Deception: Deceiving the Attackers Step by Step

TrapX Security, Inc.

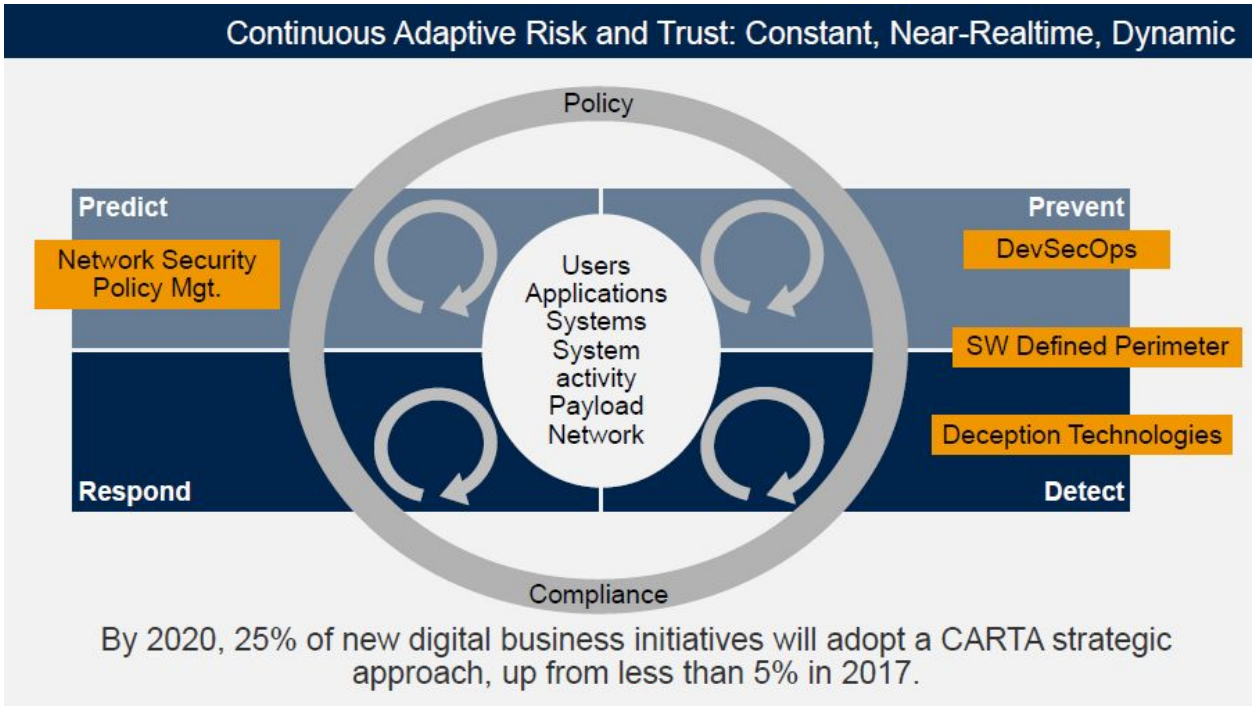
February, 2018

In 2017, Gartner emphasized how companies are transforming their security spending strategy and moving away from prevention-only approaches to focus more on detection and response.

The analyst firm predicts that global spending on security will reach $96 billion in 2018 , compared to 89 billion in 2017, and that by 2020 it will exceed $ 113 billion.

It is expected that spending on improving detection and response capabilities will be a key priority for security buyers by 2020. Around the world we have seen how private and federal-initiative organizations have begun to evaluate and acquire technologies that allow improved detection and response to security incidents, in new solution segments such as Deception, Endpoint Detection, and Response(EDR), Cloud Access Security Brokers (CASBs) and to a lesser extent User and Entity Behavior Analytics (UEBA).

Specifically, Deception has become a fundamental element of Gartner's recent Adaptive Security Architectures model called CARTA: Continuous Adaptive Risk and Trust Assessment. Deception is also part of Gartner's Top 10 strategic technology trends for 2018. Even during 2016 and 2017, this approach was also listed as part of the top technologies in information security for organizations.



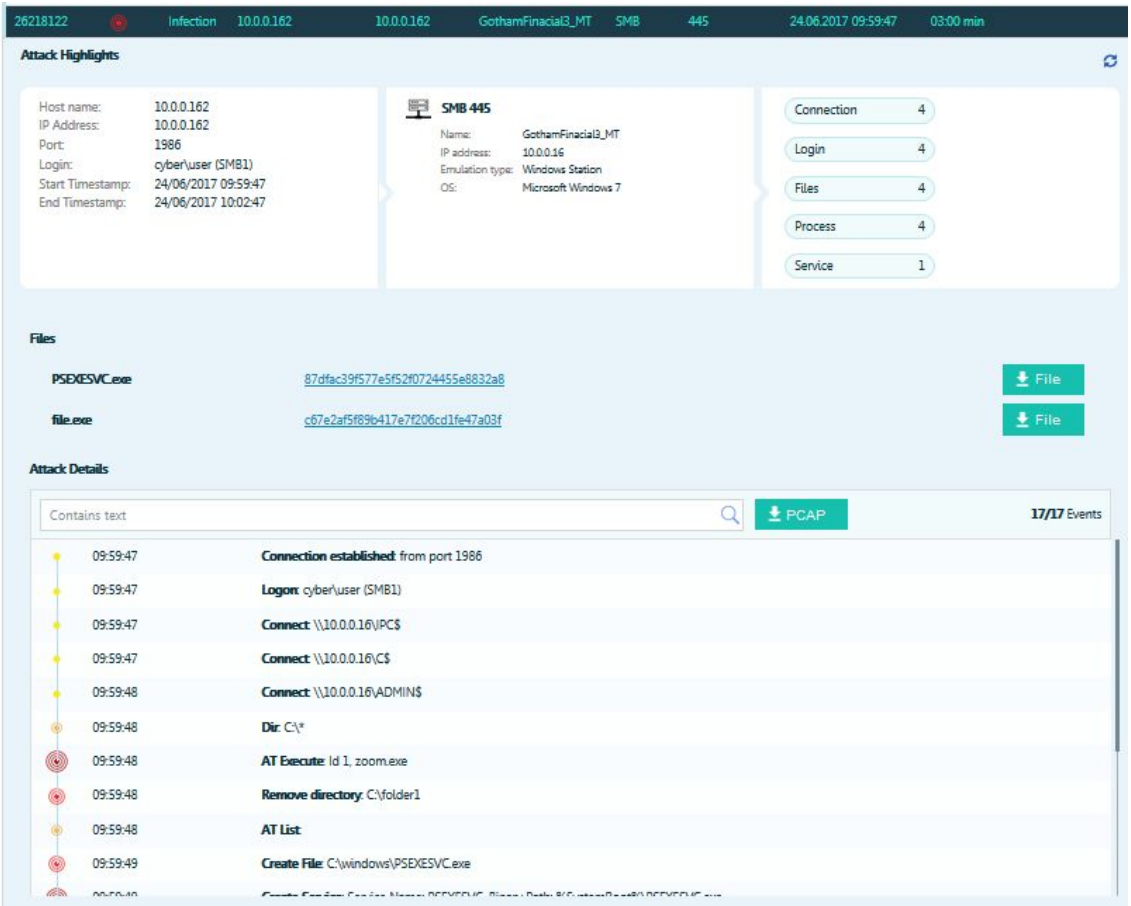
Deception has become an important component for the existing company infrastructure security, because of its main objectives and benefits:

- Detection of malicious attackers and insiders (inclusive misconfigurations) on the network.

- Deception, interruption, confusion and delay of attackers' operations and attacks in progress. This is the main goal of Deception.
- Measurement of the effectiveness of other existing solutions such as EPPs / AV, NIPS, NGFW, UTMs, BDS, SEG, SWG, etc.
- Facilitation of the delivery of managed services (Managed Deception Platforms) under SOC / MSSP systems. Particularly during 2017, Deception grew in popularity due to the model's inherent benefits for multiple business customers.
- Integration with existing cybersecurity ecosystems such as SIEMs, sandboxing platforms, network access control, and containment platforms, as well as the sharing of fully actionable intelligence with traditional prevention mechanisms.
- And, in the case of Intelligence-driven Incident Response and Active Defense, Advanced Deception Architectures (like TrapX Security® DeceptionGrid ™), exposure of attackers' techniques, tactics and procedures to identification of their activities even when the attackers try to circumvent defenses and existing prevention and detection methods.

TrapX's multi-layer architecture works to Deceive the attacker at each of the stages of attack, which is described below:

- The attacker already has a presence inside the organizational network for evasion of controls.
- A single compromised node (patient zero) enables the attacker to perform reconnaissance, searching for valuable information or a clue about valuable targets, for the attacker's "initial jump". In other less sophisticated cases, the attack only uses ransomware and spreads by taking advantage of a security hole. This is where TrapX comes in.
- During this stage, TrapX presents a layer of deception using Deception Tokens, simple endpoint configuration changes that divert the attacker to a fake resource ("trap") for quick identification and prevention of its spread to other network endpoints.
- When the attacker attempts to laterally propagate the threat through human attack, malware, or sophisticated attack, TrapX presents to the attacker a surface of traps emulating the operational platforms of the organizations (servers, workstations, network devices, SWIFT / ATMs, Points of sale, medical devices and IoT devices such as network printers, security cameras and intelligent lighting systems). This DeceptionGrid network allows us to quickly identify the source of the attack, the timeline / detail of the sequence of the attack (connection, reconnaissance, malware exploit), the payloads involved, and the packet capture of the interaction on the trap, to immediately isolate the attacking node, manually or automatically, and feed intelligence to other existing security devices.



- More advanced incident response teams "interact" with attackers in greater depth through a high-interaction trap, which has an actual full OS that presents real responses to attackers' probes. Emulations' deceptive services are redirected depending on the type of service or protocol attacked (AD, MS SQL, HTTP, WMI, SMB, CMD) to a high-interaction trap that provides all the real characteristics of a production asset. A virtual machine running on Windows 2008 R2 SP1 or Windows Server 2012 R2 allows us to proxy from hundreds of emulation traps. Any activity on the trap is recorded from start to finish providing all the forensic detail of the procedures or tools executed by the attacker.

Minimal false positives, a high fidelity of alerts, and an alternative detection method with “low-friction” in its deployment relative to other analysis technologie, are causing the market to rapidly adopt the Deception approach.

Our recent TrapX DeceptionGrid release 6.1 allows us to automatically discover your network, and to accordingly automatically deploy traps similar to existing operating systems.

About TrapX Security

TrapX has created a new generation of deception technology that provides real-time breach detection and prevention. Our field proven solution deceives would-be attackers with turn-key decoys (traps) that "imitate" your true assets. Hundreds or thousands of traps can be deployed with little effort, creating a virtual mine field for cyberattacks, alerting you to any malicious activity with actionable intelligence immediately. Our solutions enable our customers to rapidly isolate, fingerprint and disable new zero day attacks and APTs in real-time. Uniquely our automation, innovative protection for your core and extreme accuracy enable us to provide complete and deep insight into malware and malicious activity unseen by other types of cyber defense. TrapX Security has many thousands of government and Global 2000 users around the world, servicing customers in defense, health care, finance, energy, consumer products and other key industries.

TrapX Security, Inc.
1875 S. Grant St.,
Suite 570 San
Mateo, CA 94402
+1–855–249–4453
www.trapx.com
sales@trapx.com
partners@trapx.com
support@trapx.com