ON2IT × AMS-IX PRESENT: THREAT TALKS

Threat Talks
Hackers' Toolbox

What hackers use and how to counter it

Hackers continuously adapt, refining their techniques to exploit vulnerabilities in systems, networks, and security defenses. They stay ahead by keeping up with emerging technologies, bypassing existing protections like Endpoint Detection and Response (EDR), and manipulating known protocols for malicious purposes.

Understanding their methods is crucial for cybersecurity professionals to anticipate, detect, and defend against cyber threats effectively.

This infographic provides an overview of some of the key tools and techniques hackers leverage.

In this Threat Talks infographic we will discuss the following threats:

- Deepfakes
- EDR Bypass
- Precision Time Protocol (PTP)

By **2025** we can expect

8 Million

Deepfakes shared online

Source: Deepfakes and Their Impact on Society

74%

of security practitioners believe **AI-powered cyber threats** are significantly impacting their organizations

Source: The State of AI in Cybersecurity

64%

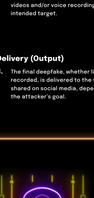
of U.S. adults say **fabricated news stories** cause a great deal of confusion about the basic facts of **current issues and events**

Source: Many Americans Believe Fake News Is Sowing Confusion

64%

of companies consider **EDR** to be ineffective against new or unknown threats.

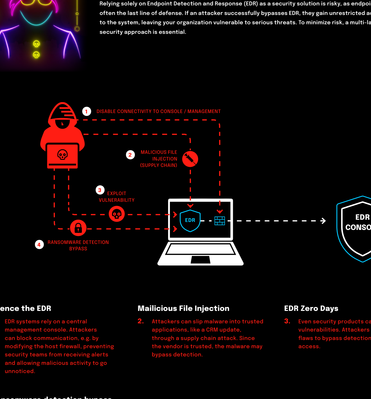
Source: Why is EDR Not good enough anymore



Deepfakes

The Rising Threat of AI-Generated Deception

Using machine learning techniques like deep neural networks, hackers and cybercriminals can convincingly alter faces, voices, and actions, making it difficult to distinguish real from fake. While deepfake technology has legitimate uses in entertainment and research, it also poses serious risks: fueling misinformation, fraud, and identity theft.



Data collection (Input)

1. A deepfake needs a dataset of images, videos and/or voice recordings of the intended target.

Training the Model

2. The AI model learns facial features, expressions, and speech patterns. Pre-recorded deepfakes have more time for refinement, achieving nearly human-like quality. Live deepfakes, however, must adjust to real-time inputs, requiring more resources and often resulting in lower quality. The trained model applies the target's face and voice to the source video, with live deepfakes syncing face and voice in real-time.

Delivery (Output)

3. The final deepfake, whether live or pre-recorded, is delivered to the victim or shared on social media, depending on the attacker's goal.

Live output

4. For live deepfakes, such as during Zoom calls, you can implement a security question to verify the identity of the person joining your meeting. This can be done by agreeing on a code beforehand, in person, providing an extra layer of security.

EDR Bypass

Why Endpoint Security Alone Isn't Enough

Relying solely on Endpoint Detection and Response (EDR) as a security solution is risky, as endpoints are often the last line of defense. If an attacker successfully bypasses EDR, they gain unrestricted access to the system, leaving your organization vulnerable to serious threats. To minimize risk, a multi-layered security approach is essential.

Silence the EDR

1. EDR systems rely on a central management console. Attackers can block communication, e.g. by modifying the host firewall, preventing security teams from receiving alerts and allowing malicious activity to go unnoticed.

Maillicious File Injection

2. Attackers can slip malware into trusted applications, like a CRM update, through a supply chain attack. Since the vendor is trusted, the malware may bypass detection.

EDR Zero Days

3. Even security products can have vulnerabilities. Attackers exploit these flaws to bypass detection and maintain access.

Ransomware detection bypass

4. Many ransomware detection systems create dummy files and monitor them for changes. Attackers can evade detection by ensuring their ransomware avoids these files, allowing the attack to go unnoticed.

Precision Time Protocol

Improving Time Synchronization

In today's digital world, machine-to-machine (M2M) communication is on the rise. While Network Time Protocol (NTP) has been the standard, it's limited to 10,000 logs per second and is vulnerable to spoofing and (DDoS attacks. Precision Time Protocol (PTP) overcomes these issues by offering microsecond accuracy, enabling up to 999,999 transactions per second to be recorded correctly. This precision is vital for security, ensuring events are properly sequenced. PTP also uses dedicated fiber connections, making it more secure than satellite-based systems.

Limitations of NTP Log Capacity

1. A single time server connects in the network to devices.
2. These devices synchronize their time with the time server.
3. The logs generated by these devices include timestamps.
4. Combined logs can be accurately compared due to synchronized time administration. However, if more than 10,000 logs per second are generated, NTP fails due to its lack of precision.

Weakness of time synchronisation over satellites

1. A satellite with a clock sends a time signal to the network.
2. An antenna receives this signal and forwards it to the time server.
3. The time server relies on two time sources, ensuring a backup if the satellite signal is disrupted.
4. A time source that delivers signals over a network is therefore not vulnerable to the same disturbances that affect satellites.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS

amsix

CONTACT US