MALWARE PREVENTION METHODS

Protecting companies' network, data and assets from file-based threats using NextGen technologies

THE CHALLENGE: HACKERS SUCEED ATTACKING SECURED COMPANIES

Cybercrime is the greatest threat to every company in the world regardless if it's small, medium or large enterprise. According to Gartner, worldwide spending on information security products and services exceeded $114 billion in 2018 and expected to reach $124 billion in 2019 and to $170.4 billion in 2022.
As companies continue investing resources in security products and services in order to protect their networks, data and assets, hackers develop new ways to bypass those security systems.
When it comes to cyber threats, one of the major attack vectors is hidden malware in a file bypassing the organization's security systems; once the file is opened the malware is executed.
Unfortunately, even enterprises who heavily invest in multiple security systems are still vulnerable to cyber-attacks.

MALWARE BECOMES COMPLEX THAN EVER

Thousands of new malwares created by motivated hackers daily. These hackers find creative ways to spread their malware and access organizations' networks. The following malware types are the most commonly used.

Weaponized Embedded File	Piece of code containing disruptive and harmful commands. The code can be embedded in any file type, once the file access the organization network the malware gets into action.
Split Malware	Distributed Malware Attack (DMA) The attacker splits the code into several different files. Once the files reach the organization network they unify and get into action.
Malware Encryption	The attacker encrypts the code so that it cannot be detected and injects another file that opens the encryption and activates the malware.

Legacy solutions in the market fall short in detection.

ANTI-MALWARE AGAINST FILE-BASED ATTACKS TECHNOLOGIES

Anti-Virus	• Most popular, used by businesses and individuals • Blocks files that were detected with known malware
SandBox	• Used by organizations as it's resource heavy (latency & price) • Executes files in a virtual environment and blocks the files in case of malware detection
CDR	• Used by organizations who look for proactive prevention approach. • Scans commonly used files, eliminates or disarms code, threat vectors and potential hidden malware.

ANTI-MALWARE TECHNOLOGIES - MALWARE RESILIENCE

Anti-Virus

- Effective in blocking known malware.
- Easily bypass by new unknown malicious code and split malware.

SandBox

- Effective in blocking 0day attack if the malware is embedded in a single file.
- Lacking to protect the following: Split malware attack, files protected with password and nested files.

CDR

- Highly effective in known, unknown malware and Zero-day attacks.
- Effective CDR algorithm effectively protect the following: Split malware attack, files protected with password and nested files.

THE odix SOLUTION

odix's technology prevents malware infiltration of organizational networks by **disarming malicious code** from a wide range of file types. The odix process is done on the fly and does not affect business continuity. The odix patented technology, based on CDR (Content Disarm and Reconstruction) is wrapped into 2 product suites; on-premises and cloud, enabling companies to sanitize files from various channels and sources such as email, portable media, web-downloads, files in transit, FTP and more.

ACTIVE DEPLOYMENT (partial list)

Dominion Energy · BAE SYSTEMS · Ashdod Port Company Ltd. THE LEADING ECONOMIC GATEWAY OF ISRAEL · European Investment Bank The EU bank · BIL 1856 Banque Internationale à Luxembourg

HAREL Insurance & Finance · VISTRA ENERGY · Tekniska verken · State of Israel Ministry of Health משרד הבריאות, ישראל · CURTISS-WRIGHT

CERTIFIED TECHNOLOGY

tested & approved by independent leading European, American and Israeli cyber labs

ABB · EY Building a better working world · pwc · Raytheon · BUGSEC one step ahead security

CONTACT US

info@odi-x.com

www.odi-x.com