BROADGATE CONSULTANTS

BROADReach – Malware Threat Management Service

Businesses today are at risk of a new cybercrime category, called Advanced Persistent Threats (APT's). These are **directly targeted** at specific organisations, their business activities or named individuals. It is not a technology only issue.

Organisations have to consider the *"evolving threat landscape"* in this context and understand not only the tools used but also the motivations, internal exposures, trusted connections and governance and therefore quantify the **business risk**.

The **BROADReach** service has been developed to allow organisations to assess the effectiveness of their existing security layers against the increasingly sophisticated techniques used by cyber criminals to compromise and control computer systems and the networks in which they reside.

Over a two week period using the market leading technology from FireEye, we will provide an extensive customized report with the following insights:

- ✓ The extent of active malware infiltration
- ✓ Exposure level assessment
- ✓ Infection point gap analysis
- ✓ Remediation plan

Malware defined in today's connected world

Cyber criminals have developed modern malware to bypass outdated security techniques, such as signatures, leaving businesses and consumers vulnerable to attack. This is evidenced by the continued and successful intrusions into commercial, federal and educational networks.

Modern Malware is used for
- Cyber crime
- Cyber espionage
- Cyber warfare

High-value enterprises are singled-out
- Using targeted attacks and custom, designer malware to spear phish victims

0-day attacks target unknown vulnerabilities
- Cyber criminals find/buy 0-day vulnerabilities that are unknown to any others

Everyone who browses is at risk
- Ordinary web sites expose systems to exploit attacks (HTML, PDF, Drive-bys, etc.)

At the same time, more and more businesses and consumers are storing data on the network, or "in the cloud," making cyber crime more attractive.

Advanced Persistent Threats

APT's are defined as a long-term pattern of targeted attacks aimed at governments, companies and political activists.

Advanced:

Wide spectrum of intelligence gathering techniques

Persistent:

Adopts a "low and slow" approach with external guidance and control.

Threat:

Have capability, intent, a specific objective and are typically well funded.

Contact:

Broadgate Consultants Ltd
21 New Street
EC2M 4HR
0203 326 8000

www.broadgateconsultants.com
twitter.com/broadgateview

BROADGATE CONSULTANTS

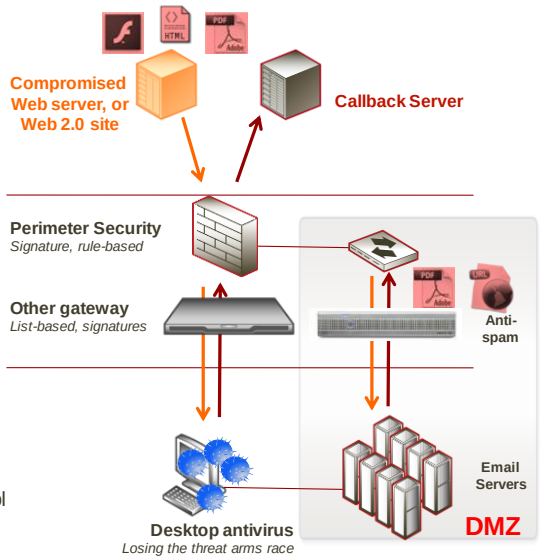
BROADReach Service – Malware Threat Management

The Modern Malware Infection Lifecycle

1 System gets exploited
- Drive-by attacks in casual browsing
- Links in Targeted Emails
- Socially engineered binaries

2 Dropper malware installs
- First step to establish control
- Calls back out to criminal servers
- Found on compromised sites, and Web 2.0, user-created content sites

3 Malicious data theft & long-term control established
- Uploads data stolen via keyloggers, Trojans, bots, & file grabbers
- One exploit leads to dozens of infections on same system
- Criminals have built long-term control mechanisms into system



Stopping the Infection Lifecycle with FireEye

- Dynamic, signature-less engine to detect & block zero-hour attacks
- Real-time protection to stop data exfiltration
- Integrated, cross protocol inbound and outbound breaks the lifecycle
- Accurate with no tuning and very low false positive rate to drive down TCO
- Global malware intelligence sharing to block 0-day malware & latest callback destinations

Getting started with the BROADReach Service

We make it easy for organisations to assess their security vulnerability against malware in four simple steps:

1. One of our specialists will visit your organisation lead responsible for internal security to scope out the evaluation process.
2. Complete a mutual NDA and Terms of Reference for the assessment phase.
3. Gain permission for the FireEye Malware Protection System to be connected to the agreed network SPAN port (non intrusive)
4. Schedule the installation of the FireEye appliance in order to gather the information for the two week period.

At the end of the period we will provide a report and discuss the findings and relevant remediation plans with you.

For more details and to schedule an appointment contact us at our main address or email BROADReach@broadgateconsultants.com

Next Generation Threat Protection

"Incumbent defence technologies fall short" (Forrester 2011)

"Some IPS/IDS/NGFW vendors are no better at handling evasions today than they were when they released their original products" (Gartner 2011)

"With FireEye, we can now see and stop the attacks targeting our in-house and remote users. It has been an eye-opener for us to be able to determine with accuracy the threats that are passing through the firewall, URL Gateway, IPS and antivirus" (Global 500 FS firm)

When evaluating FireEye, 95% of enterprises have discovered compromised hosts within what they thought were secure networks.

FireEye

Contact:

Broadgate Consultants Ltd
21 New Street
EC2M 4HR
0203 326 8000

www.broadgateconsultants.com
twitter.com/broadgateview