No.33
January 29th, 2020

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security

PUBLIC/UN-SPONSORED

Telcos Invest in Fake Infrastructure

- Attivo Networks cites a large North American telco as a customer that has derived tangible information security gains from using its ThreatDefend Deception Platform.
- Deception technology serves an important role in helping close the loop in cyber security across threat protection, detection and mitigation phases.
- Telco management should focus less on 5G security standardization and Chinese vendor software and more on filling gaps in their day-to-day IT security.

According to Attivo Networks, a number of telecom operators are investing in fake network infrastructure. They don't mean that they're trialling esoteric technology that will come to nothing. They don't mean IT transformation programs that cost a fortune and don't deliver anything. Nor do they mean the fifty – up to eighty – per cent of over-dimensioned capacity that lies around idle in many telco networks. They're not even referring to fake base stations in the sense of man-in-the-middle attacks.

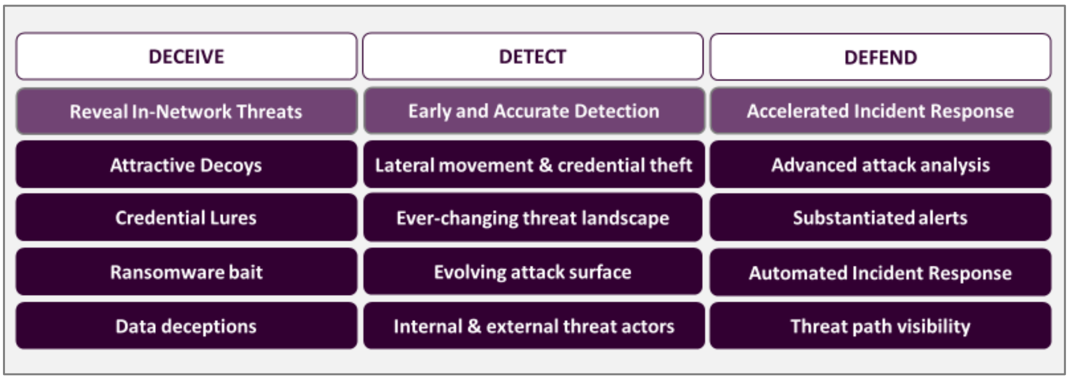
Within a very short time this telco had enough compelling information about the malicious behaviour of some employees to justify summarily firing them.

No, what Attivo is pointing to is telcos investing in actual fake or decoy IT infrastructure served up by the deception technology segment of the threat detection market. Attivo states that it already has many telco customers world-wide. The company cites a specific example of a large North American telco customer that has deployed its ThreatDefend suite of synthetic or fake infrastructure solutions in its IT environment. This example speaks to a telco protecting itself against insider threats in the IT environment but, as will be shown, there are other use cases of deception technology too.

Very Few Employees Knew the Fake Infrastructure was there

This North American telco deployed the ThreatDefend platform around eighteen months ago. According to Attivo, this operator bought a dozen systems with endpoint site licences. Any organization using deception technology is faced with a choice of whether or not to disclose the existence of the fake infrastructure to employees. This particular telco restricted this knowledge to a handful of senior information security professionals. Attivo states that within a short time of deploying ThreatDefend, this telco had enough compelling information on unauthorized and malicious behaviour of some employees to justify summarily firing them (which it did). The next page describes Attivo's deception technology and how telcos and other organizations can leverage it.

Figure 1: Key Components of Deception Technology



DECEIVE	DETECT	DEFEND
Reveal In-Network Threats	Early and Accurate Detection	Accelerated Incident Response
Attractive Decoys	Lateral movement & credential theft	Advanced attack analysis
Credential Lures	Ever-changing threat landscape	Substantiated alerts
Ransomware bait	Evolving attack surface	Automated Incident Response
Data deceptions	Internal & external threat actors	Threat path visibility

Source: Attivo Networks/HardenStance

One of the differences between the ThreatDefend platform and the traditional ‘honeypot’ product space in which a lot of deception technology has its roots, is that it creates a synthetic or fake infrastructure within an organization’s IT infrastructure rather than outside it. This comprises fake master images that are indistinguishable from real assets. They are deployed off-line so the production network is unaffected. It’s very hard for adversaries to spot when they have been lured into ThreatDefend’s fake infrastructure.

Critically, because the decoy infrastructure is isolated from the real production network, there can’t be any legitimate reason of any kind for anyone to enter it – ever. From a threat detection perspective, this has three important implications for identifying bad actors, whether they are external attackers or rogue insiders.

The ThreatDefend platform subjects the adversary to detailed forensic analysis within the fake environment.

- Compared with many other security controls, deception technology alerts are a lot less likely to be false positives. This make them more trustworthy.
- Any user that triggers an alert from within the fake infrastructure is almost by definition up to no good. Depending on the organization, an insider might have a chance of escaping with a warning by pleading that they had no malicious intent. But if their footprint within the fake infrastructure shows that they picked up fake credentials planted on an endpoint by ThreatDefend in order to access a fake folder called ‘Intellectual Property’, then there’s only one outcome: a long, last, security guard-assisted, walk to the elevator.
- A bad actor can be identified in the reconnaissance phase, before they have a chance to even launch an attack on the live production environment.

As well as being embedded in the actual infrastructure rather than outside it, current deception technology has a much richer suite of security capabilities than traditional honeypots. It spots intrusions into the fake infrastructure and triggers alarms, but it also makes it hard for an adversary to exit the fake environment. Taking up an adversary’s time is a good thing in itself. But the ThreatDefend platform also subjects a trapped adversary to detailed forensic analysis within the fake environment. It observes their lateral movement and learns their objectives and modus operandi. This helps organizations better understand their own vulnerabilities and harden their security posture accordingly.

Integration with other security controls enables deception technology to trigger mitigation and remediation actions such as adding a block rule to a firewall or isolating an endpoint with a network quarantine. In Attivo’s case, it has more than thirty integrations with other vendors in key product spaces. These include Security Orchestration Automation and Response (SOAR) with vendors like Demisto (now part of Palo Alto Networks) as well as Endpoint Protection (EPP) and Endpoint Detection and Response (EDR) with vendors such as Carbon Black and Crowdstrike.

There are Use Cases for the Telecom Infrastructure Itself too

To date, most – probably all – decoy technology deployments in telcos have been in IT environments. Attivo is also engaging with telcos to extend the technology into the telecom network itself. The model here is one in which the deception technology sits on the management interfaces behind nodes in the telecom network. It invites intrusions, watches for them, and helps detect and mitigate them according to the same model.

Of the limited attention that executive telco management gives to security, too much is being consumed nowadays by deliberations around the trustworthiness (or otherwise) of Chinese vendors and the potential vulnerabilities in 5G security standards. These are very valid concerns but the management mindshare they are getting is disproportionate.

The use of deception technology by a handful of leading telcos to augment their internal IT security posture is a welcome reminder that information security leaders in the sector know how to see beyond the media-driven telecom security agenda and push the envelope in terms of getting the most ‘bang’ for their ‘buck’. ■

More Information

- Contact HardenStance's Principal Analyst: patrick.donegan@hardenstance.com
- HardenStance received no payment - whether direct or in-kind - for publishing this Briefing.
- Register for **free email notifications** when HardenStance publishes new content.
- www.hardenstance.com

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.