Fortinet December Threatscape Report Shows High Exploit Activity and Holiday Online Shoppers Targeted

Bredolab Downloader Soars Over One-Week Period to Take Advantage of Online Transactions; Ten Zero-Day Vulnerabilities Discovered

SUNNYVALE, CA, Jan 04, 2010 (MARKETWIRE via COMTEX News Network) -- Fortinet(R) (NASDAQ: FTNT) -- a leading network security provider and worldwide leader of unified threat management (UTM) solutions -- today announced its December 2009 Threatscape report showed that, while there was a general slow-down in malware activity as compared to the previous three reporting periods, one malware variant bucked the trend to deliver more than 66 percent of total malware activity for the month. The Bredolab downloader took advantage of the expected surge in holiday online shopping by loading ZBot variants onto infected machines: ZBot is commonly configured to pilfer online banking credentials. On the exploit front, MS08-067 showed up as the most actively targeted in this reporting period. December also proved to be a busy time for vulnerabilities and zero-day attacks with 157 new vulnerabilities detected, a third of which were in active attack mode.

```
--  Bredolab Rules: Overall malware volume returned to pre-October levels
    this period after several months of record activity driven by ZBot,
    Bredolab and Pushdo/Cutwail. Nonetheless, the Bredolab loader returned to
    the top spot with a vengeance this period, accounting for a whopping 66.5
    percent of total detected malware activity. Bredolab's threat only spanned
    over several days but completely overtook all other malware activity for
    the month. The seeding engines behind Bredolab have so much horsepower that
    a single seeding campaign can manipulate Threatscape volume for the entire
    period.

--  'Tis the Season to Be Jolly -- Not!: The top three in-the-wild email
    threats featured this period, predictably, captured the spirit of the
    season -- shopping and money. Going for the easy money, two of the three
    were bank phishes that try to get recipients to click on a link with
    notification of (a) fraudulent credit card activity and (b) incomplete
    Discover Card account information. The third most popular email threat of
    the period was a money-mule campaign disguised as a job advertisement for a
    "mystery shopper," which ultimately involves the recipient receiving money
    orders and transferring funds.

--  Exploits in Active Mode: Exploitation of MS08-067 (made infamous by
    the Conficker worm) remains the most actively attacked in this period, with
    Waledac botnet traffic being second as listed in Fortinet's Top 10 attack
    list. FortiGuard(R) Labs discovered ten zero-day vulnerabilities that were
    disclosed in December and uncovered 157 new vulnerabilities in total. On
    top of this, hackers continued to find ways to exploit zero-day attacks:
    CVE-2009-4324 was one observed through Adobe Reader/Acrobat and Javascript
    -- an increasingly common attack vector. Another zero-day was addressed by
    Microsoft through MS09-072 on December 8th.
```

"The growth in cyber criminal activity we observed in 2009 will continue with force in 2010. With more digital convergence undoubtedly to occur in 2010, there will be a wealth of opportunity for cyber criminals: There is an infinite number of victims to target, the infrastructure is already in place along with development resources, and there are ample new delivery vehicles such as social media networks to help facilitate cyber criminal activities," said Derek Manky, project manager, cyber security and threat research, Fortinet. "Digesting all of this, it becomes apparent that we are in for a wild ride in 2010 -- all elements are positioned for a perfect storm in cyberspace."

FortiGuard Labs compiled threat statistics and trends for December based on data collected from FortiGate(R) network security appliances and intelligence systems in production worldwide. Customers who use Fortinet's FortiGuard Subscription Services should already be protected against the threats outlined in this report.

To read the full December Threatscape report which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_december_2009.html. For ongoing threat research, bookmark the FortiGuard Center (http://www.fortiguardcenter.com/) or add it to your RSS feed by going to http://www.fortinet.com/FortiGuardCenter/rss/index.html. Additional discussion on security technologies and threat analysis can be found at the FortiGuard Blog at http://blog.fortinet.com. To learn more about FortiGuard Subscription Services, visit http://www.fortinet.com/products/fortiguard.html.

FortiGuard Subscription Services offer broad security solutions including antivirus, intrusion prevention, Web content filtering and anti-spam capabilities. These services help enable protection against threats on both application and network layers. FortiGuard Services are updated by FortiGuard Labs, which are designed to enable Fortinet to deliver a combination of multi-layered security intelligence and zero-day protection from new and emerging threats. For customers with a subscription to FortiGuard, these updates are delivered to all FortiGate, FortiMail(TM) and FortiClient(TM) products.

About Fortinet (www.fortinet.com)

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2009 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

FTNT-O

Media Contacts:
Kim Nguyen
Fortinet, Inc.
408-486-5458
knguyen@fortinet.com

SOURCE: Fortinet

mailto:knguyen@fortinet.com

News Provided by COMTEX