Featured news

- MagSpoof: A device that spoofs credit cards, disables chip-and-PIN protection
- Another root CA cert with key found on Dell's machines
- ModPOS: The most sophisticated POS malware to date
- Amazon resets customers' potentially compromised passwords
- IoT attacks and evasion techniques will characterize threats in 2016
- Vonteera adware blocks AVs, can install uninstallable Chrome extensions
- Five big technology predictions into 2016
- Remote working on the rise despite security concerns
- Five ransomware safety tips for online retailers
- How data protection regulations will affect the infosec industry
- Network protocol analyzer Wireshark 2.0 released
- Credential manager system used by Cisco, IBM, F5 has been breached
- Zero detection GlassRAT operated undetected for years
- Analytics services are tracking users via Chrome extensions
- Inside the largely unexplored world of mainframe security
- Ivan Ristic and SSL Labs: How one man changed the way we understand SSL

IoT attacks and evasion techniques will characterize threats in 2016

Posted on 25 November 2015.

As in years past, the Internet of Things and cloud play heavily in the predictions but new malicious tactics and strategies will create unique challenges for vendors and organizations alike, according to FortiGuard researchers.

They also predict the emergence of increasingly sophisticated evasion techniques that will push the boundaries of detection and forensic investigation as hackers face increasing pressure from law enforcement.

The top cybersecurity trends for 2016 include:

Increased M2M attacks and propagation between devices

Several troublesome proofs of concept made headlines in 2015 demonstrating the vulnerability of IoT devices. In 2016, though, we expect to see further development of exploits and malware that target trusted communication protocols between these devices. FortiGuard researchers anticipate that IoT will become central to "land and expand" attacks in which hackers will take advantage of vulnerabilities in connected consumer devices to get a foothold within the corporate networks and hardware to which they connect.

Worms and viruses designed to specifically attack IoT devices

While worms and viruses have been costly and damaging in the past, the potential for harm when they can propagate among millions or billions of devices from wearables to medical hardware is orders of magnitude greater. FortiGuard researchers and others have already demonstrated that it is possible to
infect headless devices with small amounts of code that can propagate and persist. Worms and viruses that can propagate from device to device are definitely on the radar.

Attacks on cloud and virtualized infrastructure

The Venom vulnerability that surfaced this year gave a hint about the potential for malware to escape from a hypervisor and access the host operating system in a virtualized environment. Growing reliance on virtualization and both private and hybrid clouds will make these kinds of attacks even more fruitful for cybercriminals. At the same time, because so many apps access cloud-based systems, mobile devices running compromised apps can potentially provide a vector for remotely attacking public and private clouds and corporate networks to which they are connected.

New techniques that thwart forensic investigations and hide evidence of attacks

Rombertik garnered significant attention in 2015 as one of the first major pieces of "blastware" in the wild. But while blastware is designed to destroy or disable a system when it is detected (and FortiGuard predicts the continued use of this type of malware), "ghostware" is designed to erase the indicators of compromise that many security systems are designed to detect. Thus, it can be very difficult for organizations to track the extent of data loss associated with an attack.

Malware that can evade even advanced sandboxing technologies

Many organizations have turned to sandboxing to detect hidden or unknown malware by observing the behavior of suspicious files at runtime. Two-faced malware, though, behaves normally while under inspection and then delivers a malicious payload once it has been passed by the sandbox. This can prove quite challenging to detect but can also interfere with threat intelligence mechanisms that rely on sandbox rating systems.

Internet of Things

Keep your business secure and compliant
Automatic patch management and vulnerability scanning
Try it out for FREE for 30 days!
GFI LanGuard™
Network security scanner and patch management

DON'T MISS
Wed, Nov 25th

- Another root CA cert with key found on Dell's machines
- Vonteera adware blocks AVs, can install uninstallable Chrome extensions
- Credential manager system used by Cisco, IBM, F5 has been breached
- Inside the largely unexplored world of mainframe security
- Ivan Ristic and SSL Labs: How one man changed the way we understand SSL

Back to TOP