

Fortinet - a market-leading network security provider and worldwide leader of unified threat management (UTM) solutions today announced that its July 2009 Threatscape Report showed aggressive eCard spam activity throughout the reporting period. The FortiGuard Global Security Research Team reported this threat trend alongside others, including two exploits in the wild, growing mobile threats and a first-place showing for the ever-present online gaming malware variant.

Canadian Pharmacy assaults Google Groups, Tinypic: Fortinet saw a flood of eCard spam continuing from last month and using various techniques, with a majority of them leading victims to Canadian Pharmacy domains. Canadian Pharmacies success, fueled by an affiliate sponsorship model, invites cyber criminals to advertise the fraudulent pharmaceuticals and drive traffic to their domains. In this period, eCard spam primarily used direct links, Google Groups and the photo sharing service Tinypic as their distribution vehicles. While traditional spam continues to thrive through email, Fortinet has predicted and reported on many spam attacks that are occurring through new Web 2.0 platforms such as social networking sites. To help evade detection, cyber criminals have, in the past, used services such as Tinyurl to obfuscate their malicious URLs. Tinypic is a similar and recent example of how legitimate service providers are used to piggyback malicious resources.

Two in-the-wild exploits make waves: The first of the two exploits is the highly discussed MS ActiveX Video control vulnerability, patched on July 14th by Microsoft MS09-032. Exploit activity for this vulnerability was frequent throughout the month, but remained relatively low with most prevalent activity detected in Korea, China and Japan. As of this writing, the second vulnerability, MS Office Web Components, remains unpatched/zero-day, also with relatively low detection rates with leading activity in China, India and Japan. Exploits against zero-day tend to be more successful since patches are not readily available. FortiGuard IPS is capable of detecting and blocking malicious activity against both of these attacks. The FortiGuard Global Security Research team first spotted public exploit code for this second vulnerability on July 11th.

Mobile threat

development continues: In July, Fortinet saw the emergence of SymbOS/Yxes.E and SymbOS/Yxes.F, the latest updated variants of Yxes that Fortinet first reported in February. In particular, Yxes served up dynamic content to show the beginning steps of how cyber criminals are addressing a market that is fragmented due to multiple platforms. This is important because malicious binaries are often written for a single target (i.e., Windows, OS/X). On traditional desktops, these targets are limited; however, in the mobile market, the number of platforms are growing and diversifying and offers many more possible targets.

Virut posts record

levels; online gaming trojans flood cyberspace: W32/OnlineGames.BBR maintained and built heavily from its first place position last report -- accounting for 43 percent of total detected malware activity. This latest attack saw much of its volume from July 5th onward, with a peak of activity on July 8th. Aside from this, the regular faces of W32/Virut.A and JS/PackRedir built on their activity from the last report. In fact, Fortinet's detected activity for W32/Virut.A this period climbed to record levels, underscoring the fact that this behemoth has become a dominant threat --particularly in Asia.

With users flocking

to popular Web 2.0 tools, including social networking sites, cyber criminals are following the masses and using these emerging platforms as new threat-delivery mechanisms with success, said Derek Manky, project manager, cyber security and threat research, Fortinet. This is an especially effective strategy as users can view social media tools to be a trusted network. But, regardless of the image or what the link appears to be, users should always observe where any hyperlink will actually take you and exercise due care.

The FortiGuard research team

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

To read the full July Threatscape

report which includes the top threat rankings in each category, please visit: http://www.fortiguardcenter.com/report/roundup_july_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 the FortiGuard Global Security Research Team, 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 and FortiClient products.

About Fortinet (www.fortinet.com)

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, VPN, spyware prevention and antispyware -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in six programs by ICSA Labs: Firewall, Antivirus, IPSec VPN, SSL VPN, Network IPS, and Antispyware. Fortinet is privately held and based in Sunnyvale, California.

###

Copyright

2009 Fortinet, Inc. All rights reserved. The symbols and denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are 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.