MALWARE PROTECTION

ANALYSIS | MONITORING | TAKEDOWN

Sales Team
sales@menainfosec.com

Client Portal
portal.menainfosec.com

Corporate Website
www.menainfosec.com

New generation Malware can silently infect the end-user device, silently hijacking secure sessions and stealing account credentials unnoticed or silently hijacking secure sessions. Criminals are constantly changing their Malware techniques. This has rendered a reliance on endpoint protection alone to be futile. Malware now has:

- › Decreasing quantity of signature-based detection
- › Increasing number of Malware families with many emerging variants and generations
- › Increased level of advancement and sophistication
- › Zero-day attacks
- › Exploitation of endpoint vulnerabilities, such as blended threats, multiple injection points and vectors

Further to this, your customers have adopted new technologies and now rely on multiple devices, most of which are outside of the organization's control.

MOST COMMON FORMS OF MALWARE

WORM VIRUS SPYWARE TROJAN

HOW DOES MENAINFOSEC DEAL WITH MALWARE

MENAINfo Security is focussed on disrupting the attack in the most effective way - by removing the site that harvests the personal and financial details of your clients and disabling the command and control structure.

MENAINfoSec has developed a suite of proprietary Monitoring and Detection technologies that provides early detection for Malware targeting your brand and the fast removal or takedown through technical and human interaction.

MENAINfo Security provides industry leading takedown times resulting in less time that your brand is being exposed to criminal impersonation.

COMMON BEHAVIOUR FOR A MALWARE ATTACK

STAGE 1 - THE INFECTION

In order to infiltrate the customer, the criminal will design and deploy their software package to be downloaded by the consumer typically by wrapping it inside of other legitimate software of a known or common brand.

STAGE 2 - COMMAND & CONTROL

Criminals make use of centralised command centres to evade detection and also to re-route the destination of the information they are harvesting.

STAGE 3 - THE DROP ZONE

As a result of this attack, the criminal is successful in capturing personal or financial details. The captured information is sent to a "drop zone". The main purpose of a drop zone is to collate and store all captured data until retrieved by the criminals. There are often multiple drop zones to avoid detection and to successfully retrieve the data.

THE COSTS OF MALWARE TO BUSINESS

Malware can be extremely destructive to your company brand. Without active monitoring and detection, an effective Malware campaign can generate:

- › Large financial losses
- › Negative and harmful publicity against the brand
- › Mistrust of the brand

24 HUMAN SECURITY EXPERTS

http://portal.menainfosec.com
www.menainfosec.com
sales@menainfosec.com
+968 99882929

MENA Info Security