Covid-19 Changes the Rules

It has been estimated that since the start of the Coronavirus lockdown in 2020, the number of cyberattacks has increased between 260% and 450%. One source has gone as far as to quote over 1 million attacks were taking place per day during peak lockdown.

Cyber criminals are very aware of the lack of affordable security for satellite offices. Today, many home networks have multiple IP-enable devices connected to them. A single vulnerable device, such as IP-enabled doorbell or a family members PC running a non-corporate strength anti-virus, makes an ideal entry point for an attacker to compromise the home network. Once access has been gained to the home network, it is relatively simple for an attacker to pivot onto the corporate network.

Supporting Home Working

Analysts predict that about 60% of the work-force will retain some element of home working for the foreseeable post-Covid future. The security challenge in supporting satellite offices is that they typically lack the same degree of robust security controls as the corporate network.

The minimum-security controls for an employee working from home should be a locked-down corporate laptop running company approved anti-virus software. In reality, many remote workers are using BYOD devices with, if you are lucky, a free anti-virus downloaded from the in-ternet.

When surveyed, “most” homeworkers admitted that, during the lockdown rush to get back up and running, they have used services not approved by their IT department; such as videoconferencing (70%), instant messaging (60%) or cloud-based storage (53%).

The Botprobe Advantage

Anti-virus software and VPNs play an important role in securing the satellite office. However, these only protect end-point devices. One major difference between corporate security and satellite office security is protecting the network, where corporate networks implement security controls such as Intrusion Detection Systems (IDS).

Satellite office IDS is challenging for several reasons. If centralised IDS is used, how do you cost-effectively transfer the vast amount of network traffic from the remote location to the corporate IDS? If each satellite office has its own IDS, how can you remotely synchronise the detection rules quickly and efficiently?

Botprobe’s innovative ***intelligent data-capture technology*** takes the advantage away from the attacker and gives it back to the security team. By capturing only the elements of network traffic that are useful for threat detection, we can effectively reduce the volume of traffic being fed into analysis engines by 95%. This means, for example, Botprobe makes it cost effective to feed satellite office network threat data into IDS rules in a cloud-based SIEM.

Because our capture probes are handling 95% less traffic data, not only are they faster than traditional IDS solutions, but our software is optimised to run on much lower powered devices, reducing the cost of satellite office IDS.

botprobe

Secure Home Working

Information Sheet

www.botprobe.co.uk

Specification Summary

What does Botprobe detect beyond other security solutions?

VPN	Anti-Virus Software	botprobe
Malware	**Malware on the end-point**	**Malware on the network**
Connection to malicious website	**Connection to malicious website**	**Connection to malicious website**
Connection to ransomware website	Connection to ransomware website	**Connection to ransomware website**
Connection to TOR network	Connection to TOR network	**Connection to TOR network**
Connection to crypto miner website	Connection to crypto miner website	**Connection to crypto miner website**
Connection to website with weak security	Connection to website with weak security	**Connection to website with weak security**
Connection to IP bogon	Connection to IP bogon	**Connection to IP bogon**
Botnet detection	Botnet detection	**Botnet detection**
DNS whitelisting	DNS whitelisting	**DNS whitelisting**
SSL certificate blacklisting	SSL certificate blacklisting	**SSL certificate blacklisting**
Malicious/Hacker activity	Malicious/Hacker activity	**Malicious/Hacker activity**
– CVE/Vulnerability exploit	– CVE/Vulnerability exploit	**– CVE/Vulnerability exploit**
– FTP/SSH/Telnet password attack	– FTP/SSH/Telnet password attack	**– FTP/SSH/Telnet password attack**
– Network scan	– Network scan	**– Network scan**
– Corporate policy rule bypass	– Corporate policy rule bypass	**– Corporate policy rule bypass**
Data leakage	Data leakage	**Data leakage**

Benefits of Botprobe's Home Worker Protection Solution

Low cost of purchase

- Our data-capture technology is optimised for low-power devices, thereby reducing entry cost of hardware probes
- Easy integration into existing network infrastructure
- Integrates with existing analysis/detection engines such as SIEM, ELK or third-party managed services

Increased detection capability

- Brings corporate level security to satellite offices by adding a network protection layer to your existing security
- 95% reduction in analysis traffic means fewer false positive alerts
- Next generation detection rules can be written using powerful SIEM search languages
- Able to replicate existing Snort or Suricata IDS rules, where needed

Faster detection

- 95% reduction in network traffic that requires analysis
- Security analysts gain more time for threat hunting, as they can spend less time preparing analysis data
- More efficient detection rules

E:info@botprobe.co.uk T:01223 852824