November 9, 2023

International Conflict in 2024: Forecasting its Practical Impact on Data Security

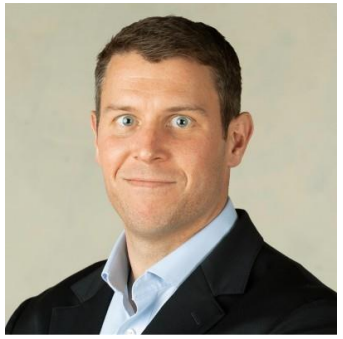
Brendan Rooney
Booz Allen Hamilton

Will Durkee
Axis Insurance

Patrick McNally, Esq.
Octillo

Privacy+ Security Forum

Speakers



Brendan Rooney

Vice President, Global Commercial IR
Booz Allen Hamilton

Patrick McNally, Esq.

Partner
Octillo

Will Durkee

Senior Cyber Advisor
Axis Insurance

Current Events

Situational Awareness

Privacy+ Security Forum

Current Events – Situational Awareness

Privacy+ Security Forum

Nation-State Adversaries

- Destructive Activity
  - Several forms of wiper malware created and used in foreign conflict(s)
- Intellectual Property Theft
  - IP theft at an all-time high per warnings from Five Eyes Intelligence Alliance
- Financial Motivation
  - Certain nations providing a safe-harbor for ransomware actors, questions arisen in ties to criminal operators to evade sanctions imposed on foreign jurisdictions.

Recent Geo-Political Activity

- Russia-Ukraine War
  - Several forms of wiper malware leveraged by Russian operators
  - Attacks against Ukrainian utilities
  - Russian spear-phishing campaigns to gather military intelligence
  - Criminal groups taking political sides
- Israel-Hamas War
  - Public defacement of websites, billboards and hacktivist involvement
  - Disinformation campaigns conducted by Hamas militants
  - Iranian and Russian groups targeting Israeli critical infrastructure

Current Events – Situational Awarenss

Privacy+ Security Forum

Criminal Operators

- Increase in Ransomware Activity
  - Substantial increase in ransomware activity beginning mid-Q3 and Q4 to date
  - Diverse population of groups involved with prior operators re-emerging in early Q4 (TimisoaraHackingTeam “THT” and others)
  - Broadening of affiliate base lowering barrier to entry, attracting novice actors
    - LockBit 3.0
    - Akira
    - PLAY
    - Vice Society
    - GNN (Group No Name)

Critical Infrastructure

- Criminal Operators
  - Exploitation of public facing applications, ransomware and email compromise activity are primary drivers for financially motivated criminal organizations
  - Criminals have easier access to hyper-volumetric, VM-based botnets to conduct large scale DDoS campaigns
- Nation-State Adversaries
  - Destructive malware observed in Russia-Ukraine War pose substantial risk to utilities providers and critical infrastructure at-large

Observations

Nation-State & Criminal Overlay

Privacy+ Security Forum

National-State & Criminal Overlay

Privacy+ Security Forum

Supply Chain Compromise

Russian State-Sponsored group Sandworm & Cyclops Blink botnet affects WatchGuard firewall firmware installed via malicious update, FBI takedown of Cyclops Blink C2 04.06

Phishing Campaigns

CERT-UA alert pertaining to phishing campaigns against Ukrainian military personnel

Ransomware

Conti ransomware group issues first statement supporting RU citizens. CoomingProject and Stormus announce support of Russian government. LockBit group expresses neutrality

DDoS Attacks

Multiple DDoS attacks against Ukrainian websites and infrastructure. Hacktivist groups like Anonymous get involved

Destructive Wiper Malware

HermeticWiper, Hermetic Wizard, HermeticRansom, IsaacWiper, CaddyWiper, RURansom, ORCSHRED, SOLOSHRED, AWFULSHRED and many more…

Supply Chain Compromises

HAFNIUM MS Exchange vulnerabilities, Kaseya, Accellion FTA Compromises, Log4Shell RCE CVE

Phishing Campaigns

Used by many ransomware groups to harvest user and admin credentials, a substantial number of ransomware deployments begin with phishing emails

Ransomware

Despite suppressed ransomware activity in Q1 2022 due to ongoing conflict and successful law enforcement takedowns, activity has quickly increased in early Q2 2022, old groups such as Sodinokibi are now back

DDoS Attacks

A constant threat posed by ransomware groups like LockBit, Royal and others, a favorite of extortion groups such as FancyLazarus

Destructive Wiper Malware

Dates as far back as Shamoon malware in the Saudi Aramco attack in 2012, given its recent increase in use, criminal groups may adapt to their playbooks

What's Next?

Looking ahead to 2024

Privacy+ Security Forum

What's Next?

Privacy+ Security Forum

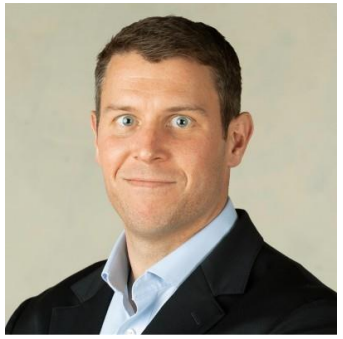
1. **Predicting the future – is it possible?**

2. **How will this impact privacy and security regulations in the next year?**

3. **How will this affect the private sector in the U.S. and abroad – and what practical steps can you take to mitigate risk?**

Speakers

Privacy+ Security Forum



Brendan Rooney

Vice President, Global Commercial IR
Booz Allen Hamilton

Rooney_Brendan@bah.com

Patrick McNally, Esq.

Partner
Octillo

pmcnally@octillolaw.com

Will Durkee

Senior Cyber Advisor
Axis Insurance

Will.Durkee@axiscapital.com