Navigating Today’s Cyber Threats and Protecting Tomorrow’s Technologies

Dmytro Sirosh, Cloud Chapter Security principal @ Tietoevry

26 November 2024

Agenda

Corporate level threats

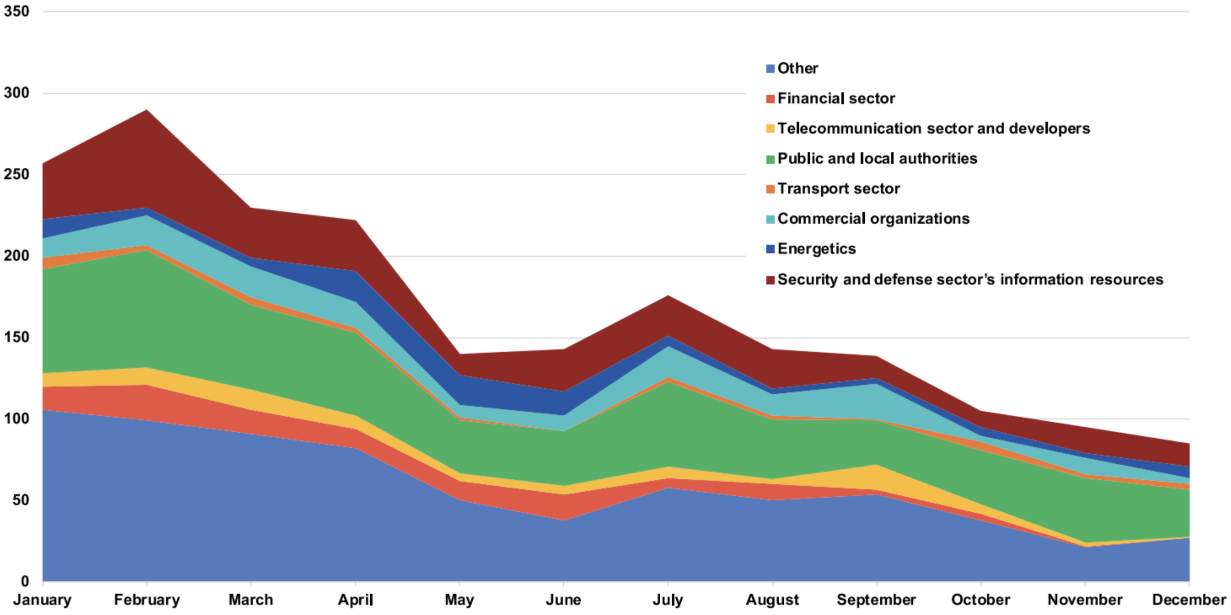
1. CERT-UA statistics for 2022
2. Categories of threats
3. Infopulse by Tietoevry corporate Security incidents dynamics
4. How Identity protection can contribute?
5. Breaking Down Phishing Risks: The Role of Email in Cyber Threats
6. Security awareness VS Email phishing
7. No Security incidents – No pain
8. Key Security Challenges to address with SOC

Nationwide threats in cyber warfare

9. Manipulation of public information
10. The Impact of Fake News on Public Trust and Democracy
11. Ethical and Security Risks of AI in Warfare
12. Building Trust Through Transparent Information Campaigns
13. Mitigating Risks of LLM Model Manipulation

CERT-UA statistics for 2022

- Overall statistics of cyber incidents and cyberattacks registered and investigated by the Computer Emergency Response Team for Ukraine (CERT-UA) has reached **2,100 over the year** and above 1,500 since the beginning of the full-scale military invasion.
- It is not military but **civil infrastructure** that has been the primary target for russian hackers throughout the year.

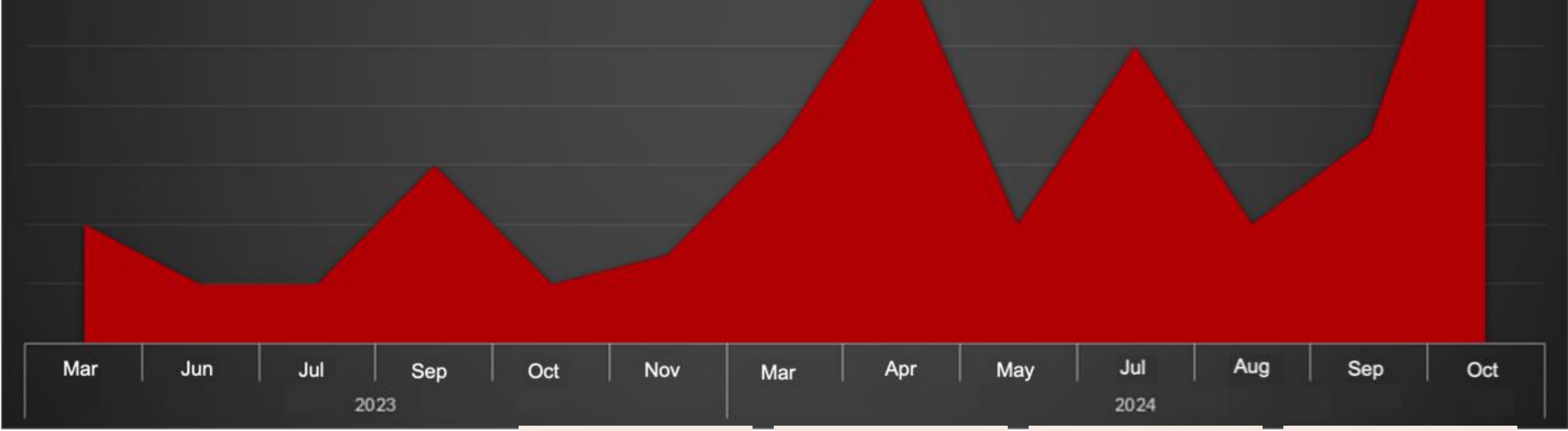


until December 15

Categories of threats

The reported incidents are categorized broadly as follows:

1. **Destructive Malware Attacks**: Russia has frequently used wiper malware, designed to irreversibly erase data, as a primary tactic.
2. **Phishing and Social Engineering**: Phishing, often impersonating trusted entities such as CERT-UA and government departments, is another highly common attack vector.
3. **Supply Chain Attacks**: Attacks on Ukraine’s energy sector through compromised software suppliers have been detected, aiming to infiltrate critical infrastructure indirectly via trusted vendors. The telecom sector and software providers, key to public and private communication, are frequently targeted in these supply chain attacks.
4. **Ransomware Attacks**: CERT-UA has also identified several ransomware attacks disguised under the guise of wiper malware.



Infopulse by Tietoevry corporate Security incidents dynamics

Number of malicious campaigns has significantly grew starting 2022

Email phishing incidents

Instant messenger phishing

Malware attacks

Identity compromise attempts

How Identity protection can contribute?

Conditional access for everyone

- Enable MFA for all users not only privileged ones.
- SMS-based MFA is not secure anymore. Use App-based MFA or security keys.

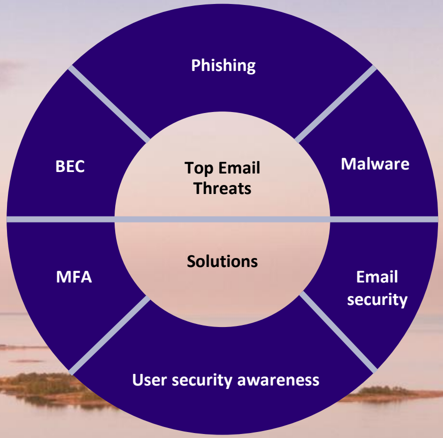
Discover and remediate permission risks

- Work with least privileges by default
- Use Privileged Access Management (PAM) to escalate privileges when they are needed

User activity monitoring and anomaly detection

- User and entity behavior analytics (UEBA) to automatically protect against identity compromise
- Get Security operations center (SOC) in place to monitor and response the threats

Breaking Down Phishing Risks: The Role of Email in Cyber Threats



Phishing in Cyber Incidents: In 2023, phishing emerged as one of the most prevalent tactics in cyber incidents, responsible for approximately 41% of cases, and contributing to data breaches and security incidents.

Increase in Credential Phishing: In 2023, credential phishing attacks increased by 67%, fueled by attackers' intent to gain access to sensitive accounts and data in corporate settings.

Malware Distribution through Email: Around 94% of all malware is spread via email, highlighting the critical need to protect email channels from phishing and harmful attachments.

Spear Phishing Techniques: In 2023, 62% of phishing attacks involved malicious attachments, while 33% used harmful links. This shift towards attachment-based attacks highlights the evolving strategies to evade detection.

Security awareness VS Email phishing

Human Error is the Weakest Link

- Employees are the primary target of phishing attacks.
- Training helps employees recognize phishing tactics and avoid falling victim.

Improved Detection of Phishing Attempts

- Employees learn to spot suspicious emails, such as fake sender addresses or malicious attachments.
- Trained employees can identify and avoid phishing attempts more effectively.

Behavioral Change and Reporting

- Training fosters a culture of reporting suspicious emails quickly.
- Faster identification and reporting minimize potential damage.

Cost-Effectiveness and Long-Term Impact

- Security awareness training is a low-cost, high-impact solution.
- It prepares employees for evolving threats, reducing the reliance on technical defenses alone.

No Security incidents – No pain

212 days to det Data breach in companies allows attackers to conduct lateral movements and carry out more extensive attacks

Ransomware Attack on a Healthcare Provider

A healthcare provider's delayed detection and response to a ransomware attack led to extensive data encryption and prolonged service disruption, due to inadequate continuous monitoring. This allowed attackers to exploit vulnerabilities and cause significant damage.

Data Breach in a Financial Institution

A significant financial institution encountered a data breach that remained unnoticed for weeks due to an inactive or improperly integrated alerting system. This delay in identifying the breach resulted in the theft of sensitive customer information, leading to regulatory fines and harm to the institution's reputation.

Insider Threat at a Technology Company

An insider infiltrated a tech company and accessed confidential data. Due to inadequate monitoring, the breach remained undetected for months, leading to substantial intellectual property theft.

Failure to Detect Phishing Attacks

The company did not identify several phishing attacks that led to the compromise of multiple email accounts. The absence of proactive monitoring and an incident response plan allowed the attackers to gain unauthorized access to essential systems.

Uncontrolled Cloud Security Incident

A company with essential cloud infrastructure did not detect security misconfigurations until a significant breach took place. The absence of continuous alert monitoring enabled attackers to exploit vulnerabilities for weeks.

Slow Response to an External Cyberattack

A company suffered a cyberattack that compromised several systems. Due to inadequate monitoring, the response team took days to detect the attack, allowing the attackers to inflict significant damage.

Loss of Customer Data Due to Malicious Activity

A telecom company did not implement continuous monitoring, resulting in an extended period of unauthorized access. During this time, attackers were able to extract customer data for several months before the breach was discovered.

Vendor Networks Compromised by Supply Chain Attack

A supply chain attack infiltrated a large corporation’s network via an unsecured third-party vendor. The breach went undetected for an extended period due to inadequate alert systems, exacerbating the impact and extending the duration of the breach.

Key Security Challenges to address with SOC

Protecting Business Reputation

Compliance with Regulatory Requirements

Adapting to Changing Threat Landscape

Minimize downtimes

Mitigating Supply Chain Risks

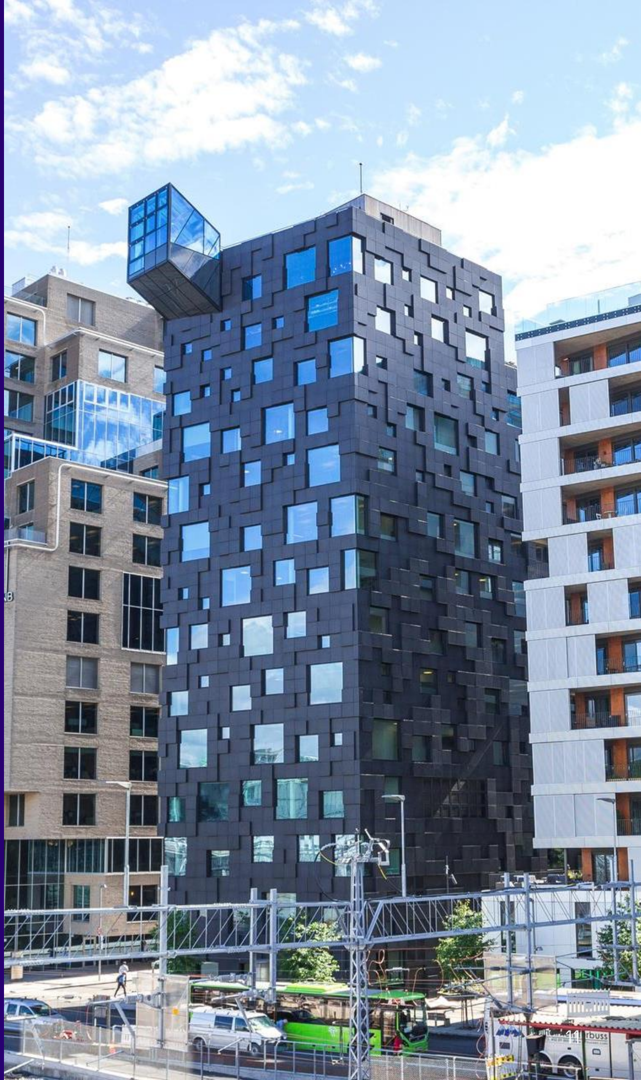
Resource and Skill Gaps

Cut down reaction time

Maintaining Competitive Advantage

Reducing the Risk of Financial Loss

Nationwide threats in cyber warfare



Manipulation of public information

Russian Disinformation Campaigns

- Russia has used disinformation to justify its invasion of Ukraine.
- False narratives include portraying the invasion as a “special military operation” for peacekeeping.
- The Kremlin spreads fabricated claims about Ukrainian atrocities and Nazi influences.

Social Media as a Battlefield

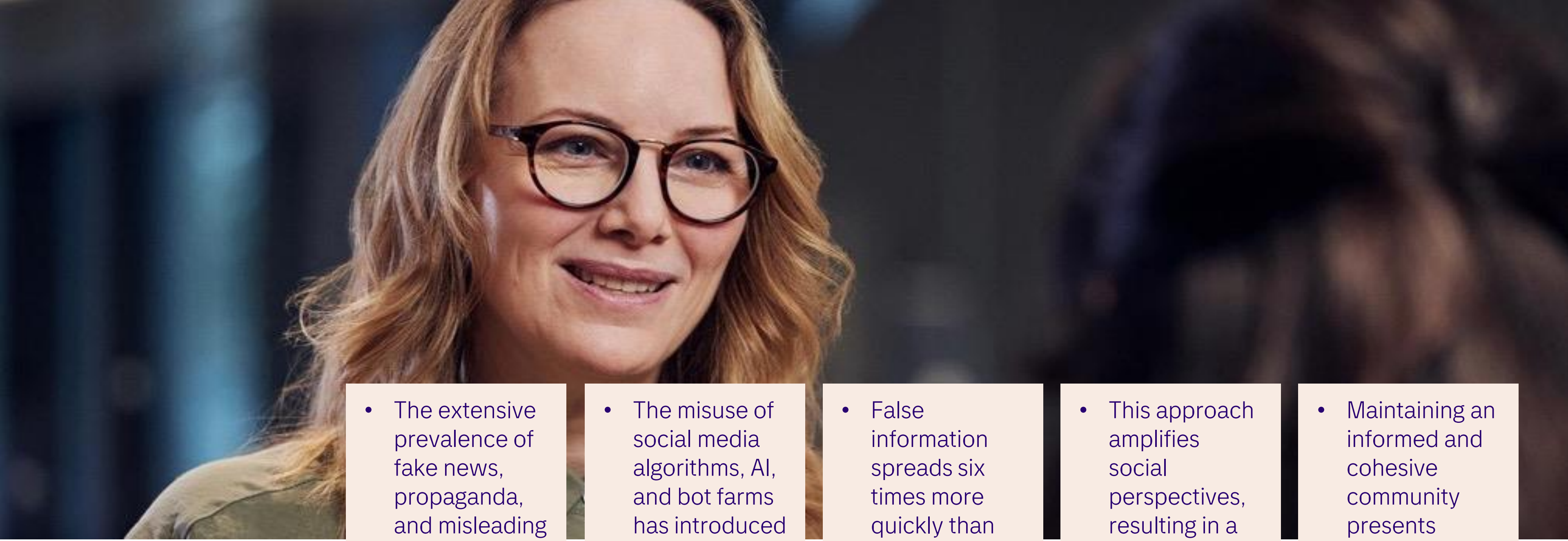
- Both Russia and Ukraine use social media to influence public opinion and sow confusion.
- Misinformation often spreads quickly due to algorithmic amplification.
- Fact-checkers and independent journalists play a key role in identifying false information.

Impact on International Perception

- Disinformation affects global opinion, particularly in countries with ties to Russia.
- False reports create divisions within international communities and influence foreign policy decisions.
- Misinformation complicates humanitarian aid efforts by distorting the truth about casualties and conditions.

Deepfakes and AI Manipulation

- Russia uses advanced AI to create deepfakes and misleading videos to manipulate perception.
- These tools allow the spread of false narratives, especially targeting politicians and military figures.
- Deepfakes raise the risk of escalation and confusion in an already tense situation.



The Impact of Fake News on Public Trust and Democracy

- The extensive prevalence of fake news, propaganda, and misleading information is distorting public perception and diminishing trust in reliable news sources.

- The misuse of social media algorithms, AI, and bot farms has introduced new risks by greatly shaping public opinion.

- False information spreads six times more quickly than accurate news, resulting in extensive misinformation
.

- This approach amplifies social perspectives, resulting in a more fragmented and polarized society.

- Maintaining an informed and cohesive community presents significant challenges.

Ethical and Security Risks of AI in Warfare

AI and LLMs can be weaponized for autonomous weapons systems and psychological warfare, raising ethical and security risks. Autonomous weapons operate without human intervention, raising accountability concerns, while AI-driven psychological warfare manipulates information to influence public opinion.

These uses challenge current legal and ethical frameworks, necessitating new regulations to ensure responsible use and global security.

Building Trust Through Transparent Information Campaigns

Proactive information campaigns and the effective distribution of reliable information are essential.

In the absence of reliable information, individuals might seek out other sources, which could lead to the spread of misinformation.

Open and honest communication, even when delivering bad news, fosters trust and manages public expectations, thereby preventing rumors and misinformation.

Mitigating Risks of LLM Model Manipulation

The manipulation of LLMs may emerge as a major concern in the coming decade because of their potential misuse in disseminating misinformation, swaying public opinion, or influencing financial markets.

As these models advance and become more integrated into everyday life, **the associated risks** also **grow**.

It is essential to maintain the **integrity** and **security** of the **data** and **algorithms** employed in training these models.

Examining data sources, **refining procedures**, and ensuring **algorithm transparency** is crucial while developing AI enabled applications.

Strong and **transparent supply chains**, combined with thorough **oversight** and **regulatory frameworks**, can help reduce AI risks and ensure the responsible and ethical use of LLM models.

Thank you

26 November 2024, Dmytro Sirosh

tietoevry