WHITE PAPER

THREATBOX®

Prepared by:
Dimitri Fousekis, CTO, Bitcrack Cyber Security – Dimitri@bitcrack.net
Jayesh Kerai, Security Consultant, Bitcrack Cyber Security

Contents

Introduction

Threat Actors that have access to internal networks have been increasing over the years. In some cases, the increase is sharp, especially with regards to financial and government entities and in recent times, ICO's and other Blockchain technologies. By designing and building ThreatBox®, Bitcrack Cyber Security wants to contribute to the ongoing defensive side of detecting and mitigating threats that originate externally, but affect internal systems.

Problem Statement

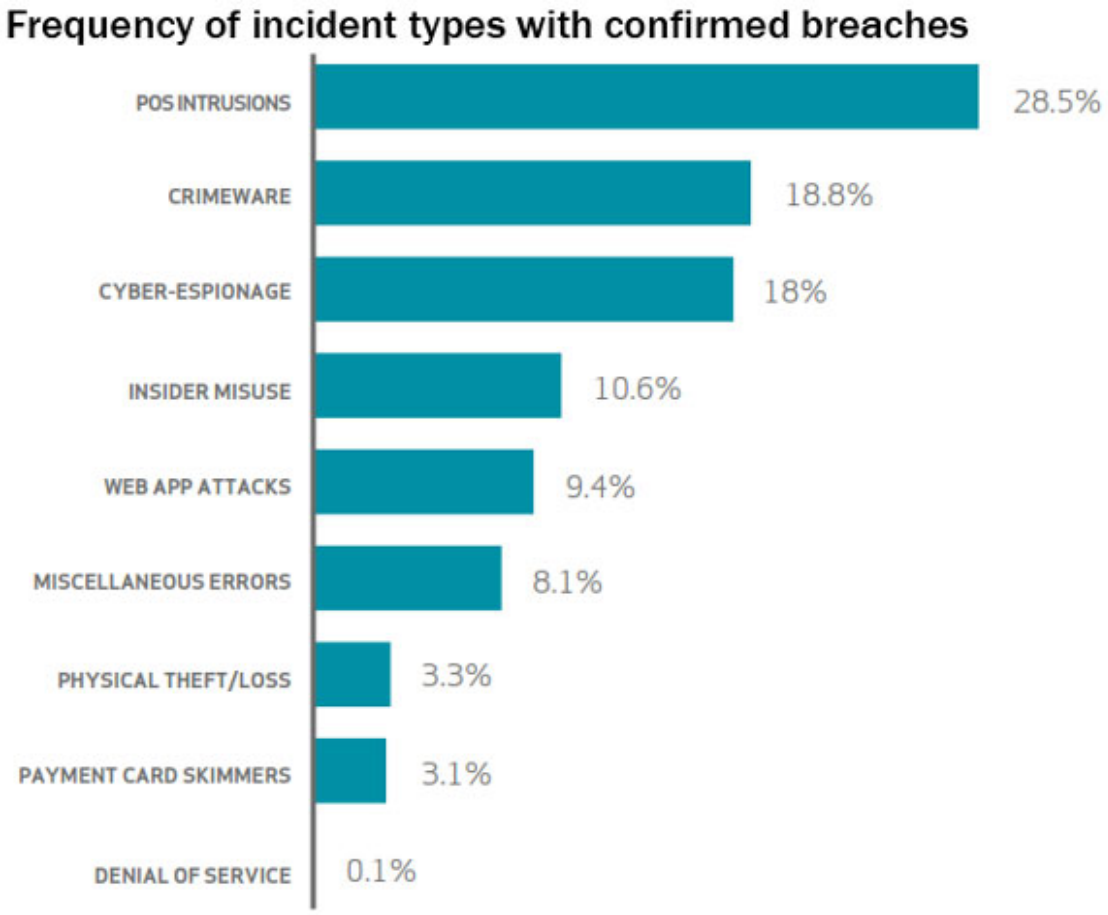
Although an entity can deploy Intrusion Detection (IDS) and Prevention (IPS) technology as well as firewalls and so forth, attackers constantly adapt and find ways to breach those technologies in order to gain temporary or permanent access to internal systems.

This, coupled with the many backdoors and "planted" access in certain commercial systems that have been revealed over the last couple of years, leads us to conclude that although such systems as IDS, IPS and FW are necessary, they are not 100% guaranteed to preventing access to your internal network. Be it a relatively lucky drive-by attack or a full-on criminal syndicate or nation state that is targeting your network and expending major resources to access it, you need to know when a threat actor has landed in your environment.

Such has been possible with technologies that combine Honeypots with network services such as file shares, SSH, Mail Servers, RDP etc. However, there is a gap in detecting such attacks against turnkey applications – in particular critical internal web applications such as HR Systems, Prepaid System, Core Banking, Check Clearing, SWIFT® etc.

In other technologies, there are no current methods for effective confirmation of internal threat actors. Such technologies include Marine systems – yachts, ocean liners and cargo ships. They also include Aircraft systems that expose internal Wi-Fi or other "connectivity" methods that attackers can try to target.

Supporting Data



Source: Calyptix

As can be seen in the above diagram, the first 5 incident types with confirmed breaches affected internal systems of one kind or another. Further, apart from the last one, the rest could all have affected Web-based systems within environments.

This is not to say that 100% of breaches did not occur due to external-facing landscapes, however once breached – internal access is no doubt the next goal of any attacker. It is in this space, that ThreatBox® operates.

Introducing ThreatBox®

ThreatBox® solves the problem above by providing corporates, governments and practically any institution with a deception-based sensor to detect insider attacks.

Unlike traditional Honeypots, ThreatBox® does not rely on simple network services or "cookie-cut" services that are simply replicated and easily detected by scanners as a Honeypot. ThreatBox® looks, acts and becomes a server on the network with a functional web-application. Said application is tailored to your business or industry to further hide the true intentions of the device.

When an attacker is browsing for vulnerable hosts, he or she will sooner or later come across the application on the ThreatBox® and attempt to hack the application. The ThreatBox® will allow this and, drawing from its ancestor - the Honeypot, it will return favorable information to appear as it is vulnerable. The Web Application will keep the attacker busy while ThreatBox® notifies you of an attack internally.

To prevent and handle false-positives, ThreatBox® categorizes its attacks by Low, Medium or High – depending whether the attacker is simply scanning, actively probing or sending an exploit or other confirmed means of breach. You can choose to be alerted to all or only some of the risk categories.

ThreatBox® is available in the following flavors;

1. ThreatBox® FlexCube™ : Looks and works like a FlexCube Core Banking Server.
2. ThreatBox® Check : Looks and works like a Cheque Clearance Platform.
3. ThreatBox® SWIFT® : Looks and works like a SWIFT® Alliance™ Gateway.
4. ThreatBox® ATM : Looks and works like an ATM Management App.
5. ThreatBox® Prepaid : Simulates Prepaid systems for vouchers.
6. ThreatBox® AccessPlus : Simulates Building Access Control Web Interfaces.
7. ThreatBox® SCADA : Simulates a web-front end to PLC/SCADA Controllers.

Niche market devices;

1. ThreatBox® Mariner : Simulates Yacht Navigation System front-ends.
2. ThreatBox® Air-IFE : Simulates Aircraft Onboard Entertainment System Interfaces.

ThreatBox® AI-Client is our client-based device that "simulates" activity to a ThreatBox® unit above to make the system even more visible to those performing network sniffer or ARP-spoof attacks. By deploying multiple ThreatBoxes, you increase your chances of identifying an attacker internally. By adding AI-Clients, the attacker even sees "legitimate" traffic that he or she can profile.

Summary

ThreatBox® has taken the best of many technologies, combined with our many years of security architecture and hacking knowledge to create a device that fills a gap in the front-end attack sensor market. ThreatBox® can play nicely with any other intrusion systems you have as it is passive in nature and does not create network traffic (with the exception of ThreatBox® AI Client)

When a ThreatBox® triggers, you can be confident there is strong potential of an adversary in your network who is up to something suspicious.

Further, ThreatBox® Can boost Blue-Team response times by waiting for Red-Teaming attackers to target it. Hence our slogan for the device is: "*The Black Box, For Blue Teams"*.

Anti-Reconnaissance

A common question asked is, "Can intruders not detect a ThreatBox?" While this is possible especially if such intruder, through leaked information or social engineering obtained sensitive information, we have taken the following steps to make ThreatBox® as invisible to its true identify as possible;

1. Proprietary Ethernet (network) MAC address is changed to mimic server-grade devices or devices usually used for that purpose.
2. Hardened Operating System that returns non-valid TCP fingerprints to bypass Nmap® and other scanning tools from identifying the OS.
3. Re-versioned web-server that does not disclose its actual system version.
4. Other changes that are not publicly released.

A ThreatBox® unit.