Protecting Online Privacy

Prevention is the best form of defense

Dr. D. Williams, BlackFog, Inc.

Introduction

Data and identity theft protection is an important subset of your computer security regime which includes Anti-Virus, Anti-Malware and perimeter defense tools like Firewalls and Intrusion Prevention Systems (IPS). Most security products today focus on resolving problems based on known vulnerabilities and inbound traffic whereas data and identity theft protection is concerned specifically with data loss prevention.

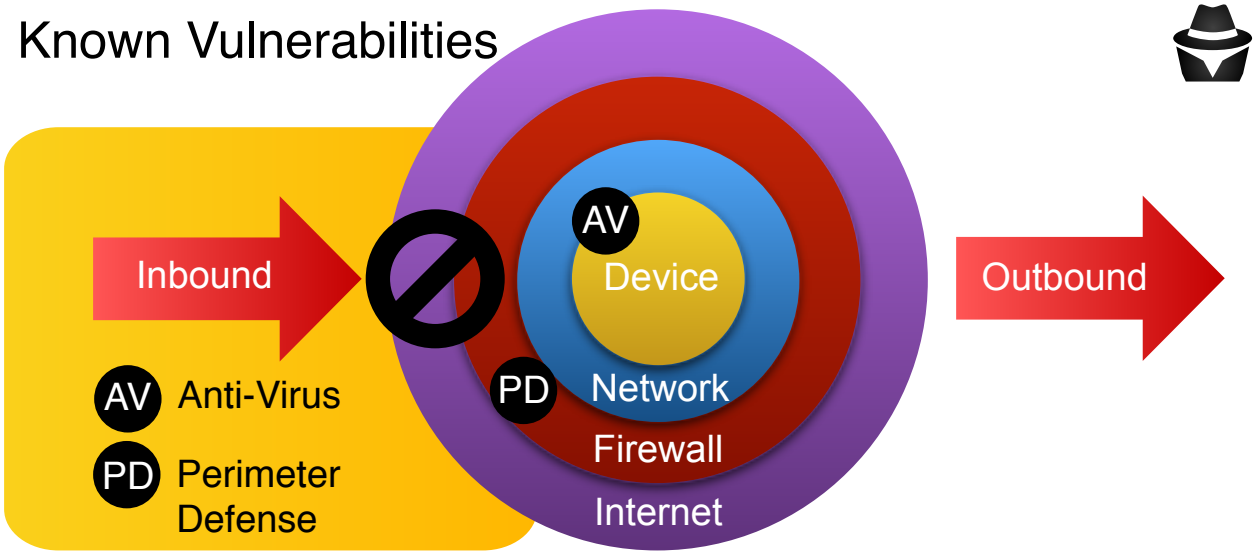
This paper discusses the different types of defense mechanisms available and how they differ from BlackFog's approach to threat detection and prevention.

Perimeter Defense

Firewalls are perimeter defense tools that have been the cornerstone of threat prevention for well over a decade. They can block specific ports, endpoints and known vulnerabilities effectively. Since they exist at the gateway they provide an invisible layer of detection for devices within the network.

The challenge for firewalls and most perimeter defense tools is that they only work against well known vulnerabilities and attack vectors. Cyber threats have evolved considerably and now focus on completely different vectors to carry out their attacks. Instead of targeting known channels for weakness (which is always the first stage) they focus on specific channels and protocols that are already open.

Since primary access to the Internet is through a web browser, cyber attacks now focus on weaknesses in browsers and the HTTP/S protocol itself. With more than 80% of your exposure to the Internet through this mechanism cyber criminals utilize this to target you and effectively bypass firewall rules. By leveraging this open port (typically 80 or 443) cyber criminals are able to create tunnels through your network and communicate back to their command and control servers (C&C servers) at will.



Anti-Virus Tools

In contrast to firewalls, anti-virus (AV) tools focus on the device itself. These tools are great at removing the problem once it is discovered. While clearly and important part of your toolkit once you have been infected they do little to prevent problems in the first place.

Anti-virus tools use a technique known as signature detection. When threats have been discovered researchers fingerprint the files, providing a unique signature that can be used to detect these problems on your device. The signatures are then added to a database which is then sent back to all the clients running the vendor's software ready for the next detection scan.

Like perimeter defense tools, anti-virus tools focus on known vulnerabilities and therefore cannot adapt to future threats. In the next section we will explain how BlackFog approaches the problem of data loss and identity theft protection using preventative techniques.

Prevention

In the previous section we discussed how Perimeter Defense and Anti-Virus solutions are an important part of your overall security regime to protect your online privacy. These solutions focus specifically on known vulnerabilities rather than zero day defense mechanisms. Just as you go to the doctor once you have a problem, these solutions focus on resolving a problem after it has occurred.

Network Defense

Ransomware

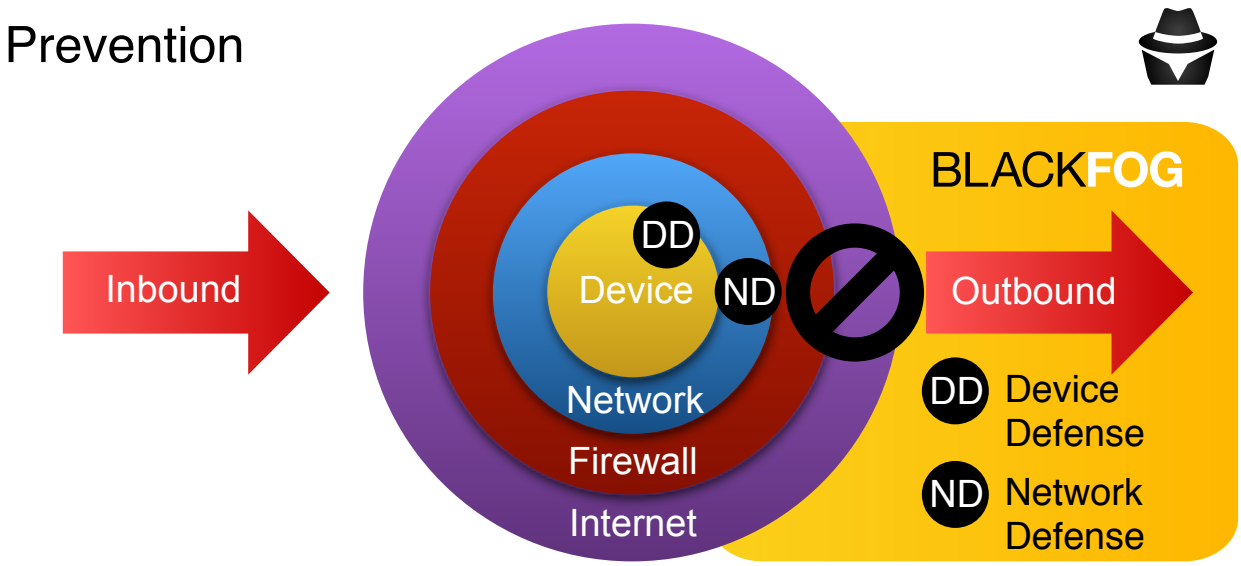
The subject of much controversy over the last few years is ransomware. This software encrypts the files on your device and then locks your machine until you pay a ransom fee to the perpetrator. If you pay the ransom then your files are decrypted and your machine is unlocked.

This software is unwittingly installed by clicking links inside emails, or visiting web sites with links to infected software or spread through advertising (refer to the paper on malvertising).

The impact to a consumer machine can be severe, resulting in the loss of personal data (at best) on the impacted machine, and potentially across the entire network.

Should a corporate machine be impacted, the stakes become much higher as the ransomware can potentially replicate itself across entire corporate networks, locking proprietary data for eternity (or until the ransom is paid).

Preventing this replication is an important part of data theft and identity protection such as BlackFog Privacy. By preventing outbound connections to other machines or remote servers it is possible to stop these infections before they occur and effectively stop the attack.



Spyware

Like ransomware, spyware is malicious software that is deployed on your machine through many of the same methods employed by ransomware. The difference is that spyware focuses on collecting information about you, such as credit cards, social security numbers, your address, location, etc. and sending it back to their servers to exploit at a future time. This is typically related to identity theft.

Spyware can be quite difficult to detect because most people don't even realize they are infected as the software often remains latent until it is activated. It can continually collect information about you for years before it is discovered. It can even be used for transmitting other files across the network so that it can replicate to other devices.

By monitoring the data flowing out of your computer BlackFog Privacy is able to detect anomalies in data leaving the network and protect your personal data.

Device Defense

Another important aspect of data and identity theft protection is device defense. Rather than detecting and preventing suspicious network transactions as we described above, this focuses on preventing the collection of data on your device in the first place.

Your computer or mobile device is a very complex machine which runs hundreds of background tasks and processes on a daily basis which are constantly collecting information at both the system and application level. This includes information not only about the device itself, such as where it has been, but what you have been doing with it.

The system stores this information in databases, registries, log files and other file types on your device. BlackFog operates at both the process level and the system itself and monitors the collection of any personally identifiable data and constantly cleans it. This also includes closing applications, background tasks, removing certain cache files and other recorded information that might be collected and sent to remote servers.

BlackFog focuses on prevention rather than cure and is an important part of a layered approach to data security and your online privacy.