Input to the Commission on Enhancing National Cybersecurity
Defend USA Now

Whitepaper - Combating Cybercrime, Cyber Warfare, Cyber Espionage & Cyber Terrorism

Dennis L. Meharchand
CEO, VALTx Cyber Security
12425 W Bell Rd, Surprise, AZ 85378, United States
E: dennis@valtx.com
C: 416-618-4622

9th September 2016

"Self Healing Computers is the next big thing in the fight against Hackers" - Philip Quade, COO, National Security Agency (NSA) 11-2014

Executive Summary

In the face of unprecedented levels of successful cyber attacks, Governments should take action to ensure that Military, Government, Critical Infrastructure, Enterprise, SMB and Consumer Computing Devices are secure and uncompromised - mitigating escalating cyber warfare, cyber crime, cyber espionage and cyber terrorism threats.

Cyber crime and cyber espionage have huge economic costs including loss of jobs to both friends and rogue nations as some countries seeks to gain advantage for their domestic corporate organizations and steal military secrets.

Cyber warfare is a growing concern due to nation to nation tensions around the world. Compromised computers anywhere within a country can be likened to enemy soldiers behind the lines - used to attack and disrupt critical infrastructure, Government and Military installations and networks.

There is a need to secure all the computing devices in a country - Military, Government, Critical Infrastructure, Enterprise SMB and Consumer as all devices can be used to further attacks.

Current cybersecurity products and tools are not working - new self-healing architectures providing resilient device integrity need to be put in place.

Recent studies showed that:

a) 97% of organizations had been breached with three quarters of those having active Command and Control communications back to the responsible Hackers

b) Over 70% of Data loss Breaches involved compromise of endpoint computing devices

c) Detection technologies are not working - the average time to discovery of malware breaches is 8 months

Recommendations:
1. New Lockdown Technologies are available to ensure that endpoint computing devices are malware free and uncompromised after every reboot eradicating or neutralizing all malware including Advanced Persistent Threats and Zero Day attacks. These technologies also substantially reduce maintenance costs. These technologies should replace the unsuccessful detection technologies currently in use. We should KNOW that our computers ARE malware free. Products should be able to:
a) Eradicate or neutralize all malware upon every reboot ensuring a clean malware free operating environment eliminating advanced persistent threats
b) Be able to defend itself from adversity attacks and remain operational
c) Facilitate Patch Updates with Instant Rollback architecture
d) Be cost-effective

2. Governments should try to ensure that all computers in the country are cyber secure as a matter of National Defence and Public Safety and should take action to ensure so. Given the importance and economic cost of cybersecurity consideration should be given to purchase and promote the new vetted technologies for the entire country for a One Year Period.

DEFEND USA NOW

We need to cyber secure ALL computers in the Country to defend against Cyber Warfare, Cyber Crime, Cyber Espionage and Cyber Terrorism Threats

Current Cyber Technologies are Not Working

Mainstream technologies widely utilized today by large companies to secure endpoint computing devices are: Signature based Anti-Virus; White listing of authorized Applications, Heuristics/File Behavior, Virtualization and Sandboxing. These technologies provide minimal to zero security, and exhibit failure rates exceeding 50% in today's threat landscape rife with new, 'Zero Day' Advanced Persistent Threats (APT), and targeted attacks--all designed to elude these outdated detection-based methodologies.

The FireEye Study:
FireEye, a leading cyber security firm, conducted a real world study of the Defence in Depth security model. The first of its kind study examined data from more than 1,600 FireEye network and email appliances in real-world settings with over 1,200 actual deployments.
What they found:

- **Nearly all (97 percent) organizations had been breached**, meaning at least one attacker had bypassed all layers of their defense-in-depth architecture.
- More than a fourth of all organizations experienced events known to be consistent with tools and tactics used by advanced persistent threat (APT) actors.
- **Three-fourths of organizations had active command-and-control communications, indicating that attackers had control of the breached systems and were possibly already receiving data from them.**
- Even after an organization was breached, attackers attempted to compromise the typical organization more than once per week (1.59) on average.

The New Lockdown Self-Healing Technologies

New software and semiconductor based products have been developed to ensure that systems are malware free upon every system boot - eliminating all malware, new 'Zero-Day' Threats, Advanced Persistent Threats (APT) and targeted malware. The technology also negates the need for frequent and time consuming patch updates while facilitating testing and rapid implementation of updates as needed with an Instant Bit-Level Rollback feature. Such technology provides an Absolute Defense against all malware types, all persistence mechanisms and all threat vectors without degradation of system performance.

IT Administrators and computing device owners utilizing these technology solutions can be certain that their computing devices remain in a safe operating state and are in fact malware and hack free.

Principles behind creation and development

The concept behind creation and development of these technologies are as follows: The content of a computer systems hard disk drive, which contains the Operating Environment (Operating System, Applications, Registry and Scripts) is typically targeted for attack as malware purveyors seek to infect and execute 'Command & Control' of the computing device. The Operating Systems and Applications with the greatest global prevalence are most frequently targeted – Microsoft Windows Operating System and applications such as Internet Browsers, Adobe PDF, Oracle Java and Microsoft Office Programs. Once a system is initially compromised the attackers then deploy additional controlling malware in order to take complete control of the system and use it to launch attacks within an organization and externally.

Key Criteria for an Effective Security/Protection System:

1. Lock down, secure and protect the Operating Environment without causing the system to break while facilitating authorized updates.

2. Lock down, secure and protect Static Data/Files from unauthorized modification and theft.

3. Allow Dynamic Data to be changed by authorized users – Hide Sensitive Dynamic Data from general view for an additional layer of protection.

4. The Security Technology used must itself be immune/effectively resistant to attack and should not rely on Signatures, Heuristics, Whitelisting or Sandboxing. The majority being Zero-Day, APT' and targeted attacks designed to avoid detection. The Security Technology also should not degrade system performance.