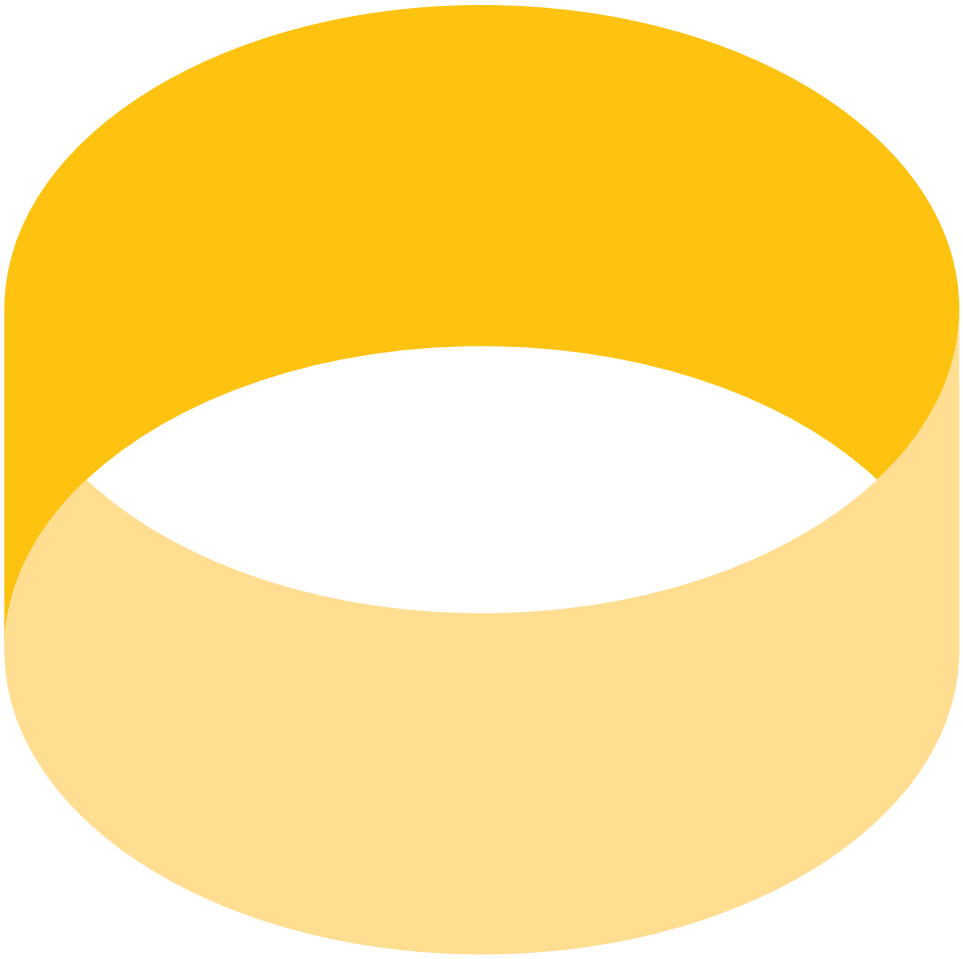


A Look at Deception

How to start playing offense against advanced attackers

WHITE PAPER | SEPTEMBER 18, 2017

Acknowledgements: Initiated and released by Symantec, this document was developed with support from the organization and in direct collaboration with the following:

Authors: Ashok Banerjee, Torry Campbell
Contributors: Balaji Prasad, Alpesh Mote, Spencer Smith, Shireen Rivera

Symantec™

Table of Contents

Background

By 2021, cyber attacks are expected to cause $6 trillion in damages worldwide. To combat, spending is predicted to hit $1 trillion between 2017 and 2021. Attackers benefit from an infinite amount of time and tactics at their disposal, as they work to get around the typical static network and endpoint defenses organizations put in place. Deception can complement endpoint and network defenses, adding dynamic security mechanisms that can be customized for every environment to take the attacker's advantage away.

While endpoint and network security protects you from being compromised, deception mitigates the effects of a compromise by detecting it early and identifying the attacker intent which helps coordinate a faster and better response. Endpoint and network security targets the pre-breach techniques of an attacker, while deception targets the post-breach intent and workflow of an attacker. Per a recent Ponemon Institute report, the average attacker dwells 191 days in the network before they are detected – deception is designed to go on the offensive to reveal an attacker in your network. It misleads an attacker, disrupting their workflows and decisions, to quickly identify them to cut down on their dwell time and prevent them from accomplishing their attack objectives. Deception is now an integrated capability within the Symantec Endpoint Protection (SEP) family, making it easy to go on offense and add more dynamic functionality to your layered defenses.

Deception Evolution

Deception is not a new concept. Throughout history, you can see examples of deception in nature and warfare. A number of animals have developed sophisticated camouflage techniques to trick predators into passing them by and some of the world's best war-time strategists have used deception to create an advantage over their enemies (e.g. Trojan horse). When it comes to cyber security, deception can be used to trick attackers into doing something different than what they intend.

Initially, cyber security deception started with simple network honeypots. These honeypots emulated a subset of a system's functionality, which was enough to fool script kiddies, but not sophisticated attackers. The limited capabilities (e.g. database that had a couple relational data sets but couldn't do bulk uploads) made the systems easy to spot and avoid. Organizations could try to improve the illusion and increase the probability that an attacker would make contact with larger deployments of honeypots, often called a honeynet or honeyfarm, that added functionality and interaction complexity within a completely different, isolated subnet.

The more believable the fake network, the better chance it had to lure an attacker into interacting with it to keep them away from the real resources. Unfortunately, it required a lot of time and expertise to deploy, manage and maintain all the hardware and software needed to create a believable, isolated subnet – with all its fake credentials, databases, web servers, vulnerable systems, and content. These requirements made honeynets impractical or unsustainable for many organizations.

To put deception on individual endpoints, organizations traditionally had to rely on the reachability of the endpoint. This dependence quickly becomes complicated and unwieldy for endpoints behind firewalls, proxies, network address translation (NAT), or virtual private networks (VPNs). Because of how challenging it has been to reliably deploy and monitor deception on endpoints within a large, distributed environment, most vendors focused on network deception.

Symantec, however, has tackled the issues that plagued traditional deception solutions to provide endpoint security that can both protect endpoints from attack and proactively target attackers already on the endpoint. Symantec is currently securing more than 270,000 customers, with 125 million endpoints – all these customers can now work with Symantec to turn on deception and deploy the high-interaction bait that is integrated in the SEP family to dramatically improve attack detection.

Because you know what your critical assets are and where they are located, you can exploit this knowledge to mislead attackers targeting your organization. You can deploy a wide variety of 'bait' - fake files, credentials, network shares, cache entries, and endpoints – throughout your environment to trick attackers into identifying themselves and revealing their attack objectives:

- **Fake Files:** you can create fake files to entice an attacker out into the open. Think of how attractive a "ConfidentialMerger.doc" would be on your CEO's desktop, or a "FundraisingCycle.doc" on your CFO's desktop, or a "Salary.xls" file on your human resources server. The options are endless.
- **Fake Credentials:** you can create and distribute fake passwords throughout systems to make it easy to identify an attacker – any attempt to use one of the fake passwords is evidence of malicious activity. Advanced, high-interaction deception systems can enable an attacker to log into a controlled system with a fake-password and interact to reveal their tactics and true intent.
- **Fake Network Shares:** you can use fake network shares on desktops to prompt attackers into interacting with resources to reveal themselves. Any engagement with these network shares, such as clicking to open, copying files, etc., indicates an attack.

- **Cached Items:** you can use fake cache entries, such as a DNS cache, remote access tool caches (RDP, VNC), etc. to mislead an attacker and identify their potential targets.
- **Fake Endpoints:** you can make fake nodes on the network visible to tempt an attacker into trying to access that machine remotely – because the endpoint is fake, you know that as soon as someone tries to access it, it's an attack.

The Need for Deception

Why do you need deception, when you have so many other layers of defense already in place? Because you need to cover all your bases. Attackers are increasingly sneaky. Stealing user credentials is a top method for how they infiltrate networks. In addition, they use tools that are already installed on targeted computers. These "living off the land" tactics often don't load malware and don't create new files on the device's hard disk (they run directly in memory). In addition, today's attack surface continues to grow and change.

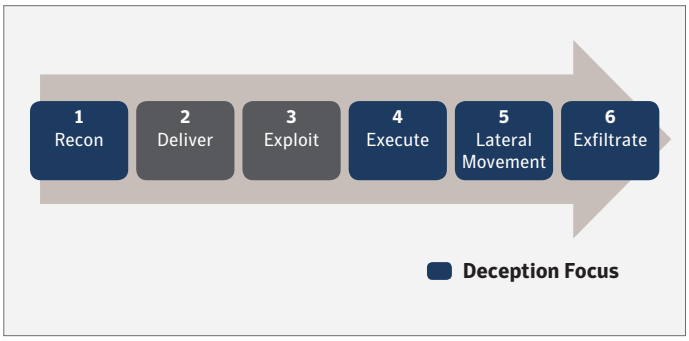
To combat, you need a variety of mechanisms in place to help you close the window of opportunity for attackers and shut down some of the attack vectors they are using:

1. **Social Components**
   a. 43% of the 42,068 security incidents analyzed in 2017 Data Breach Investigations Report involved social engineering attacks.
   b. The human attack surface is expected to reach 4 billion by 2020. Enterprises have a revolving number of employees, partners, contractors, vendors, customers, etc. who all have access to enterprise resources and can exfiltrate corporate data, both intentionally and unwittingly.
   c. Two-thirds of technology professionals surveyed identified phishing/spearphishing and social engineering as the biggest threat to their organization. Post-phishing, an attacker has the credentials they need to get the information they want – there are no further exploits to identify.
   d. 56% of email users and 40% of Facebook users will click on a link from an unknown sender.
2. **Technology Vulnerabilities**
   a. 99% of computers are vulnerable to exploit kits (unpatched OS or software).
   b. Over 75% of all legitimate websites contain an unpatched vulnerability.
3. **Endpoint Weaknesses**
   a. Endpoint protection may not be deployed to all endpoints (accidentally).
4. **Misconfigurations**
   a. Protection is often out of date, leaving assets exposed and vulnerable to attack.
   b. Capabilities designed to protect may be turned off.

Deception adds an offensive layer to your security that increases the chance an attacker in your network will be discovered. You can quickly and easily place an infinite amount of bait in your enterprise (fake credentials, files, vulnerable endpoints, critical assets, etc.) to deceive an attacker into revealing themselves. Deception picks up where other security technologies leave off, providing offensive tactics that can uncover the later stages of an attack.

Attack Workflow

While most security technologies are designed to identify and stop the early stages of an attack, deception is optimized to identify the later stages. Based on the following simplified attack sequence, most security technologies focus on steps 1, 2, 3 and 6, while deception technologies target steps 1, 4, 5 and 6 to uncover the attack activity that's already in the network:



1. **Reconnaissance** – The attacker explores the attack surface, looking to discover the systems, services, applications, people, vendors, etc. that make up your environment.
2. **Delivery** –The attacker crafts and then delivers an attack. Often the delivery is achieved through email phishing, email attachments, malicious links, a watering hole, USB, or other removable drive.
3. **Exploitation** – The attack is initiated and in the network.
4. **Execution** – The attacker will complete the steps of the attack. Often they will:
   - **Establish Persistence** – This ensures the attacker will be able to remain in the network, even if a component of the attack is identified. (E.g. they will try to ensure their reverse shell is maintained across system reboots.) This is frequently achieved by application shimming or embedding themselves in startup items, registries, Windows Authentication packages, etc.

- **Escalate Privileges** – Privilege may need to be escalated to get access to critical assets. Some techniques they may use include access token manipulation, AppInit DLL(s), application shimming, DLL injection, launch Daemon, etc.
- **Command and Control** – Given that every environment is different, the attacker needs a general purpose remote access tool (RAT) or reverse shell to explore the environment and plan their next course of action. Command and control traffic is frequently encrypted and tunneled inside HTTP or IRC to avoid detection by the firewall.

5. **Lateral Movement** – The attacker traverses the internal network, looking for critical assets. They may potentially use the credentials they have obtained (via privilege escalation).

6. **Exfiltration** – Once critical data is obtained it is frequently encrypted and transferred. Encryption used by an attacker often follows the encryption preferences and tools used in the enterprise. Exfiltration will frequently upload data to cloud services used by the enterprise, such as Box, Dropbox, Google Drive, etc.

Art More Than Science

Deception can be more art than science - it's a game of evasion and counter-evasion. The key is to ensure the bait blend into your environment, so attackers will interact with them and reveal themselves. Symantec's deception is supported by Symantec Cyber Security Services (CSS), for continuous threat monitoring and incident response expertise, and Symantec Consulting Services, to customize your deception deployment to fit the tactics, techniques and procedures (TTPs) that will work best in your environment. Together, they will support:

- Deploying and customizing the initial bait embedded throughout your environment.
- Ongoing, 24x7, monitoring of any alerts triggered by SEP Deception and other devices across your on-premise and cloud environments – a CSS SOC analyst can contact you (10 minute SLA) when an incident has been confirmed as critical and provide you with the attack details, assets impacted, and any recommended courses of action.
- Incident response typically requires sealing the entire ingress path, which often requires forensics and EDR analysis.
- Closing the feedback loop to continue to refine the bait and optimize the deployment.

Conclusion: Modern Deception with Symantec

Deception picks up where most security technologies leave off, adding a complementary layer of protection that enables you to go on the offensive and lure attackers out of hiding. Symantec enables you to easily deploy an infinite amount of customizable bait throughout your environment, using the Symantec Endpoint Protection Manager, so you can identify attackers that are in your network and stop them from achieving their objectives. And because deception uses the same single Symantec Endpoint Protection agent and management console, the solution is already optimized to have no tangible performance impact. The Symantec deception approach solves the endpoint reachability problem that has plagued vendors in the past. With Symantec, you don't have to relax firewall rules or enable vulnerable endpoint services and you don't have to procure, manage or monitor any additional hardware. You simply turn on deception to add bait on the endpoints in your large, distributed environment. By placing realistic bait on your endpoints, you significantly enhance the probability that an attacker will come across it. Because it's bait, there is no legitimate reason for someone to try to access the fake remote connections, credentials, files, network shares, etc., so as soon as an attempt is made, you know you have an attacker. The bait (deceptors) are professionally tuned, monitored and refined by Symantec Cyber Security Services.

Contact your sales representative or call 1-855-487-1449 to get started with SEP Deception.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

SYMC_WP_Deception_EN_v1a