Infopercept has perfected the Cybersecurity Kick

Infopercept’s Vision and core values revolve around making organization more aware and secure through the core values of **Honesty, Transparency and Knowledge**, so as to enable them to make better informed decision about their Security Practices & goals. With our synergistic vision to combine, technical expertise and professional experience we aim to further establish our place as a one stop shop for our clients and partners’ cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & continuous knowledge in the Cybersecurity domain, latest trends and Security innovations, ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

"I fear not the man who has practiced 10,000 kicks once, but I fear the man who has practiced one kick 10,000 times."

- "Bruce Lee"
All War is Based on Deception!!

The supreme art of war is to subdue the enemy without fighting

Chingis Khan

“If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle

Chingis Khan – Art Of War
WFM2020 Malwares Strategy – Unknown Unknown Situation

Target

Office Network

Fake Host
Fake Wifi
Fake Document
Fake Mobile Applications
Fake Email
Fake Website

Fake COVID Campaign
Unknown Unknown Situation for Business Leaders

CEO Concerns

1. Formulas,
2. Pricing
3. Business Secrets
4. Go-To-Market Strategy
5. Innovation etc.

Intellectual Properties

Companies are ready with

1. Compliance
2. Best practice
3. Secure remote user access with MFA
4. Anti-Virus?

CIO and CISO are worried about

1. Advance Attacks on endpoints
2. Existing endpoint solutions not enough
3. What will happen when this compromised system will come back to network
Proposed Strategy to fight at end points

**Scenario 1**
Attacker builds knowledge about the environment

**Scenario 2**
In a *changing environment*, the attacker needs much more skill, effort and resources to hit

**Scenario 3**
With practice and skill, can achieve accuracy in a *standard/static environment*
Step 1

Installing the Morphisec Agent on all End Points and Servers, which is a next generation solution that has a disruptive approach and uses a moving target defense to protect advanced threats.
Step 2

Isolate all the devices that come back from “Work from Home” and will be connecting to the network, and screen these isolated devices for any malicious threats.
Strategize the Decoy’s implementation across business networks to be able to early detect - later movements, detect potential breaches and advance attacks in the environment.
Step 4

Perform 24*7 Security Monitoring to Actively look for new threats that may arise in the IT Landscape.
Advanced Threats Exist In-Memory

Recent Example

- LockerGoga ransomware cost Norsk Hydro $45 million so far and gains dropped 82%
- Lake City and Riviera Beach, Florida together paid attackers over $1 million following ransomware attacks
- POS malware stole millions of customer payment details from restaurant chains Buca de Beppo, Planet Hollywood and other Earl Enterprise companies

The 2017 State of Endpoint Security Risk, Ponemon Institute, October 2017

- 80% of attacks happen on the endpoint
- 76% of breaches are caused by file less, in-memory attacks
- 51% of attacks are in-memory

EXISTING SOLUTIONS rely on PRIOR KNOWLEDGE and are DEFENSELESS against unknown, evasive threats.
Moving Target Defense Implementation

Level 11

**Prevention**
Prevents zero-days, targeted and unknown attacks, with no prior knowledge

**Deterministic**
Eliminates false positives

**Resilience**
Randomization of each process
- Moving Target

- **Antivirus**
- **Memory:** App/OS | Vulnerabilities
  - Infopercept Application Memory
  - Morphed Application Memory
  - Skeleton Application Memory

- **Disk**

- **Endpoint**
Most of advanced attacks use memory resources and vulnerabilities in applications and operating systems.

Memory is used at one or multiple stages in the attack kill chain in order to penetrate or evade from traditional Prevention and Detection systems.

Traditional security products focus on executables and inefficient memory scanning thus fail to prevent advanced memory based attacks.

Denial-of-attack stops attacks at initial penetration stage, before malware downloaded from C2C or if malware already persistent and tries to evade.
## Current Cyber-Defense Landscape

### USE CASE

<table>
<thead>
<tr>
<th><strong>Signature / Whitelist</strong></th>
<th>Implemented at both network and endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sandbox</strong></td>
<td>Devices placed at the perimeter to emulate files in a contained environment and assess risk</td>
</tr>
<tr>
<td><strong>Artificial Intelligence</strong></td>
<td>Machine Learning/Deep Learning work on principle of training set deployed on the cloud.</td>
</tr>
<tr>
<td><strong>Behavior Monitoring</strong></td>
<td>Looks for behavior anomalies of processes to make a decision</td>
</tr>
</tbody>
</table>

### SHORTCOMINGS

<table>
<thead>
<tr>
<th><strong>Signature / Whitelist</strong></th>
<th>Requires constant updates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sandbox</strong></td>
<td>Sandbox aware malware can easily evade sandbox detection by delaying mechanism</td>
</tr>
<tr>
<td><strong>Artificial Intelligence</strong></td>
<td>IOA needs to be downloaded to the host to prevent if connectivity to cloud is not present. - League of signature based solution plus false positive - also adds burden to users</td>
</tr>
<tr>
<td><strong>Behavior Monitoring</strong></td>
<td>Based on known behaviors only</td>
</tr>
</tbody>
</table>
# ADDITIONAL LIMITATIONS

<table>
<thead>
<tr>
<th>Signature / Whitelist</th>
<th>Only known attacks can be prevented.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sandbox</td>
<td><strong>Time:</strong> On average sandboxes require 5 mins to analyze a file and most have a cut-out time of 20 mins, after which file is released termed as benign. This is enough time for a patient zero infection to occur in the environment.</td>
</tr>
<tr>
<td>Artificial Intelligence</td>
<td>Works on principle of prior knowledge. The training set needs to be configured by humans to understand the pattern. If the malware strain is not identified by the training set then it is marked as clean, resulting in infection in network. If IOA downloaded locally does not identify the malware, then it needs to be sent to cloud and await results, bringing to prominence Time factor</td>
</tr>
<tr>
<td>Behavior Monitoring</td>
<td>Programmed to detect certain anomalies which means it works on principle of prior knowledge. If malware evades the detection mechanism, then it bypasses the solution.</td>
</tr>
<tr>
<td><strong>Endpoints</strong></td>
<td><strong>Servers</strong></td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>- Prevention of in-memory zero days or file-less attacks</td>
<td>- Enhanced Lateral movement attack prevention by WMI coverage</td>
</tr>
<tr>
<td>- Application Virtual Patching against in-memory attacks for commonly used applications</td>
<td>- Prevention of Shell Code Injections</td>
</tr>
<tr>
<td>- Protection from Mimikatz Credential Stealing attacks</td>
<td>- Protection from Mimikatz Credential Stealing attacks</td>
</tr>
<tr>
<td>- Enhanced Lateral movement attack prevention by WMI coverage</td>
<td>- Application Virtual Patching capabilities against in-memory attacks on default applications installed on server’s (ex browsers, adobe etc)</td>
</tr>
<tr>
<td>- Prevention of Shell Code Injections</td>
<td></td>
</tr>
</tbody>
</table>
THANK YOU

Email
sos@infopercept.com

phone
+91 9898857117

website
www.infopercept.com

No warranty: Infopercept sites, services, and software are provided “as is,” with no warranty, implied or statutory, including, without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement of proprietary rights. Infopercept disclaims any implied, express, or statutory warranties regarding the security, reliability, timeliness, and performance of the solutions & services, including information or advice obtained through the Infopercept.