FORTINET

November 24, 2015

FortiGuard Labs Researchers Predict That IoT Attacks and New Evasion Techniques Will Characterize Emerging Threats in 2016

SUNNYVALE, CA -- (Marketwired) -- 11/24/15 -- As 2016 approaches, Fortinet® (NASDAQ: FTNT) -- global leader in high performance cybersecurity solutions -- and its threat research division, FortiGuard Labs, have made their annual predictions of the most significant trends in malware and network security going into 2016. As in years past, the Internet of Things (IoT) and cloud play heavily in the predictions but new malicious tactics and strategies will create unique challenges for vendors and organizations alike. FortiGuard also predicts 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.

New Rules: The Evolving Threat Landscape in 2016 report is designed to reveal the new trends and strategies that FortiGuard researchers anticipate cyber criminals will employ in the year to come. Fortinet researched these predictions to arm our customers with the knowledge they need to maintain their advantage in the cybersecurity arms race and proactively change the way all businesses look at their security strategies going into the new year.

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.

Each of these trends represents a significant and novel challenge for both organizations deploying security solutions and for vendors developing them. Fortinet is on the cutting edge of threat research and network security, providing complete network protection from edge to endpoint, continuously updated by FortiGuard and the threat intelligence feeds from millions of devices deployed worldwide.

As Derek Manky, global security strategist for Fortinet explained, "FortiGuard Labs was formed over a decade ago to monitor and detect the latest threats, zero days, and emerging malware to provide the best possible protection for our customers. We leverage our incredible visibility into the global threat landscape to develop actionable threat intelligence, allowing us to respond quickly to new threats."

Ken Xie, Fortinet founder and CEO, also noted that "As we look ahead at the threats associated with our increasing connectedness and the proliferation of new devices, Fortinet is committed to delivering uncompromising security and further enhancing our solutions to meet both the current and future needs of our customers."

About FortiGuard Labs

The FortiGuard Labs global research team continuously monitors the evolving threat landscape and distributes on a daily basis to Fortinet customers worldwide preventative measures to protect those customers from newly introduced, sophisticated cyber-threats. More than 200 researchers and automated detection and prevention technology provide around-the-clock coverage to ensure your network stays protected, despite a sophisticated and ever-changing threat landscape. FortiGuard Labs delivers rapid updates and detailed security knowledge, providing protection from the latest threats.

About Fortinet

Fortinet (NASDAQ: FTNT) helps protect networks, users and data from continually evolving threats. As a global leader in high-performance network security, we enable businesses and governments to consolidate and integrate stand-alone technologies without suffering performance penalties. Unlike costly, inflexible and low-performance alternatives, Fortinet solutions empower customers to embrace new technologies and business opportunities while protecting essential systems and content. Learn more at www.fortinet.com, or follow Fortinet at the Fortinet Blog, Google+, LinkedIn or Twitter.

Fortinet has not independently verified statements or certifications herein attributed to third parties and Fortinet does not independently endorse such statements. Notwithstanding anything to the contrary herein, nothing herein constitutes a warranty, guarantee, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release contains forward-looking statements, including, among others, predictions related to threats, that involve uncertainties and assumptions. Threat predictions by their nature are uncertain and may not materialize, and changes of circumstances, product release delays, or other risks as stated in our filings with the Securities and Exchange Commission, located at www.sec.gov, may cause results to differ materially from those expressed or implied in this press release. If the uncertainties materialize or the assumptions prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Fortinet assumes no obligation to update any forward-looking statements, and expressly disclaims any obligation to update these forward-looking statements.

FTNT-O

Media Contact
Daniel Mellinger
Fortinet, Inc.
415-572-0216
dmellinger@fortinet.com

Investor Contact
Michelle Spolver
Fortinet, Inc.
408-486-7837
mspolver@fortinet.com

Analyst Contact
Ron Davis
Fortinet, Inc.
415-806-9892
rdavis@fortinet.com

Source: Fortinet

News Provided by Acquire Media