

HELP NET SECURITY

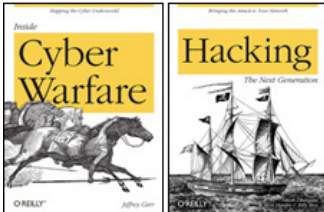
HOME NEWS ARTICLES SOFTWARE SERVICES DATA STATE AFFAIRS SEARCH RSS INSIDE MAGAZINE
 COPYRIGHT 1998-2010 BY HNS CONSULTING LTD. // READ OUR PRIVACY POLICY //



LATEST NEWS >> Friday, 18:12 EST

Hackers steal \$50,000, bank refuses to assume responsibility
 Lawful wiretap interfaces accessible to cyber criminals?
 Rogue software details: MalwarePro Chip and PIN system on banking cards seriously flawed
 Google Buzz for spammers
 Fake AV's double attack
 Simulated cyber attack will test US Government response
 Critical infrastructure is a primary cybercriminal target
 Hacking games: Key to finding cybersecurity talent
 Security advice for Valentine's Day
 Rogue software details: Security Antivirus
 Will virtualization and cloud computing change how we achieve security?

LATEST REVIEWS



Critical infrastructure is a primary cybercriminal target

Posted on 11 February 2010.



Critical infrastructure such as energy, pharmaceutical and government assets are more than twice as likely to be targeted by cybercriminals than other organizations, according to a ScanSafe report.



The report is based on an analysis of more than a trillion Web requests processed in 2009 by the ScanSafe Threat Center on behalf of the company's corporate customers in more than 100 countries. It represents the world's largest security analysis of real-time traffic.

This research reflects a disturbing trend – organizations that harness the most valuable intellectual data are encountering Web malware with much greater frequency than other verticals. Most at risk are:

1. Energy & Oil with a 356% greater rate of direct encounters with data theft Trojans
2. Pharmaceutical & Chemical with a 322% greater rate
3. Government with a 252% greater rate
4. Banking & Finance with a 204% greater rate.

"There is a misconception that cybercriminals are only intent on stealing data intended for credit card fraud and identity theft. In reality, cybercriminals are casting a much wider net," said Mary Landesman, senior security researcher at ScanSafe. "Consumer credit card details are child's play compared to the value of infrastructure and intellectual data from these sensitive verticals. The message is clear – cyberwar is already here. The Web is the battlefield and the enterprise is on the frontlines."

In addition, the report reveals that Web-delivered malware more than doubled through the course of the year. At the start of 2009, the average enterprise experienced 8 Web malware encounters each day. By the end of 2009, the rate of exposure had more than doubled to 19 encounters per day. Twenty-three percent of those encounters were with zero day malware undetectable by signature-based methodologies and nineteen percent were direct encounters with data theft Trojans.

Other key findings include:

Malware is the new Internet business of choice

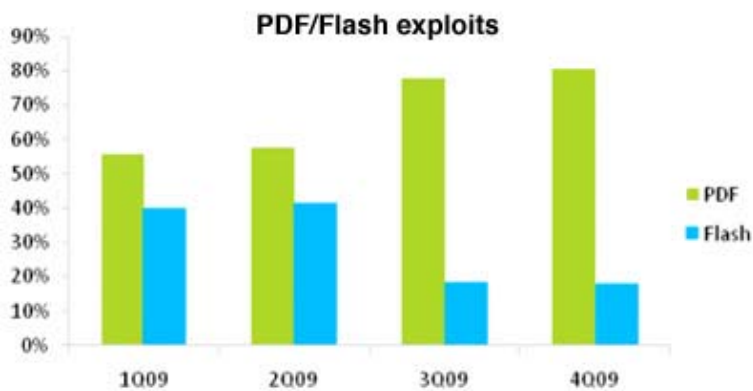
The business structure behind cybercrime today is not unlike the business structure behind any other global economy. Attackers play many roles in this commercial world including 'The Sole Proprietor', 'The Middleman', 'The Developer', and 'The Buyer'.

Gumblar botnet dominated the malware scene in 2009

14% of the total Web malware blocks for the year were from Gumblar. This peaked to 35% of all blocks in November 2009. Asprox was the second largest at 2% of all Web malware blocks and Zeus was the third largest with 1%.

Malicious PDF files are up, malicious Flash files are down

Malicious PDF files comprised 56% of Web-encountered exploits in 1Q09, growing to 80% by 4Q09. Flash exploits encountered via the Web dropped from 40% in 1Q09 to 18% in 4Q09. This trend is likely indicative of attackers' preference for PDF exploit, likely due to the increasing availability of vulnerabilities and the continued widespread use and acceptance of PDF files in the workplace.



"To confront the challenges of the coming years, we must reposition our thinking to match the new reality. We must forgo our perceived familiarities and see the issues that are already at hand – the criminal business of data harvesting," comments Landesman. "Our defenses must extend beyond the confines of brick and mortar and into the cloud to ensure end-to-end protection of our most sensitive assets and people, regardless of operating system, device or geo-locale."

For a copy of the ScanSafe Annual Global Threat Report, go [here](#). (Registration required)

GF Take care of your security vulnerability management needs with... 
GF LANguard – Freeware

 Download your **FREE** version today!

Entrust
 SSL Certificates

 EV SSL Certs
\$199

Receive daily security news by e-mail

Subscribe