications Networks Act of 2019
- **Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, AO Kaspersky Lab, China Mobile International USA Inc., China Telecom (Americas) Corp., China Unicom (Americas) Operations Limited**

SCD Israel Summer Delegation 2023 June 23-30 Tel-Aviv Israel

- Centered Around CyberWeek 2023
- 2 Days of Israel Cyber Startups
- Custom Israel Gov't Site Visits
- International Cyber Discussions
- Family's welcome – Tours Available
- Delegation Site Seeing
- Network Internationally

Contact Shawn Waldman
swaldman@secdef.com
937-802-7521



May - Industrial Control System Advisories

- ICSA-23-136-01 Snap One OvrC Cloud
- ICSA-23-136-02 Rockwell ArmorStart
- ICSA-23-136-03 Rockwell Automation FactoryTalk Vantagepoint

June 2023 Intel

June - News Roundup

- Asus Critical Router Vulnerabilities - ASUS urges customers to patch critical router vulnerabilities (bleepingcomputer.com)
- Over 100,000 compromised from Chat GPT - Over 100,000 ChatGPT accounts stolen via info-stealing malware (bleepingcomputer.com)
- Priority Dispatch Impacted by Breach - LockBit 3.0 Ransomware Victim: prioritydispatch[.]net - RedPacket Security
- Fortinet Vulnerability - Analysis of CVE-2023-27997 and Clarifications on Volt Typhoon Campaign | Fortinet Blog
- Barracuda Vulnerability – Replace the device? - Barracuda Urges Replacing — Not Patching — Its Email Security Gateways – Krebs on Security
- CLOP Ransomware, Lockbit3.0 - Understanding Ransomware Threat Actors: LockBit | CISA
- Ride in DDoS Attacks
- MoveIt File Transfer Vulnerability - Progress Software Releases Security Advisory for MOVEit Transfer Vulnerability | CISA

July 2023 Intel