TEMPERED NETWORKS®

Highly Available. Radically Secure. Remarkably Simple.

Use Case

Stop Malware Propagation by Eliminating Recon and Command & Control

Identity-Defined Networking: Instant Overlay Networking

The Inevitable Security Breach

Malware is a pervasive problem and a weekly news story across the world. In most malware attacks, infected devices are used as pivot points to the rest of the network where attackers will scan the network for valuable systems and data. Once infected, devices will reach out to Command-and-Control (C&C) servers that send commands and receive outputs of compromised systems. Unfortunately, as the attacks are becoming more advanced, the breaches are becoming more difficult to uncover—until it's too late.

Cloaking Delivers Stronger Security

With our IDN solution, critical systems and endpoints are cloaked to prevent reconnaissance. Your protected devices and networks have no visible IP footprint and will not respond to any untrusted device or system—meaning ones that haven't been whitelisted onto your IDN overlay network. Even if one of your devices was compromised, IDN eliminates its ability to communicate out to a C&C server, reducing your attack surface by as much as 90%.

Stop Attacks in Their Tracks

- Eliminate DDOS, MiTM attacks, IP spoofing and other types of network and transport layer attacks
- Grant network access to only authenticated, authorized, and accountable (AAA) machines
- Gain a previously unattainable level of isolation and containment through peer-to-peer encryption and segmentation

Decrease IT CapEx and OpEx costs as much as:

50%

Reduce networking & resource provisioning time up to:

97%

Reduce attack surface by up to:

90%

To learn more or schedule a no obligation demo, email: info@temperednetworks.com or visit www.temperednetworks.com

 |