Connection®
we solve IT®

Frontline Cybersecurity: Trends, Impacts, and Zero-trust Insights

November 2024

Agenda

- Introduction
- 2024 Attack Vector Trends and Landscape
- Findings Summary of a Security Event
- Zero-trust Lessons Learned Post-event

Introduction

John Chirillo is currently a Principal Security Architect at Connection in the Security Center of Excellence. He's a seasoned ethical hacker, programmer, and author of several books. He specializes in IT Governance Frameworks and Managed Compliance using AIOps.

Rob Di Girolamo is a Senior Security Architect at Connection in the Security Center of Excellence. He is an experienced cybersecurity professional with specialized interests in vulnerability management, zero-trust security architectures, and security program development.

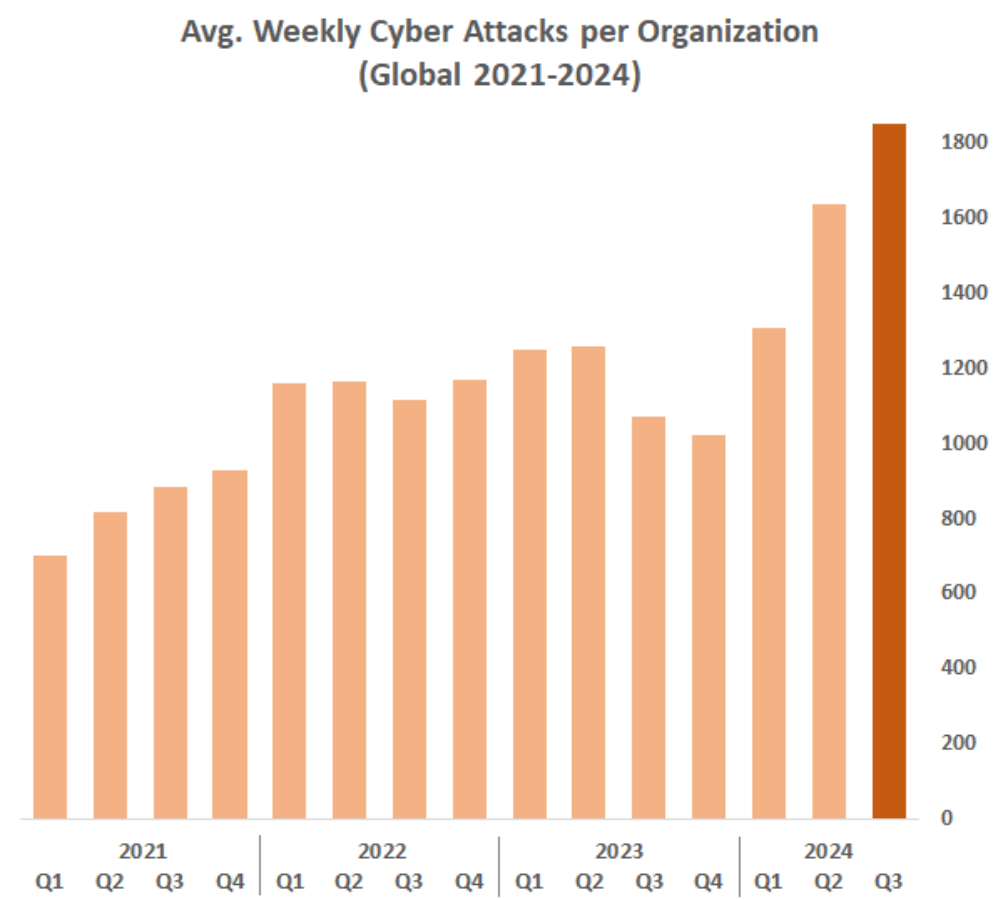
Pamela Kennedy is a Cybersecurity Engineer working with Government, Healthcare, and Financial Services sectors in service management, cybersecurity, compliance, and audit. She specializes in providing advisory services to organizations looking to strengthen their internal controls in order to meet regulatory requirements.

Kevin Knapp is an accomplished Director of Technology and Senior Cybersecurity Engineer with 28 years of experience in Information Technology, excelling in key skills such as, strategic planning, team leadership, and project management. He has proven success in risk management and remediation for numerous Fortune 500 companies.

Attach Vector Trends and Landscape

Key Trends in 2024:

- Increased Sophistication of Ransomware Attacks
- Rise in Cloud-based Attacks
- AI-enhanced Cyber Threats
- Increased Targeting of Critical Infrastructure
- Supply Chain and Vendor Attacks
- Identity-based Attacks



Increased Sophistication of Ransomware Attacks

Ransomware Evolution:

- 73% increase in ransomware attacks from 2022 to 2023
- Evolution to “double extortion” and “triple extortion” tactics
- Example: McLaren Health Care attack in August 2024

…a cyber attack crippled systems at its 13 hospitals throughout Michigan, Indiana, and Ohio…
Aug. 5 through Aug. 27

Rise in Cloud-based Attacks

Cloud-based Attacks:

- 75% increase in cloud intrusions
- Targeting of cloud-conscious adversaries, especially eCrime actors
- Example: Breach of Toyota North America's cloud infrastructure in August 2024

Data size: *240GB*
Contents: *Contacts, finance, customers, schemes, employees, photos, databases, network infrastructure, emails, and a lot of perfect data. We also offer you AD-Recon for all the target network with passwords.*

AI-enhanced Cyber Threats

Attacks with Gen AI:

- Use of generative AI for more convincing social engineering, including deceptive deepfake audio and video
- AI-powered malware creation and deployment
- Example: Sophisticated phishing campaign against U.S. government officials using AI-generated content

This looks like Tom Cruise doing a coin trick, but it's actually a deepfake created by Chris Umé.
From TikTok

Increased Targeting of Critical Infrastructure

Critical Infrastructure Targeting:

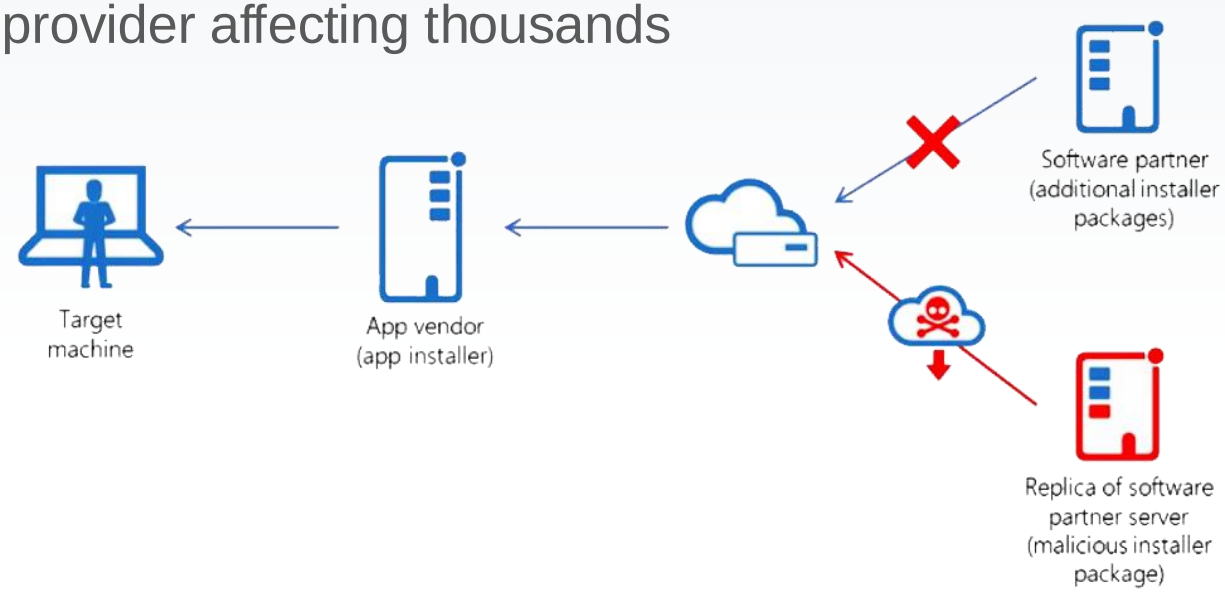
- Focus on energy, healthcare, and government sectors
- Geopolitical motivations behind many attacks
- Example: Danish power grid attack by Russian hackers

Denmark's critical infrastructure experienced the largest cyberattack in the country's history this spring, with 22 energy companies breached in just a few days.

Supply Chain and Vendor Attacks

Rising Supply Chain/Vendor Attacks:

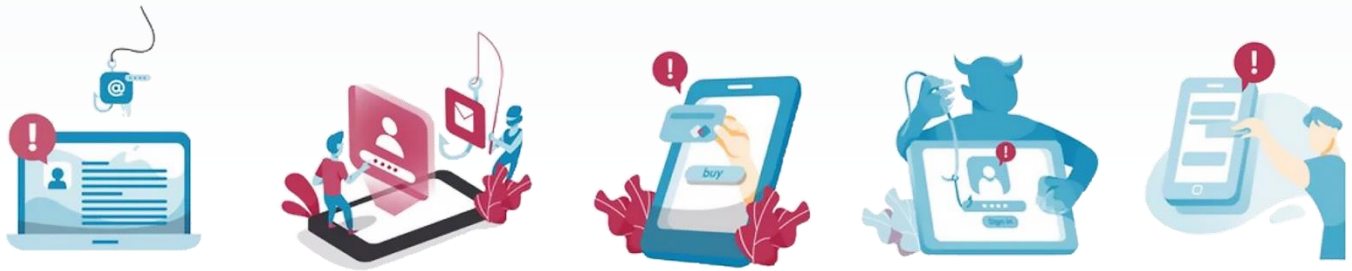
- Exploiting vendor-client relationships for maximum impact
- Compromising software supply chains
- Example: SolarWinds-style attack on a major IT service provider affecting thousands



Identity-based Attacks

Identity Threats:

- Attackers are using sophisticated methods
- Stealing or bypassing authentication
- Examples: SIM-swapping, MFA bypass, and stolen API keys



Trends in 2024: Key Take-aways

Identity Threats:

- Multi-layered security approach has never been greater
- Employee training is crucial
- Zero Trust:
  - Identity and privileged access
  - Management should be a top priority
- Cloud security needs special attention
- Have a solid incident response plan in place
- Stay informed about the latest threats and trends

Findings Summary of a Security Event

The Ghost in the Machine: Analysis of a Sophisticated Cyber Attack

I. Introduction

- Timeline: March 11–April 4 analysis
- Wave Browser: Not traditional malware, but not harmless

II. Wave Browser Behavior

- Initially classified as: Adware and Evader
- Key actions: Pop-up ads, new tabs, link redirects, browser modifications
- Connection to api.wavebrowserbase.com for ad injection
- Installation without elevated privileges or user consent

III. Patient Zero Analysis

- Dell micro desktop (Windows 10)
- Extensive log analysis: Endpoint security, DNS, firewall
- January 2: Entry-point was email (personal) via low-rated phish

IV. Entry Point and Vulnerabilities

- Malicious ad in phishing email
- Existing n-day vulnerabilities, several CVEs

V. Malware Analysis Findings

- 55 threat intelligence sources used
- 4 files identified as low-to-medium risk (PUPs and grayware/adware)

VI. Network Activity

- Multiple domains accessed (wavebrowser.com, wavebrowserbase.com, etc.)
- Automatic updates via swupdater.com (AWS-hosted)

VII. Key Concerns

- Personal web browsing/email as entry point
- China-hosted malware repository connections and escreen RMM access

Lessons Learned Post-event

So, what can we learn from this event?

- **Personal web browsing and email use on work devices can be a significant security risk.** In this case, all reported Wave Browser installations were sourced from personal Gmail or Yahoo mail use.
- **Keeping systems updated is crucial.** The vulnerabilities present on the affected desktop made it an easy target.
- **User awareness is key.** The initial infection likely came through a phishing email, highlighting the importance of cybersecurity training for all staff.
- **Regular security assessments are invaluable.** This deep dive allowed us to understand the full scope of the Wave Browser incident and take appropriate action.
- **Layered security measures work.** While Wave Browser slipped through initial defenses, our endpoint detection and response tools, along with thorough log analysis, allowed us to detect and respond to the threat.
- **Zero Trust.** Create a robust zero-trust architecture that enhances security by ensuring that every access request is thoroughly vetted, regardless of its origin.
  - Identity Access Management helps control user access to information.
  - Privileged Access Management is for protecting users with elevated rights.
  - Unified Endpoint Management is for centrally managing, securing, and provisioning resources.

What Were the Consequences from This Event?

Financial Impacts:

- Direct cost was ~ $300k.
- Lost revenue due to service disruptions and operational downtime for 4 weeks.
- Increased cybersecurity insurance premium rose by ~ 26%.

Human Impacts:

- Disruption to patient care, including delayed treatments, delayed surgeries, and inability to access and transfer patient records.
- Stress and increased workload for healthcare and IT staff dealing with the aftermath of attacks and implementing workarounds.
- Some reported job losses due to organizational financial and operational strain.
- Erosion of trust between patients and healthcare provider, potentially leading to patients avoiding or delaying necessary care.
- Delayed advancements in patient treatments and therapies.

Thank You!

Learn more at
connection.com/Cybersecurity

Or call 1.800.998.0067 to
start the conversation with
a Connection expert today.

Connection
we solve IT