HOT TOPICS

Special Report: The Micro Cloud
2012 Budget
Cloud / Virtualization
Contracts and Procurement
CXOs
Defense
Enterprise Architecture
Government 2.0
Health IT
Homeland Security
Management and Workforce
Policy and Funding
Program Management
Security / Cybersecurity
State and Local
Telework
Training and Certification

FCW OPINION

Blogs
Columns

Resource Center

Special Report: Virtualization and Consolidation
New! The STAND: Rugged IT
New! NASA SEWP IV Contract Guide
CHESS Special Report

Printable Format E-Mail this page

0 Recommend Neale Mahoney recommends this.

Recommended reading

By FCW Staff Jan 25, 2011

Wiser year-end spending

Source: Harvard and Stanford universities

It's hard not to notice the rush of spending that occurs at the end of the government's fiscal year, when managers try to use what's left of their budgets so they don't lose those funds. But is that money well spent?

Federal spending on IT projects in the last week of the fiscal year — the last week of September — is seven times higher than the weekly average for the rest of the year, according to a report by **Jeffrey Liebman and Neale Mahoney**, economists at Harvard and Stanford universities, respectively. That spike is a persistent feature across agencies and over time.

The researchers also saw a sharp drop-off in the quality of investments and the performance of projects that received lavish year-end spending. Significantly, neither trend was as prominent at the Justice Department, which has obtained special authority to roll unused funds into the next fiscal year's budget.

Although the authors said it was difficult to draw firm policy conclusions from the research, they did offer some ideas, including switching to a two-year budget cycle and applying increased scrutiny to year-end spending.

Malware: It's not just for techies anymore

Source: Network World

Bill Snyder at **Network World** notes that 25 years ago, two brothers from Lahore, Pakistan, introduced the first malware that could infect a DOS-based PC. They said they did it to protect their medical software from piracy.

Times certainly have changed. "No longer just a way to make a political point or demonstrate one's technical prowess, malware has become a useful tool in the bag of tricks bad guys use to steal from consumers and institutions alike," Snyder writes.

And he points to a particularly disturbing trend: "the production and online sale of 'kits' that allow relatively unskilled hackers to create and launch malware attacks."

Such kits usually contain prewritten malicious code and all the necessary tools for customizing and launching an attack, which means even unskilled hackers can launch damaging attacks by the thousands. Some of the higher-end kits "offer online support and subscription services, so customers can get updated versions of the malware," Snyder writes.

« previous 1 2 next »

Related Articles

- What LulzSec teaches us about hacktivism 07/07/2011
- Federal 100: Gary 'Gus' Guissanie 03/28/2011
- 9 things feds should know about secure international travel 09/15/2010

Most Popular Articles | Most Emailed Articles

Union launches campaign in defense of feds
Pay for performance? Yeah, right.
NSPS: anatomy of a failure
Agency to standardize on mobile tech
DOD cyber defense plan draws fire

Related Webcasts

- Delivering Secure Mobile Operations to the Warfighter-From Concept to Reality
- Mapping Identity Credential and Access Management to Meet Inter-Agency and Private Cloud Interoperability Challenges
- Using Continuous Monitoring for Improving Cyber-Situational Awareness

Related White Papers

- INSIGHTS: IT Modernization
- Strengthening Our Nations Security by Building a Trusted Identity Environment
- Why Smart, Innovative Businesses are Turning to Cloud Computing

Related Podcasts

- Counter the Insider Threat with Security Intelligence

Related Resources

- Evolving cyber threats demand coordinated defense
- Funding, self-awareness stymie consolidation efforts
- Metrics matter when setting consolidation goals
- Is securing data easier than securing entire systems?
- Centralized computing catches fire with lower costs, easier maintenance, better security

GSA IT Schedule 70 Special Report

Insights Special Report: IT Modernization

The STAND: Information Security

Client Computing Special Report

Rugged IT Special Report

Cloud Computing Special Report

Collaboration Tools Special Report

The STAND: Virtualization

Securing Government Systems Special Report

2011 DISA Contract & Program Guide

2010-2011 Library

- US-CERT systems riddled with vulnerabilities, audit finds 09/09/2010
- Malware's role in fatal 2008 air crash 09/01/2010

Share this Page

LinkedIn Facebook Twitter Google Slashdot

Reader comments

Please post your comments here. Comments are moderated, so they may not appear immediately after submitting. We will not post comments that we consider abusive or off-topic.

(optional) Your Name:

(optional) Your Email:

(optional) Your Location:

Comment:

NUAV

Please type the letters/numbers you see above

Submit

Editorial Webcasts

Delivering Secure Mobile Operations to the Warfighter-From Concept to Reality

The proliferation of mobile devices in the marketplace is changing how Federal agencies share information, collaborate, and conduct business. Register now to attend this Webcast where you will learn about DOD plans to address specific mobile security requirements, meet challenges, and leverage technologies for enhanced secure remote access. **Read more**

More Editorial Webcasts

Federal Computer Week eNewsletters

SUBSCRIBE

Subscribe to Newsletters

Federal Computer Week's eNewsletters deliver the latest policy and management news to your inbox.