ТЕМПЕРИЛОДЖИСТИКСЕООД
TEMPERI LOGISTICS LTD

DECEPTION TECHNOLOGY:

traps for hackers

2023

What is deception technology?

The goal of any security measure is to protect against any unauthorized access.

Deception technology is a type of cybersecurity that uses deception tactics, from fake network environments to traps and decoys, to catch attackers and learn more about them. Decoys mimic legitimate servers, applications, and data so that criminals are led to believe they have infiltrated and gained access to a business's most important assets, when in fact they have not. This strategy is used to minimize damage and protect the true assets of the organization.

Deception technology, unlike traditional security infrastructure such as firewalls and endpoint detection systems, does not seek to protect only the perimeter - it detects any illegal activity, even if it comes from within the organization, and does so by taking into account the attacker's perspective and interests to create an active defense. The ultimate goal of deception is to prevent damage to the system by being better informed and prepared.

Advantages of deception technology

Deception technology can prevent attacks and problems that cannot be solved by other methods. Let's look at why you should use deception technology.

1. With deception, you can detect attackers and observe their movements before they even penetrate your network.

2. Deception technology can operate without affecting normal network operations, which means minimal disruption to normal processes and business flows.

3. Deception can be easily scaled and automated for maximum efficiency, even as your organization grows and changes.

4 Eliminating false positives: Deception creates an environment and data that by definition cannot be entered or touched. This means a near total reduction in false positives, noise, and dead-end alerts.

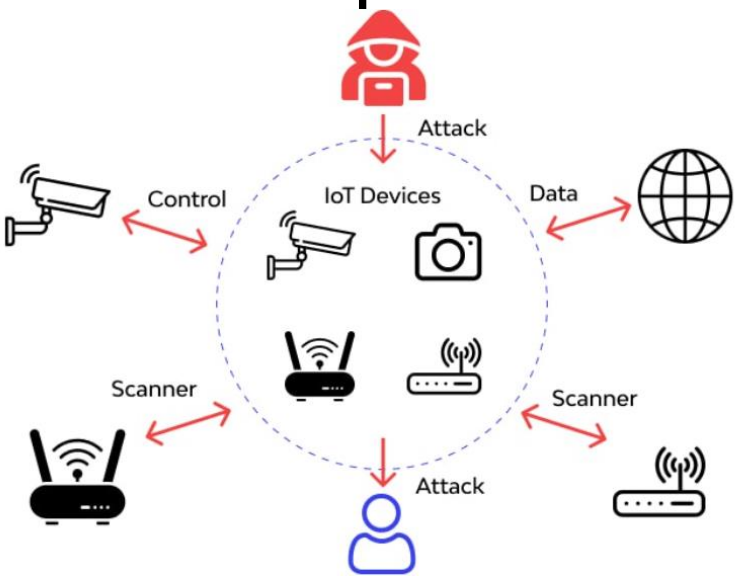
5 Cyberman is versatile and adaptable, working on many types of systems, including legacy systems.

6 Deception technology doesn't rely on generic threat intelligence streams - it creates threat intelligence by attracting attackers and delivers it to your security team in real time.

7 Deception technology is particularly effective at detecting lateral movement and insider threats, as well as sophisticated targeted attacks.

TO FUNCTION PROPERLY, THE DECEPTIVE TECHNOLOGY MUST NOT BE OBVIOUS TO EMPLOYEES OF THE BUSINESS, CONTRACTORS OR CUSTOMERS.

What cybersecurity attacks can be detected with threat deception technology?

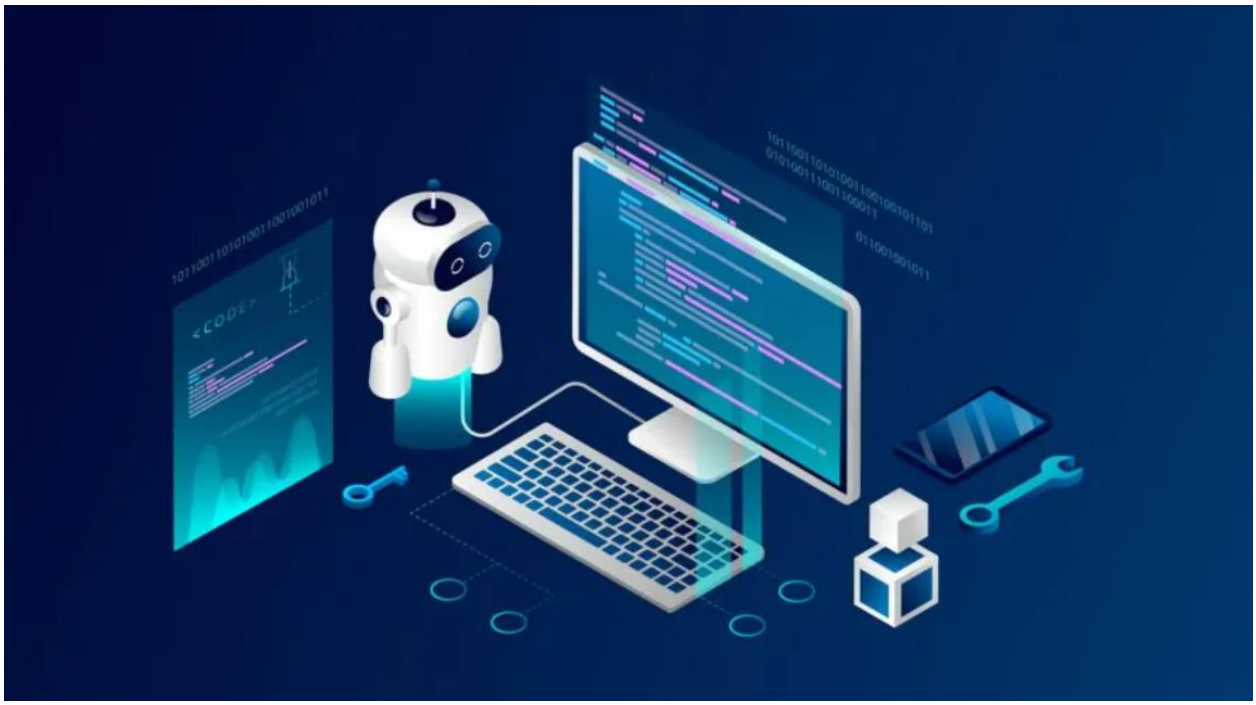


- **Account hijacking attacks: Account takeover attacks** they involve an attacker attempting to take over someone's account using stolen credentials.
- **Credential theft:** this type of theft centers around an attacker gaining access to a list of credentials and then using them in a future hack.
- **IoT attacks:** these occur when a hacker targets Internet of Things (IoT) devices using what they believe to be weaker access credentials, such as default passwords, to gain access to an organization's network.
- **Lateral movement attacks:** these involve a hacker attempting to move east-west or laterally across a network. They do this by first gaining access to one system and then attempting to spread their attack to other systems to which the computer is connected. This way, they can take advantage of the interconnected assets within your organization.
- **Spear phishing:** this occurs when an attacker targets a specific person or group of people in an organization in an attempt to trick them into providing sensitive information, but with deception and cybersecurity technology you can also learn how to prevent such attacks.

How deception technology works

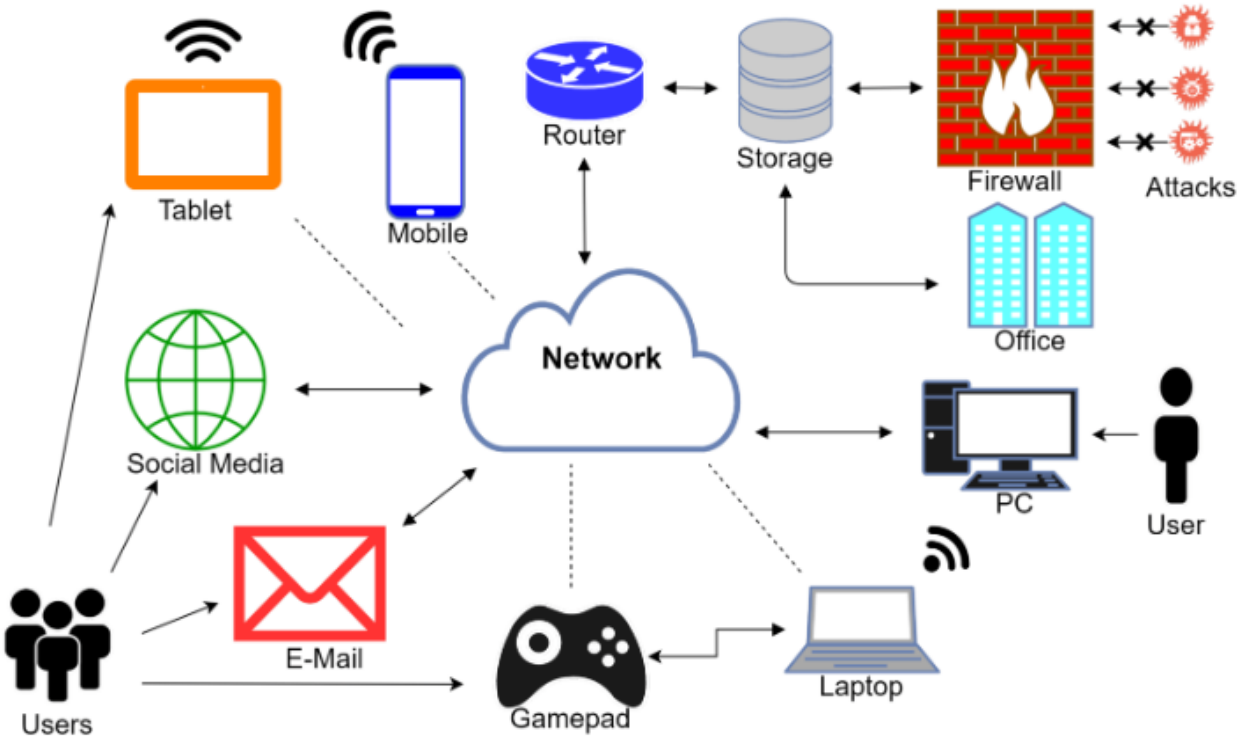
Deception technology works by forcing a hacker to use false resources on your system. It mimics the types of digital assets that are commonly found in your infrastructure. However, these are just traps or decoys, and when an attacker pursues them, they don't damage business-critical systems.

As attackers interact with various aspects of the deception environment, believing they are navigating a real enterprise, specific information is collected by the assets through a combination of agentless and sophisticated software deception agents at many levels, creating a comprehensive record of activity tracking.



Enterprise cyber defense professionals can create and deploy deception campaigns, as well as monitor in real-time the current visual status of ongoing campaigns and attackers at various stages of the attack lifecycle.

Deception technology works by getting the attacker to use false resources on your system. It mimics the types of digital assets that are commonly found in your infrastructure. However, these are just traps or decoys, and when a hacker pursues them, they don't damage business-critical systems.



The goal of threat deception technology is to make the attacker think that he has actually infiltrated a system and is conducting a successful privilege escalation attack. When he engages in activities that he thinks give him the same privileges as a network administrator, he is actually just working without gaining any additional rights or significantly impacting your infrastructure.

Another key element of threat deception technology is a notification system configured to record attacker activity. Once the server receives a notification, it begins recording what the hacker is doing in the specific area it is attacking. In this way, cyber deception technology can provide valuable information about hackers' attack methodologies.

Another benefit of deception technologies is that they allow the IT team to determine which assets are most attractive to attackers. For example, while it's safe to assume that a database with user information such as payment information, names, addresses and Social Security numbers is an attractive target, with security deception technology you can verify that these are indeed assets that hackers are using after the fact.

In addition, you can determine the exact types of data that a hacker is after by simulating environments that contain one or more types of information. For example, you can create fake databases containing Social Security numbers, names and addresses, and login credentials for the accounts of specific company executives. You can then observe which assets the attackers choose to attack. This gives you more insight into what they are looking for.

This is an illustration of what deception can look like in action.

Deception tactics and techniques

1 **Hiding the truth:**

- **Masking.** Masking mechanisms make it impossible to discover the truth.
- **Repackaging.** Repackaging mechanisms work by making the truth appear to be something else.
- **Blinding.** Blinding mechanisms work by making the truth difficult to distinguish from false information.

2 **Substitution of true information with false information:**

- **Imitation.** Imitation mechanisms operate by causing the deceiver to portray false information in a way that makes it appear to be true.
- **Invention.** Invention mechanisms operate by making completely new information appear to be true.
- **Deception:** Deception mechanisms operate by diverting opponents' attention from the truth**.**

DECEPTION TECHNOLOGY IS ONE OF THE BEST TOOLS TO UNDERSTAND WHO IS TARGETING YOUR BUSINESS AND WHY.

IMPROVING YOUR KNOWLEDGE OF YOUR ADVERSARIES BEFORE ANY SUBSEQUENT HACK OR CYBER INCIDENT WILL GIVE YOU, AS A DEFENDER, THE BEGINNINGS OF AN ADVANTAGE.

What cybersecurity threat uses deception tactics?

Sometimes the cybersecurity threat actors themselves resort to deception. An example is a targeted phishing email (the most popular attack vector). It pretends to be an innocent email, but in reality it is something much more sinister.

What to look for when choosing a deception technology provider?

Many vendors would like you to focus on scalability or other trickery, but you should ask questions about their baits (are they unique?), their level of R&D, and the security of their platform.

Today, deception technology has gone beyond a simple decoy and now has features that make it look more credible, extracting key data and performing telemetry rather than the tedious manual process of previous decoys.

The best software for deception technology

Deception technology products are usually standalone solutions specifically designed for deception and investigation. Sometimes data loss prevention (DLP) software and network security software may have some features for setting traps or decoys, but they cannot match the same variety of false targets as technology platforms designed to deceive.

To qualify for inclusion in the deception technology category, a product must:

- Use decoys, lures, and traps to fool attackers.
- Alert security teams to attacks and track them.
- Track and report on attacker behavior and navigation paths.
- Offer tools for vulnerability, risk, and forensic analysis.

1 What is Cynet 360 AutoXDR?*

Cynet enables any organization to put its cybersecurity on autopilot, streamlining and automating their entire security operations while providing enhanced levels of visibility and protection, regardless of the security team's size, skill or resources and without the need for a multi-product security stack. It does so by natively consolidating the essential security technologies needed to provide organizations with comprehensive threat protection into a single, easy-to-use XDR platform; automating the manual process of investigation and remediation across the environment; and providing a 24-7 proactive MDR service - monitoring, investigation, on-demand analysis, incident response and threat hunting - at no additional cost.

https://www.cynet.com/platform/

2 What is Morphisec?

Morphisec Endpoint Threat Prevention thwarts hackers with their own strategies like deception, obfuscation, modification, and polymorphism.

https://www.morphisec.com/

3 SentinelOne Singularity

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. The Singularity Platform protects and empowers leading global enterprises with real-time visibility, cross-platform correlation, and AI-powered response across endpoints, cloud workloads and containers, network-connected (IoT) devices and identity-centric attack surfaces.

www.sentinelone.com

*G2 is the largest and most trusted software marketplace that does not allow paid placement in any of the ratings and reports.

4 LMNTRIX

LMNTRIX Active Defense is a best in class Managed Detection & Response (MDR) service that detects and responds to advanced threats that bypass perimeter controls. We combine deep expertise with cutting-edge technology, leading intelligence, and advanced analytics to detect and investigate threats with great speed, accuracy, and focus. This is our cyber defence SaaS platform that provides a new utility model for enterprise security, delivering pervasive visibility, automated threat detection & prevention, threat hunting, investigation, validation and unlimited forensic exploration on-demand and entirely from the cloud. It is a single investigative platform for insights into threats on enterprise, cloud, hybrid, and industrial control systems (ICS) networks.

https://lmntrix.com/

5 Attivo BOTsink

The Attivo BOTsink solution stands guard inside your network, using high-interaction deception and decoy technology to lure attackers into engaging and revealing themselves.

https://attivonetworks.com/

6 Labyrinth Deception Platform

Labyrinth Deception Platform is deception technology software designed as an early detection and prevention solution for cyber threats. It utilizes decoys, traps, and other deceptively attractive data sources that an attacker might consider valuable. Labyrinth Deception Platform changes the attack surface, giving attackers the illusion of real infrastructure vulnerabilities. Each part of the simulated environment replicates the services and content of a real network segment. At the heart of the solution are Points - smart simulator hosts that mimic specific software services, content, routers, devices, etc. Points detect all malicious activity within the corporate network, providing comprehensive coverage of all possible attack vectors.

https://labyrinth.tech/

European Cyber Security Association

The European Cybersecurity Organization (ECSO) is a European cross-sector membership organization that promotes the development of cybersecurity communities and builds a European cybersecurity ecosystem. ECSO brings together the European public and private cybersecurity sector, including large companies, SMEs and startups, research centers, universities, end-users and operators of essential services, clusters and associations, and local, regional and national public administrations around the world. European Union Member States and the European Free Trade Association (EFTA).

https://ecs-org.eu/

Conclusions

While a couple of decades ago, classic antivirus was enough to ensure cybersecurity, nowadays not only network and host-based defenses are used, but also a number of other systems that help identify attackers.

These systems include new solutions of the DDP (Distributed Deception Platform) class, whose purpose is to create a false infrastructure with which a hacker will interact. The task of the DDP platform is not only to create a distributed infrastructure of false targets to divert the attacker's attention, but also to signal the information security officer about the penetration of the perimeter and the beginning of malicious activity.

When the system is deployed, decoys are created that will contain fake accounts with administrator privileges in various systems and services, from Active Directory (AD) to browsers. It is also possible to customize traps that will mimic information systems where sensitive data is supposedly processed. This will help disorient an attacker and identify his actions when he tries to use false assets to develop an attack.

The purpose of placing traps is to attract the attacker's attention, divert it away from real enterprise resources and keep it busy for a while, while gathering information about the attacker's location, tools and attack methods - in other words, everything necessary to detect and stop a missed attack. Traps range in complexity from simulating simple network services such as SMB, RDP, SSH, HTTP(S), MySQL and others, to simulating devices such as switches, ATMs, POS terminals, Internet of Things (IoT) devices, medical equipment and SCADA systems. And the number of traps placed in an enterprise network can reach several thousand. Thus, an attacker will inevitably encounter traps when scouting the network or following decoys. Lures, or breadcrumbs, are fake data placed on real network devices, such as RDP credentials in the Windows Credentials Manager, SSH credentials in command history, web application credentials in cookies, and so on. Another example would be false data sets, such as confidential documents, databases, which would be of interest to attackers. Attacker deception techniques are most effective in the early stages of an attack, when attackers collect infrastructure data, analyze it, and use it to move horizontally across the network. At the same time, the use of deception techniques is potentially possible at all stages

of an attack using the Cyber Kill Chain model. A fake infrastructure layer created using traps and decoys allows the attackers' tactics to be used against them.

It should be noted that this class of defenses is intended to be the last line of defense for enterprises when an attacker has gained access to enterprise resources by overcoming all echelons of defense.

Despite its relative novelty, the market for deception technologies is actively developing. The market size is estimated to be US$1.9 billion in 2020 and will reach a size of US$4.2 billion by 2026. The main sources of growth are expected to be the United States with an average annual increase of 15.7%, Canada (13.4%), Japan (12.2%), China (15.5%) and Germany (13.3%).

Reasons for interest in DDP include the spread of new technologies such as IoT, the increase in the number and complexity of targeted attacks, as well as the changing landscape of information security threats due to an increase in the proportion of employees working remotely.

The integration of DDP with artificial intelligence technologies seems especially promising. Training AI using examples of real attacks against false infrastructure can lead to the development of completely new methods of protection against attackers by compiling a knowledge base about various combinations of actions on their part.