How Cybersecurity Professionals are Combating AI-Enabled Malware: State of Cybersecurity with AI and Zero-Trust

Opportunities for Cybersecurity Professionals

Artificial Intelligence (AI) has emerged as a powerful tool for innovation and a challenge for cybersecurity professionals. With ever-evolving AI-powered malware, cybersecurity professionals are meeting the threat head-on by evolving their strategies and tactics to counter and proactively defend their security infrastructures through zero-trust, early detection, and investment into quantum capabilities. Leading the way are those deploying AI-counter technology measures.

AI-Powered Detection

How Gen-AI Can Help:[1]

- Accelerate threat detection
- Create quick incident summaries
- Automate security operations tasks
- Simulate attacks

44% of organizations globally use AI to detect security intrusions[2]

AI-Powered Defense

Areas defensive AI is expected to deliver the biggest impact:[1]

61% Cloud security

50% Data security

46% Network security

Growing Cybersecurity Trends

Artificial Intelligence

76% of enterprises are prioritizing AI and machine learning in their IT budgets[2]

70% business executives will deploy Gen AI tools for cyber defense within the next 12 months[3]

50%+ of security professionals believe that GenAI will greatly impact the security field compared to other types of AI[1]

Zero Trust

66%+ of organizations are implementing zero-trust policies[4]

2/3 of organizations worldwide have begun to implement a zero-trust strategy[1]

Post-Quantum Cryptography

98% expected growth of post-quantum cryptography by 2034, totalling more than $17 billion[5]

Threats to Cybersecurity's Critical Infrastructure

Cybercriminals are taking advantage of the evolving AI landscape and advancing the technologies in their tool belt to exploit vulnerabilities across an array of platforms, ecosystems, and infrastructures.

Attackers are increasing their capabilities to bypass conventional threat detection methods using AI-empowered malware, exploiting IoT devices, and attacking supply chains.

AI-Powered Malware Threats

3/4 of organizations feel the impact of AI-powered security threats[1]

85% of cybersecurity leaders believe their company's sensitive data is in jeopardy due to evolving AI technologies[6]

74% of security leaders across an array of global industries witness their organizations being impacted by AI-powered cyber threats[1]

43% of security professionals predict AI-powered threats will evade traditional detection techniques[7]

(IoT) Threats

107% increase in IoT malware in 2024. And, a 30% growth in malware across all ecosystems[8]

45% growth in IoT malware attacks between 2023 and mid-2024 [9]

Mirai and Gafgyt malware families pose the biggest threat to IoT[9]

10x/day home networks devices are attacked 10 times on average every day[10]

Supply Chain Threats

73% of operation technology professions (OT) experienced intrusions that impacted their OT systems in 2024, up 24% from 2023[11]

Polymorphic Threats

94% of malware today is polymorphic[12]

Top Industries Under Attack

Year-over-Year increase in published ransomware attacks by sector:[13]

+56% Manufacturing

+27% Healthcare

+31% Govt./Military

Top 3 most attacked industries were:[13]

1. Education/Research (3,341 attacks per week)
2. Government/Military (2,084 attacks per week)
3. Healthcare (1,999 attacks per week)

How Connection Can Help

Connection is your partner for modern infrastructure and cybersecurity solutions and services. From hardware and software to consulting and customized solutions, we're leading the way in infrastructure modernization.

Explore our Solutions and Services

Malware Analysis
Modern Infrastructure
Cybersecurity

Contact an Expert

1.800.998.0067

Sources:

1. Darktrace, 2024, State of AI Cybersecurity
2. Tech Magic, 2024, AI in Cybersecurity, Exploring the Top 6 Use Cases
3. PWC, 2024 Global Trust Insights
4. IBM, 2024, What is Zero Trust?
5. Global Newswire, 2024, Post-Quantum Cryptography Market Research Report 2024
6. Code 42,2024, Annual Data Exposure Report 2024
7. Palo Alto, 2024, The State of Cloud-Native Security 2024 Report
8. Sonicwall, 2024, Sonicwall Mid-Year Cyber Threat Report
9. Zscaler, 2024, 7 Takeaways from IBM's Cost of a Data Breach Report 2024
10. Netgear, 2024, Every 24 Hours, Home Networks See an Average of 10 Attacks. Is Your Network Secure?
11. Fortinent, 2024, State of Operational Technology and Cybersecurity
12. Wiley Online Library, 2023, Metamorphic Malware and Obfuscation: A Survey of Techniques, Variants, and Generation Kits
13. Check Point Research, 2024, Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks

Connection
we solve IT