The rapid evolution of deception technologies

Evaluating the latest deception techniques as part of your threat detection strategy

CISOs have invested heavily to keep out would-be thieves, but determined actors still routinely breach corporate defenses.

The number of threats organizations face continues to increase. Attacks grow more sophisticated and target more widely.

Current security tools are very good at flagging up anomalies, but not so good at defining their impact and risk potential. The result is a hailstorm of alerts, most of which need to be investigated by security teams, despite the vast majority of them being benign. Resources are expended wastefully assessing false positives, while real and present threats can be missed.

That's why interest in deception technology is also on the rise. According to research firm Technavio, the global deception technology market is growing at a compound annual growth rate of 9%, and may reach convUSD 1.33 billion by 2020. Deception technology has typically been the preserve of governments and major banks. It's now broadening its reach into other sectors.

The expansion is being driven by new approaches that are both more effective at capturing breaches, and less expensive to implement and manage. But the pace of innovation has led to some confusion about their efficacy, capabilities and appropriate use cases.

Is deception a fad, or the next leap forward in realizing malware-agnostic networks?

What is deception technology?

The concept is as old as Sun Tzu's ancient maxim that 'all warfare (is) based on deception'. On the modern IT battlefield, security teams have the ability to create false targets to attract a hacker's attention. These fakes are then monitored, so that anytime a hacker takes the bait, the security team is alerted.

The advantage of this approach is that only high-confidence network alerts are generated – as any interaction with a decoy asset on must be a serious anomaly. By creating lures for hackers rather than sifting through thousands of possible breaches, security analysts swamped with incident reports can zero-in on cases of actual, ongoing infiltration.

Fake assets include traditional honeypots, but also a new class of distributed decoys installed on servers and endpoints. These new deception technologies mark a heightened level of aggressiveness in addressing the rise in cyber-attacks. When the outer wall is breached and prevention systems fail, deception provides an efficient way to continuously detect intrusions without requiring additional IT staff to manage it.

Deception supplements tools that rely on known attack patterns and monitoring. It also allows CISOs to capture anomalies that happen on lateral network traffic, where a breach has previously occurred but gone undetected (see our recent paper on insider threats).[1]

The hacker uses fake credentials to move around the network looking for high-value information.

While the average length of an undetected inside breach is around 99 days[2], we have dealt with situations where an actor has been operating inside a network for up to six months.

The art of deception

When people talk about deception techniques, they usually mean **honeypots**, a technology which has been around for decades. These are fake servers made to look like an integral part of the network, but are really traps set with bait for hackers. Honeypot software is installed on the server and then connected to the network. Hackers scanning for vulnerabilities find it, 'break in' and run their malware. Security teams receive an alert that the honeypot has been accessed and monitor the attack. The hacker will either attempt to install new malware or move on in frustration.

If honeypots have a key weakness, it lies in the time and effort required to maintain them. Like any server they need to be configured, patched, and updated.

And in addition to being labor-intensive, honeypots can also be a passive line of defense, relying on attackers to somehow identify them as high-value targets. Someone also needs to be tasked with closely monitoring each one in order to quickly react when an attack occurs.

That's because hackers are getting better at spotting attempts to fool them. Real information assets leave an activity trail created by the authorized users who access them – for example log files and browser histories – which become a kind of authentication marker for assets worth stealing. As honeypots generally don't host actual network assets there is no activity trail to pick up, so smart attackers have learned how to avoid them.

Those trails are actually essential for attackers to move undetected through a network. Even if they can break into an endpoint, the overall topography remains invisible. Any attempt to locate nearby assets with a port scan can be easily detected with current defenses, so hackers need to analyse compromised local assets in order to figure out where to go next – and how to copy the behaviour of real traffic when they do. By creating confusion with false assets, CISOs can force hackers to spend more time searching for the information they want. This increases the likelihood of detection.

Like other security techniques, honeypots needed an evolutionary leap to make deception a cornerstone of security operations and incident response workflow. The **latest deception technologies** build on the idea of decoys by pointing hackers to fake assets actually deployed on real endpoints – including servers and laptops. Attackers think they are looking at real folders and files, and real credentials left behind by actual users or administrators.

> 75% of respondents said their most serious attacks entered the network via an email attachment, **while 46% also noted attacks that started with users clicking email links.**
>
> *SANS Institute, 2017 Threat Landscape Survey*

Sometimes called dynamic deception, this emerging category of infosec technology often uses a mix of lures to trick attackers, and then refreshes or updates them regularly to maximize confusion.

The use case for sophisticated deception is to defend against corporate espionage, or state-sponsored theft of sensitive political, scientific or military intelligence. Up to now, it has been used mainly by national governments, defense, power utility and finance/ insurance organizations due to the value of their information assets and the number of attacks they receive daily. However, they are increasingly being used by enterprises in other industries due to their ease of deployment, and the lack of in-house security skills required to detect threats moving laterally inside the network.

[1] *NTT Security: The accidental hacker: While malicious employees generate more press, error and negligence are the real insider threats*
[2] *Security Boulevard; Mandiant M-Trends Report 2017*

How it works

The latest deception technologies allow security teams to install decoys on endpoints, creating a flood of false data with cached credentials for user accounts, browser history and file shares.

This is important because although attacks come in many variations and styles, the majority start through endpoints – particularly user endpoints. According to the SANS Institute's 2017 Threat Landscape Survey, 75% of respondents said their most serious attacks entered the network via an email attachment, while 46% also noted attacks that started with users clicking email links.

Any ratio of fake assets can be created on an endpoint, which makes the job for hackers much more difficult, while increasing the likelihood of detecting the threat. With every move the attacker makes to find the valuable data, the probability of stepping on a fake asset increases.

When a decoy asset is accessed, security teams can learn more about the attacker and the mode of attack. Malware analysis is a common additional feature of deception technologies, augmenting alerts automatically with an analysis of how an attacker interacted with a fake asset.

Some solutions allow attackers to be engaged during a breach, in order to follow and understand their methods and motives. They can be distracted from completing their mission while security teams assess the method, technology and likely target of the attack.

The decoys themselves are made to look authentic using artificial intelligence, which analyses common network naming conventions and shared folders to create false activity trails that mimic actual user behaviour.

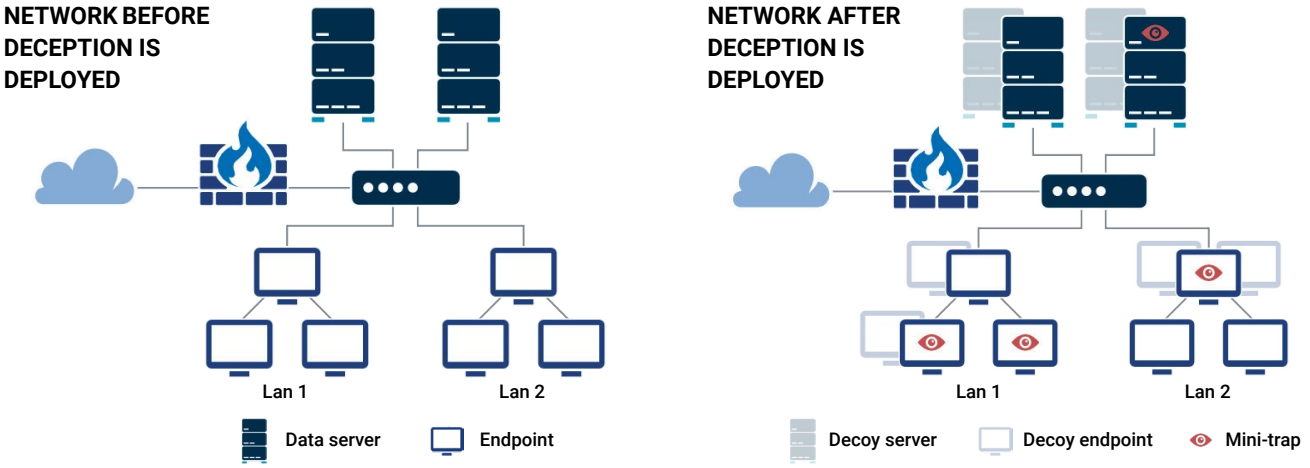

Figure 1: Before and after deployment of deception. Using decoy assets to defend the corporate network enables security teams to assess the method, technology and likely target of the attack.

Despite these capabilities, hackers still sometimes identify decoys and mark them for avoidance. The emergence of **adaptive deception** allows security teams to refresh any fake asset previously marked by a hacker and set new lures to pull them in.

Paths to enterprise adoption

Growing interest in deception solutions is connected to the larger move towards services like Managed Detection and Response (MDR) and Advanced Analytics. As threats and attacks grow more sophisticated, organizations need advanced capabilities that allow them to detect anomalous lateral traffic inside the network.

In addition to focusing on real threats rather than false positives, information gathered using deception technologies can feed into existing security controls and validate or improve current prevention tools like EDR, firewalls and IPS/IDS. Using decoys on endpoints immediately exposes the attacker and the tools used in the attack, providing valuable intelligence for more effective planning of protective controls, and preventing similar breaches in the future.

For overstretched security teams, deception can relieve the need for deep investigation and forensics. It also promises to make the network malware-agnostic, as security teams can focus on the seriousness of a breach rather than the mode of attack.

Dynamic deception technologies aren't necessarily suitable for every organization. Readiness depends on the sensitivity of your operation and the partners you are in business with. There needs to be a level of sophistication in your existing network infrastructure in order to implement decoys on endpoints.

Enterprises should build a multi-layered approach with defense-in-depth first, so that the right responsive controls are in place to work seamlessly with a deception environment. This can include securing data with access control, patching and scanning of files to minimize exposure, and using a post-breach technology as the last line of defense to detect the most advanced attacks.

Conclusion

Due to the sophistication of today's cyber threats, organizations increasingly need to detect and mitigate advanced threats that have already breached the network. Prevention systems continue to have gaps and will be unreliable on their own for the foreseeable future.

By altering the asymmetry of an attack, deception technology frees security teams to focus on real threats to the network. Enterprises should consider adopting deception solutions as part of a resilient cyber defense architecture. This will enable security teams to focus on leveraging the right skills, processes and technology to achieve effective prediction, prevention, detection, and response.

With governments beginning to mandate deception technology in certain sectors such as shipping and banking, it's time for corporates to consider shifting their posture from purely defensive to a mix of defense and offense – turning the tables to outsmart the hackers.


NTT