Fortinet August Threat Landscape Report Shows Return of Ransomware and Rise of 'Do-It-Yourself' Botnets

TotalSecurity Adopts Polymorphic Server Technique to Boost Reach

SUNNYVALE, CA, Sep 01, 2010 (MARKETWIRE via COMTEX News Network) -- Fortinet(R) (NASDAQ: FTNT) -- a leading network security provider and a worldwide leader of unified threat management (UTM) solutions -- today announced its August 2010 Threat Landscape report, which showed ransomware variant TotalSecurity with its biggest comeback since March. Ransomware is malware that locks out applications and data from a user's PC and then demands ransom for restored access, and TotalSecurity loader (W32/FakeAlert.LU) was the no. 1 malware detected this month by Fortinet's FortiGuard Labs.

"One indicator we observed this month was that the Ransomware application had gone server-side polymorphic, which means that the loader will connect to a single server and request a single file, but the code changes on an hourly basis in order to avoid detection," said Derek Manky, project manager, cyber security and threat research, Fortinet. "This is a technique typically seen with botnets, such as Waledac, and has been picked up by the developers of TotalSecurity. This is another example of how relying purely on antivirus is not a silver-bullet approach to protecting systems from infection."

"Do-It-Yourself" Botnet Kits In addition to ransomware, another highly detected infection this month is Zeus/ZBot, a do-it-yourself botnet kit that provides a malware creator all of the tools required to build and administer a botnet. The Zeus tools are primarily designed for stealing banking information, but they can easily be used for other types of data or identity theft. This month, ZBot variants were noted to target U.S. military personnel. A control panel application is used to maintain/update the botnet, and to retrieve/organize recovered information. A configurable builder tool allows the author to create the executables that will be used to infect victim's computers.

"We continue to monitor for in-the-wild Zeus/ZBot attacks, and due to the kit's prevalence we continuously release antivirus detection for these when they occur," Manky said. "Generic detection is also available to try to stay ahead of future variants, while FortiGuard web filtering will also help guard against malicious controller domains."

One other notable attack this month is the recent Windows Help Center vulnerability, which was propelled to the front position in our top 10 attack list. The attack (CVE-2010-1885) experienced an exceptionally large spike in activity earlier in the month. Exploitation of this attack can be rather potent since the vulnerability is not Web browser-specific.

FortiGuard Labs compiled threat statistics and trends for August 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 July Threat Landscape report which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_august_2010.html. For ongoing threat research, bookmark the FortiGuard Center or add it to your RSS feed. Additional discussion on security technologies and threat analysis can be found at the Fortinet Security 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 protect against threats on both application and network layers. FortiGuard Services are updated by FortiGuard Labs, which enables 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 a 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.

not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiDB and FortiWeb. Other trademarks belong to their respective owners. Fortinet has not independently verified statements or certifications herein attributed to third parties and Fortinet does not independently endorse such statements. This news release may contain forward-looking statements that involve uncertainties and assumptions. 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, including but not limited to, any statements related to expected trends in cybercriminal activity. These trends are difficult to predict and any stated expectations regarding these trends may not ultimately be correct. Fortinet assumes no obligation to update any forward-looking statements, and does not intend to update these forward-looking statements.

FTNT-O

Media Contact:
Rick Popko
Fortinet, Inc.
+1-408-486-7853
rpopko@fortinet.com

SOURCE: Fortinet

mailto:rpopko@fortinet.com