Govtech.com Security News Podcast – Episode 5:

Ransomware with 1024-bit keys, attacks hiding in data streams, policy guidelines from GFIRST Security Conference.

Tuesday, June 10, 2008

Summary

- Ransomware hold data hostage with strong 1024-bit key
- New report show spike in attacks hidden in innocent-looking internet traffic
- Security policy guidelines from GFIRST Security Conference 08, Orlando

Podcast sponsored by DeviceLock and Emergency Management Magazine.

Notes

Hijack

- Ransomware Hijack using 1024-bit encryption key

Laptop

- Stanford alerts employees that stolen laptop had personal data

Web malware

- Web-based malware on legit sites soars

New Browser Wars

- Haute Secure
- Opera
- Firefox site security policy

Stanford alerts employees that stolen laptop had personal data

- FREE whole disk encryption

Tales from the Dark Web

Spear Phishing and Whaling

Resources

Interview 1

Paul Royal, Principal Researcher at Dambala

Damballa press release based upon the work of Paul's research team

Targeted threats analyzed (i.e., the interesting part)
This spreadsheet includes document names, domains looked up, whether the malicious document stole HTTP proxy settings, C&C IPs, country of ownership for C&C, etc.

BlackHat Briefings

Interview 2

James L. Geuin, Information Security Manager, Florida Department of Law Enforcement

Jim's Presentation at the 4th Annual GFirst Security Conference, Orlando, Florida