SIEBEN

Cisco Advanced Malware Protection (AMP) for Endpoints

by

DimitrisSkenderlis
Senior Engineer
CCSI#30839

cisco
Premier Partner

Endpoints continue to be the primary point of entry for attacks!

70% of breaches start on endpoint devices

WHY?

Gaps in protection

65%

of organizations say attacks evaded existing preventative tools

Gaps in visibility

55%

of organizations are unable to determine cause of breach

100

DAYS

industry average time to detection

What's the difference between

Next-Gen Endpoint Security

vs

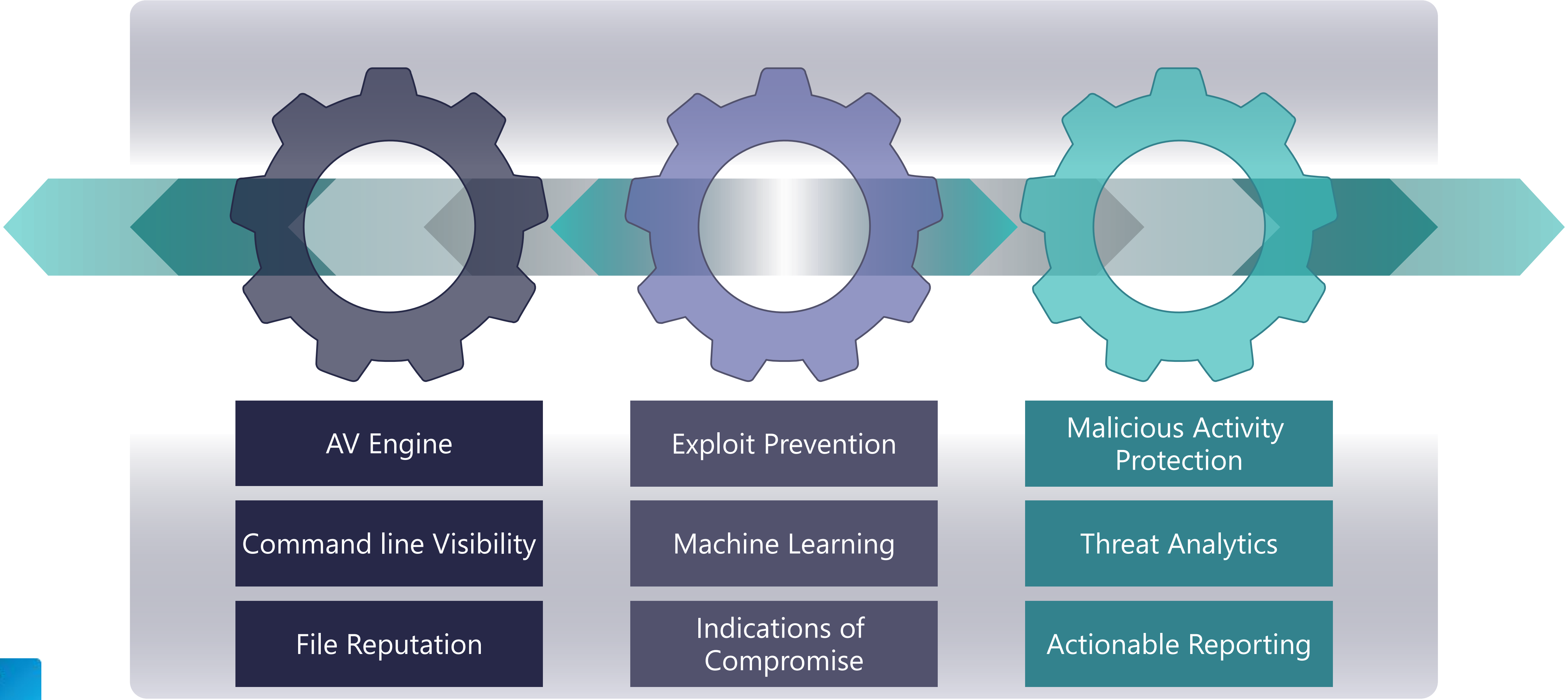
Traditional Antivirus

Nyetya, Petyam, WannaCry and other sophisticated ransomware

- The WannaCry attack took advantage of a recently-patched Windows vulnerability to spread via the network, and then dropped previously-unseen malware that encrypted users' files.

- This shows that a comprehensive security program, that covers everything from your users' behavior to what enters your organization via email or web to how your endpoints are protected, is critical.

Cisco AMP Protects across the Full Attack Continuum



AV Engine	Exploit Prevention	Malicious Activity Protection
Command line Visibility	Machine Learning	Threat Analytics
File Reputation	Indications of Compromise	Actionable Reporting

Malicious Activity Protection (or MAP) defends your endpoints from ransomware attacks

Observes the behavior of running processes File Reputation

Identifies malicious actions of processes when they execute

Stops them from encrypting your data

AMP for Endpoints

> “File-Less Attacks Prevention!”

AMP for Endpoints - Exploit Prevention to Stop File-Less Attacks

Cisco AMP for Endpoints now introduces "**exploit prevention**" capabilities that will defend your endpoints from **file-less attacks** that use **memory injection on unpatched software vulnerabilities**.

These types of attacks include:

- **Web-borne attacks**, such as Java exploits that use shellcode to run payload
- **Malicious Adobe** and **Office document files**
- Malicious sites containing **Flash, Silverlight** and **Javascript attacks**
- Vulnerabilities exploited by **file-less and non-persistent malware**
- **Zero-day attacks on software vulnerabilities** yet to be patched
- **Ransomware, Trojans**, or **macros** using in-memory techniques

AMP for Endpoints - Exploit Prevention to Stop File-Less Attacks

An example of how these work:

1. The user **clicks a link in an email** that they believe is from a trusted source (it isn’t)

2. This brings them to a website that looks legit (it isn’t)

3. The **website loads Flash** (which is the poster boy for vulnerabilities)

4. Flash **opens PowerShell**, which is a tool on every Windows operating system that can issue commands through the command line interface (basically it can talk to things and tell them what to do, **all in memory**).

5. PowerShell connects to the **attacker’s command** and **control server**, whereby it downloads and **runs a malicious script** that searches for your data, finds it, and sends it to the attacker.

AMP for Endpoints - Exploit Prevention to Stop File-Less Attacks

When a user starts an application, it will load in **Memory**;

The AMP connector will allocate a **new space in memory** for the application. The allocation is performed automatically, using a one-way randomization algorithm. This makes the **memory unpredictable for potential attackers**.

The application processes will be pointed towards the **newly allocated memory resources**, however the original allocated memory will be preserved and will function as a "decoy".

The application will now start running as usual. Malicious code, unaware of the memory change, will attempt to use the original memory, triggering the decoy and therefore the AMP connector. The **exploit attack will be immediately killed** and **stored in the AMP console** for forensic **research**.

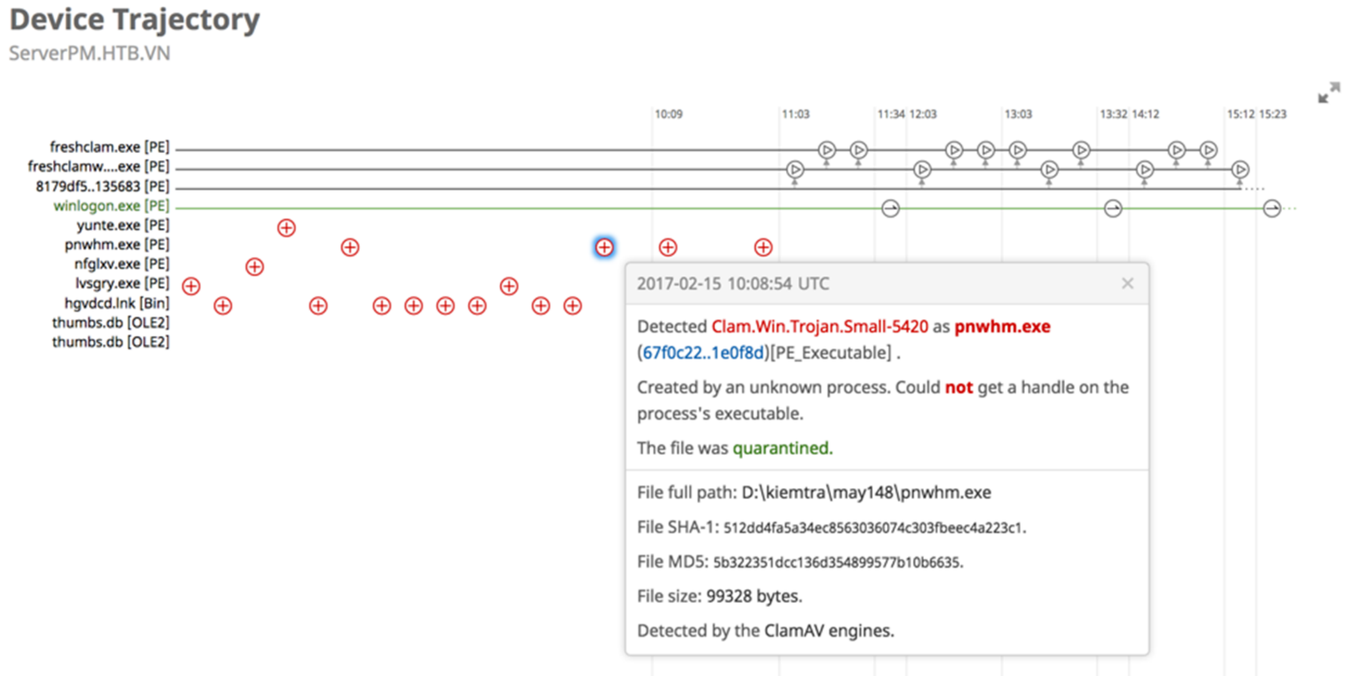
SYSTEM MEMORY

AMP SPACE MEMORY

What happened to an endpoint?

1st

Device Trajectory



Device Trajectory

ServerPM.HTB.VN

2017-02-15 10:08:54 UTC ×

Detected Clam.Win.Trojan.Small-5420 as **pnwhm.exe** (67f0c22..1e0f8d)[PE_Executable] .

Created by an unknown process. Could **not** get a handle on the process's executable.

The file was quarantined.

File full path: D:\kiemtra\may148\pnwhm.exe

File SHA-1: 512dd4fa5a34ec8563036074c303fbeec4a223c1.

File MD5: 5b322351dcc136d354899577b10b6635.

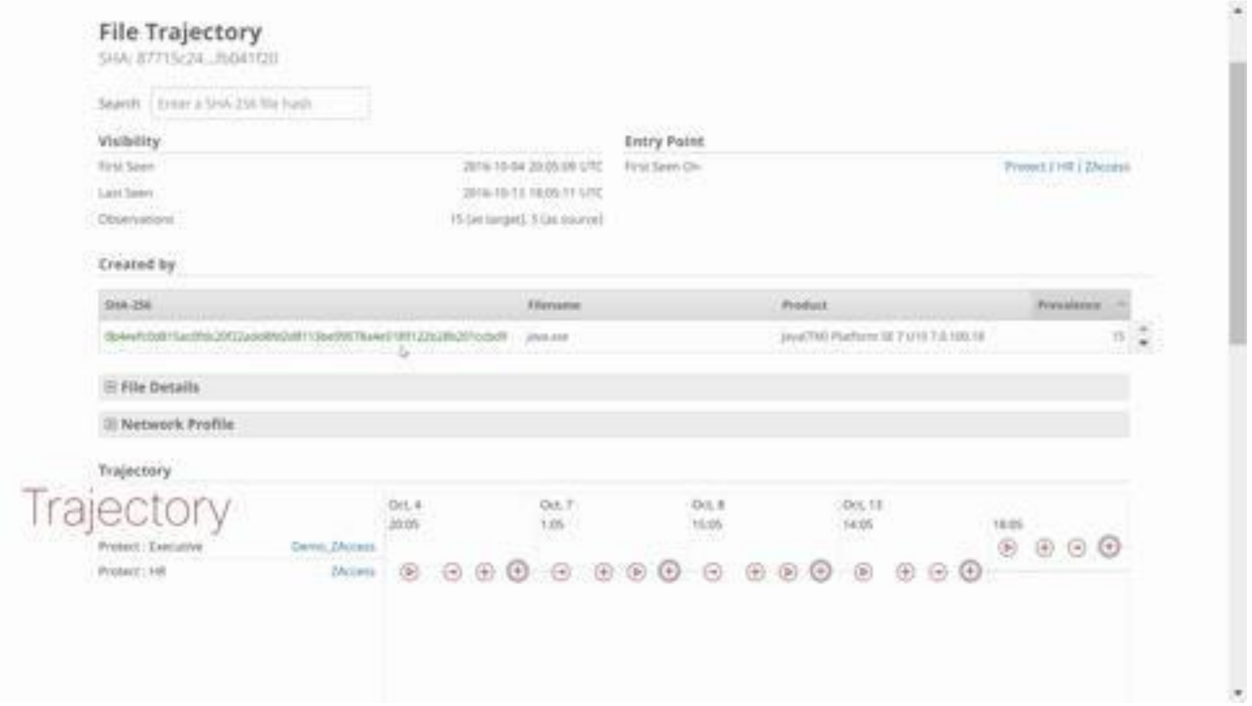
File size: 99328 bytes.

Detected by the ClamAV engines.

Where else is that malware?

File Trajectory

2nd



File Trajectory

SHA: 87715c24...fb041f20

Search: Enter a SHA-256 file hash

Visibility

First Seen	2016-10-04 20:05:09 UTC
Last Seen	2016-10-13 18:05:11 UTC
Observations	15 (as target), 5 (as source)

Entry Point

First Seen On: Protect / HR | ZAccess

Created by

SHA-256	Filename	Product	Prevalence
[illegible]	java.exe	Java(TM) Platform SE 7 U10 7.0.100.18	15

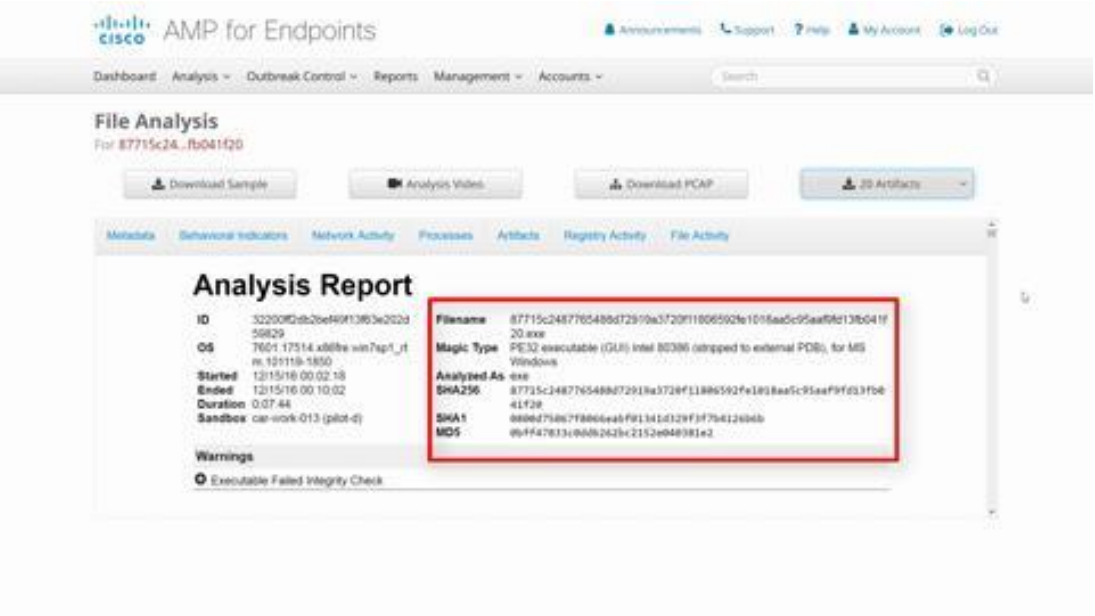
⊟ File Details

⊞ Network Profile

Trajectory

What is it doing?

3rd



File Analysis

For 87715c24...fb041f20

Analysis Report

ID	32200ff2db2bef49f13f63e202d59829
OS	7601.17514.x86fre.win7sp1_rtm.101119-1850
Started	12/15/16 00:02:18
Ended	12/15/16 00:10:02
Duration	0:07:44
Sandbox	car-work-013 (pilot-d)

Filename	87715c2487765488d72919a3720f11806592fe1018aa5c95aaf9fd13fb041f20.exe
Magic Type	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Analyzed As	exe
SHA256	87715c2487765488d72919a3720f11806592fe1018aa5c95aaf9fd13fb041f20
SHA1	0800d75867f8066eabf01341d329f3f7b6126b6b
MD5	0bff47833c0dd6262bc2152e040381e2

Warnings

- Executable Failed Integrity Check

File Analysis (Build in Sandbox)

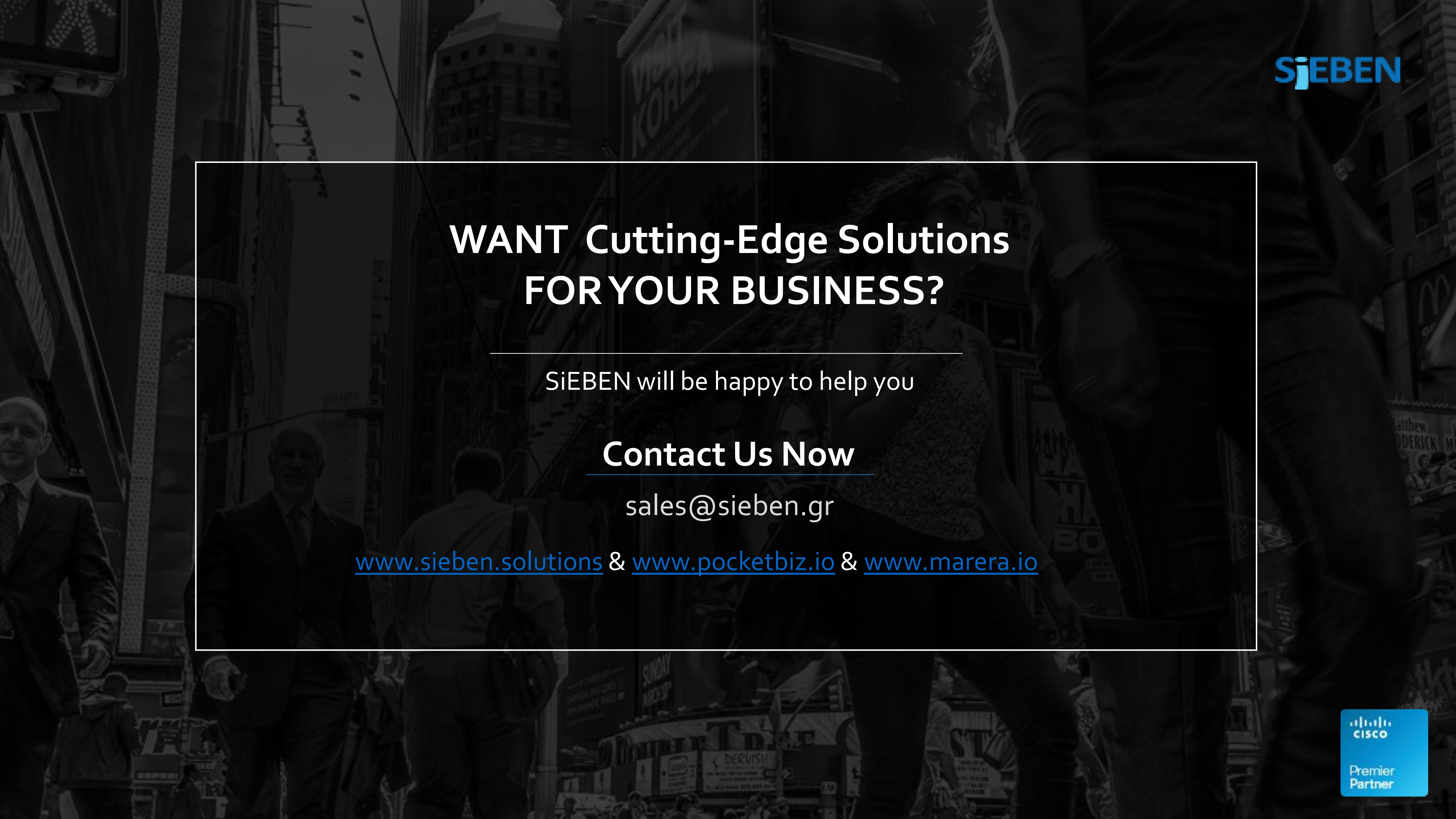
How do we stop it?

4th

Block List & Quarantine

ThreatGRID

Malware Threat Intelligence Platform



SiEBEN

WANT Cutting-Edge Solutions FOR YOUR BUSINESS?

SiEBEN will be happy to help you

Contact Us Now

sales@sieben.gr

www.sieben.solutions & www.pocketbiz.io & www.marera.io

cisco
Premier
Partner