Current Security Threats

David Perez

SANS Institute

(david.perez.conde AT gmail.com)

Yours Truly

- David Perez
- Independent Security Consultant & SANS Certified Instructor
- GIAC GSE (includes GCFW, GCIA, GCIH, GCWN, GCUX, GSNA, GCFA)

Contents

- Example of Current Threat
- Today's vs. Yesterday's Threats
- How to defend

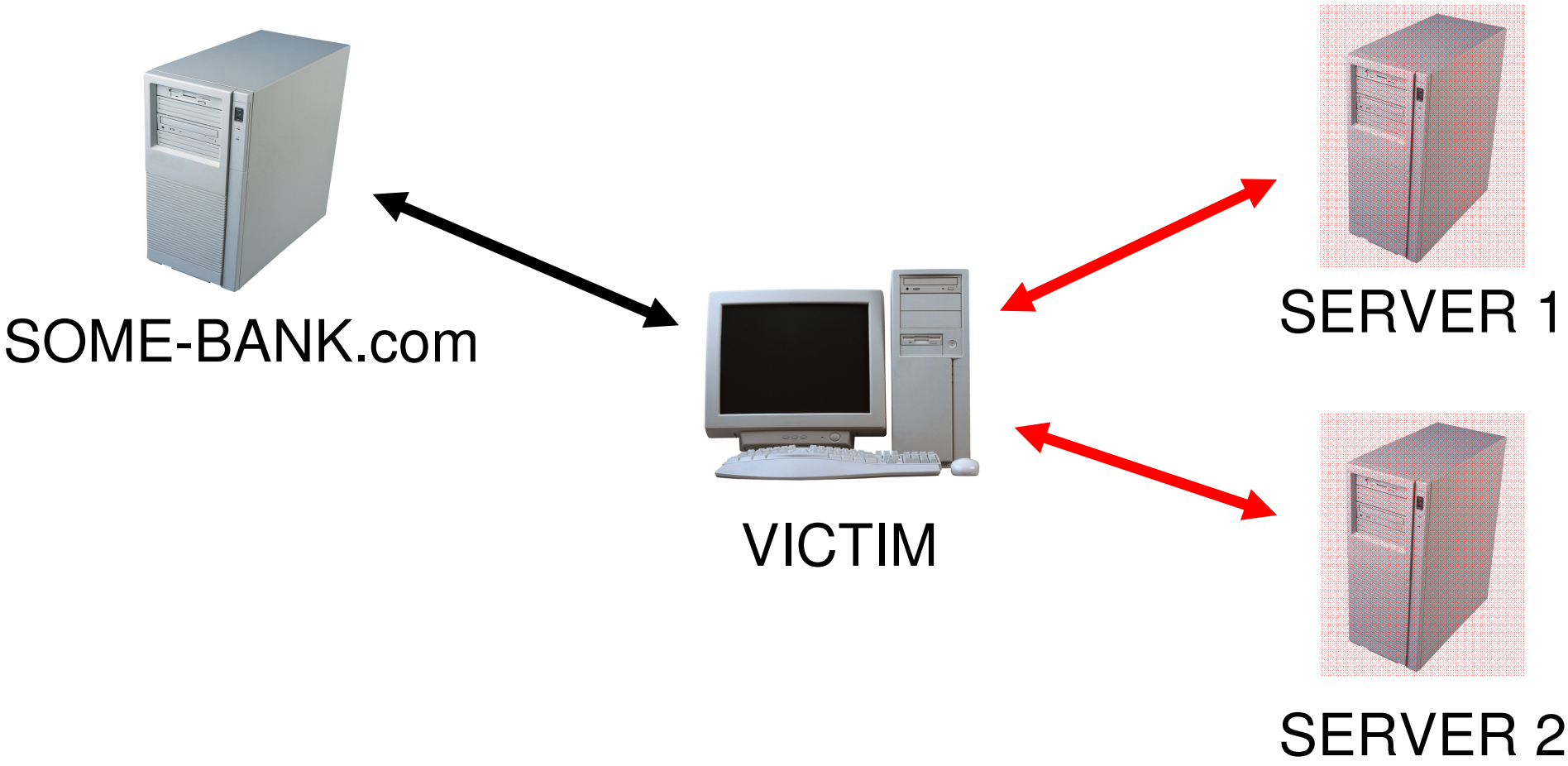
Contents

- *Example of Current Threat*
- Today's vs. Yesterday's Threats
- How to defend

Example of Current Threat

- Malicious program
- If it gets into your PC…

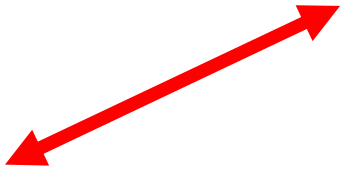
Architecture

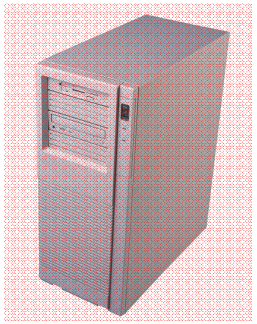


Upon Infection…

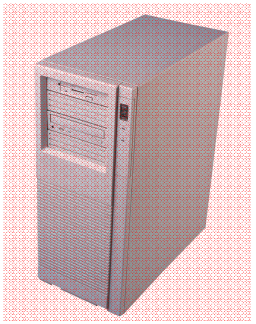
SOME-BANK.com

VICTIM





SERVER 1

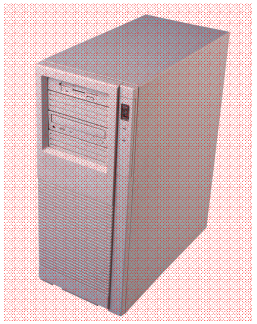


SERVER 2

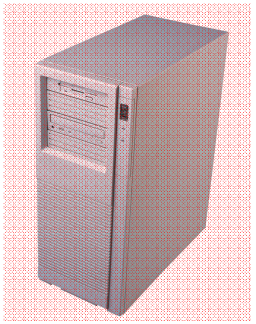
Connecting to the Bank

SOME-BANK.com

VICTIM



SERVER 1

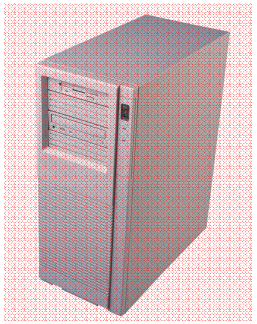


SERVER 2

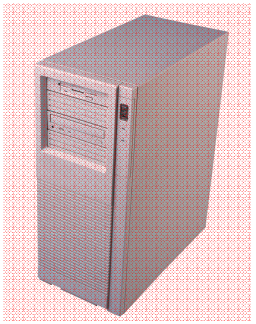
Sending Captured Data

SOME-BANK.com

VICTIM

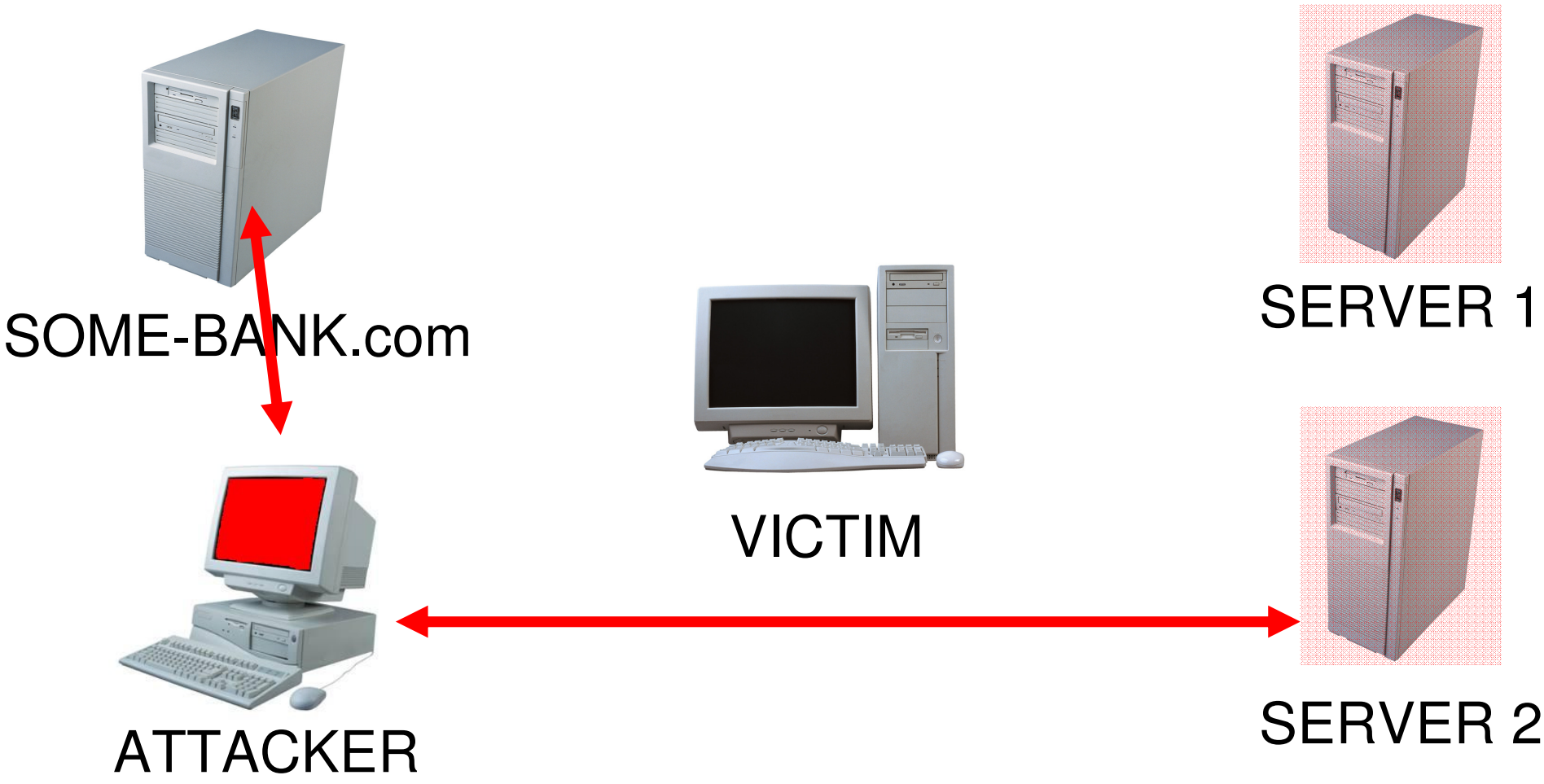


SERVER 1

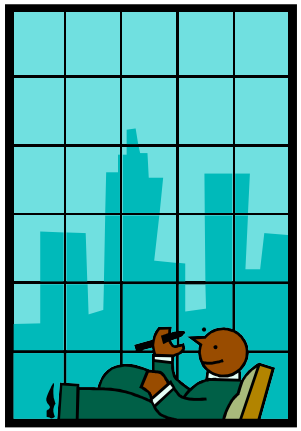


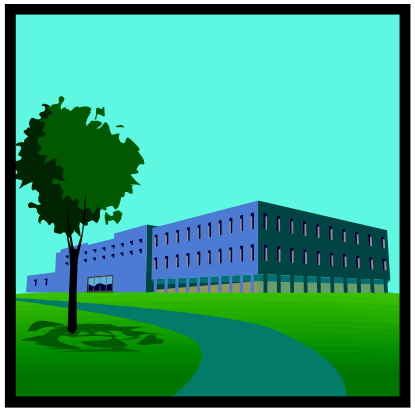
SERVER 2

Game Over!

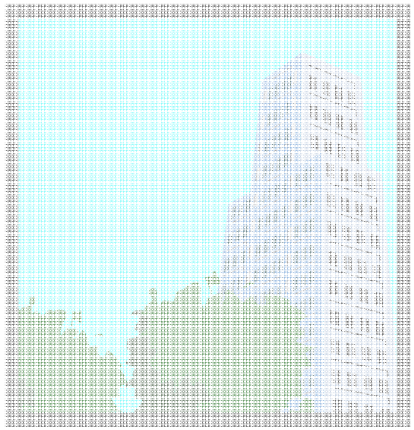


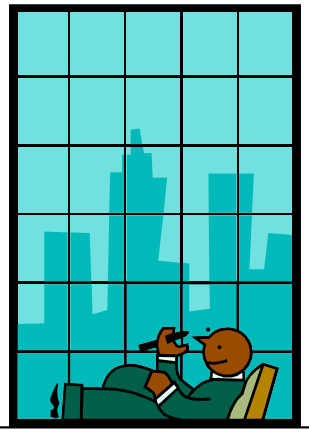
People Involved



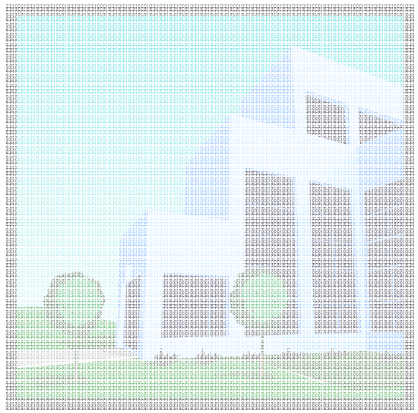


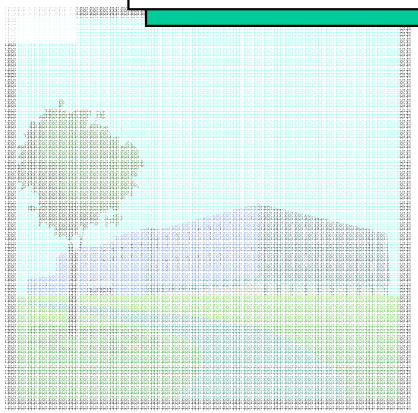
People Involved

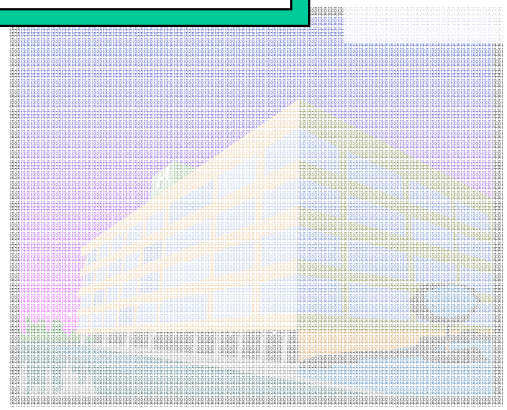




BADGUYS INC.

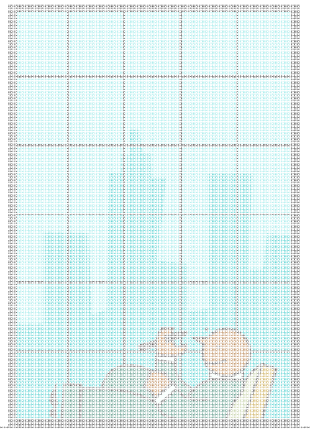




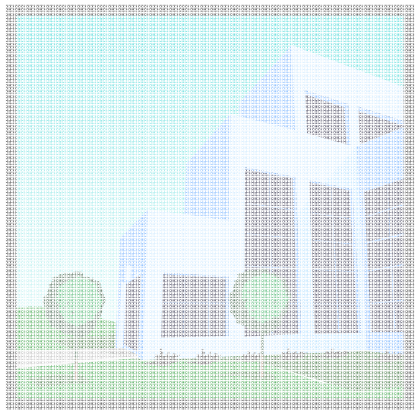


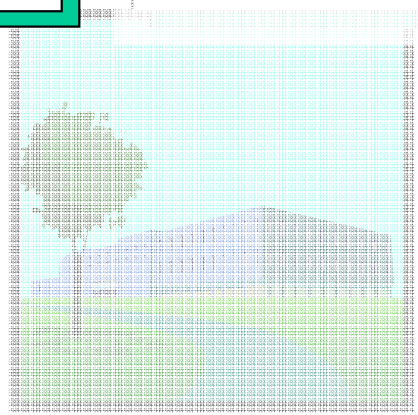
People Involved

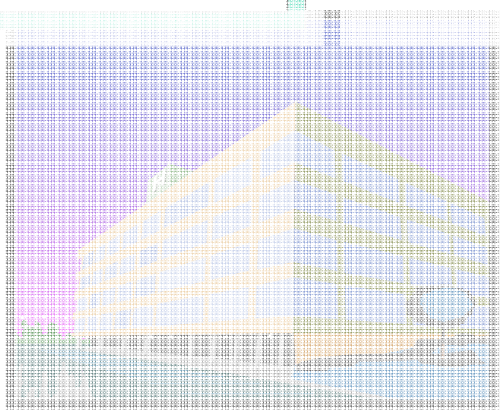
BOTNET INC.



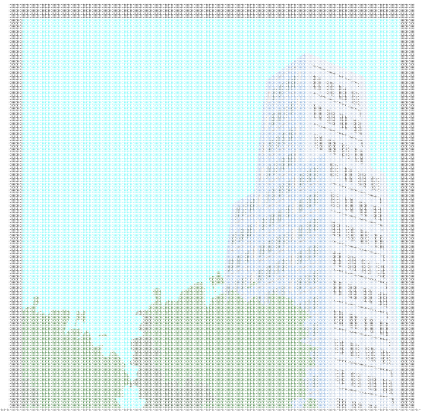
BADGUYS INC.



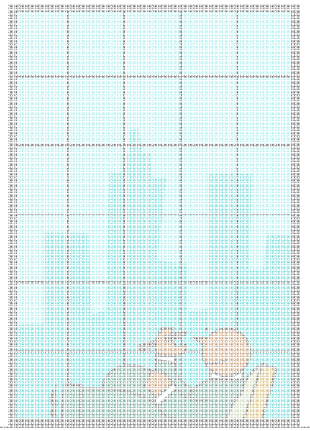




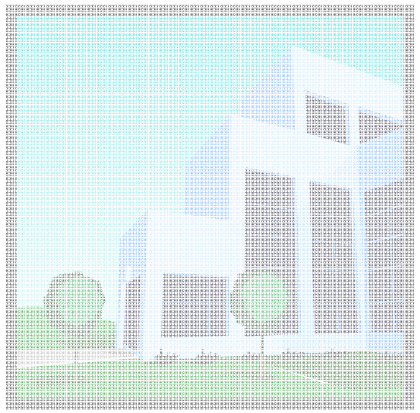
People Involved

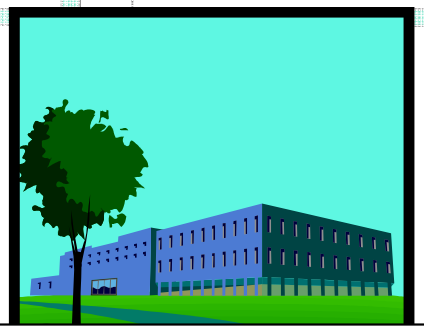


BOTNET INC.

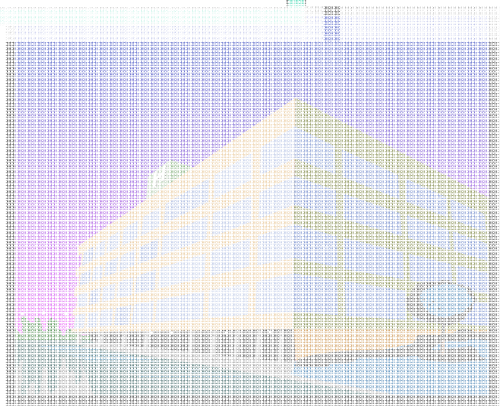


BADGUYS INC.

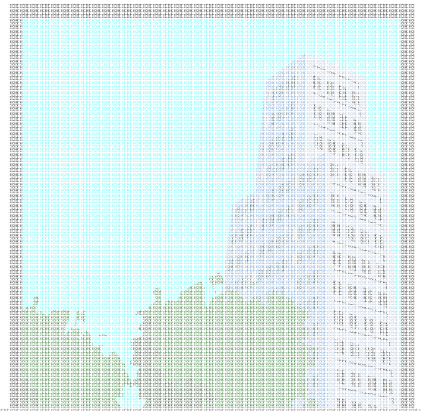




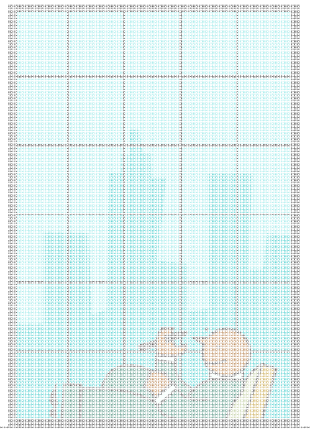
MALWARE INC.



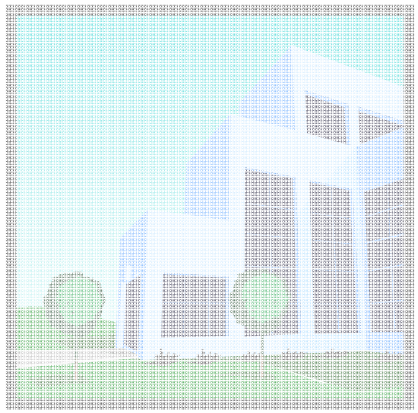
People Involved

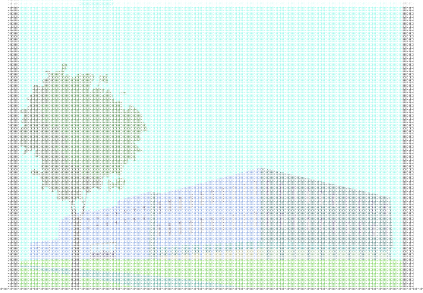


BOTNET INC.

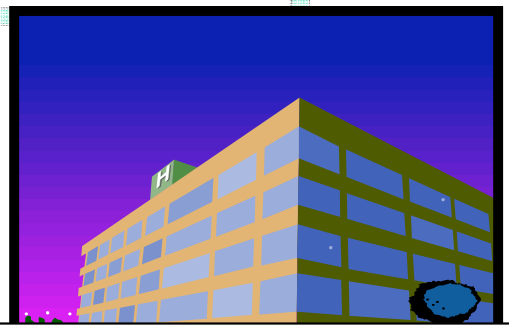


BADGUYS INC.



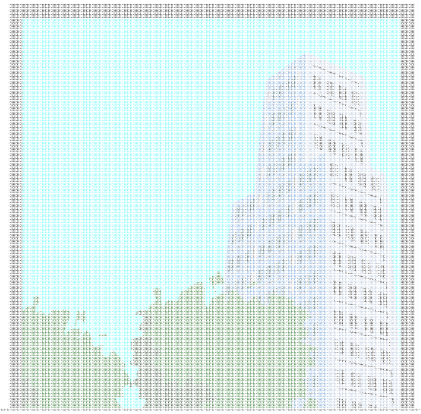


MALWARE INC.

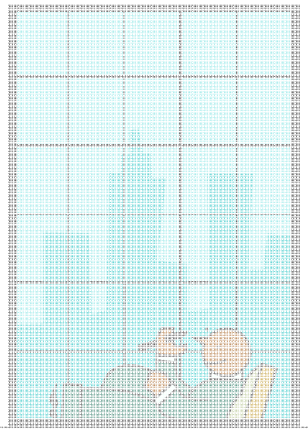


INFECTION INC.

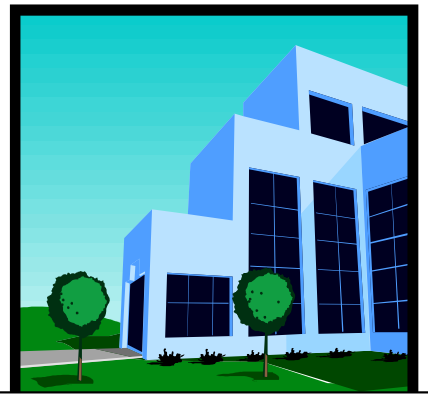
People Involved



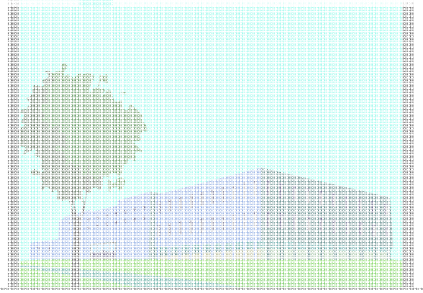
BOTNET INC.



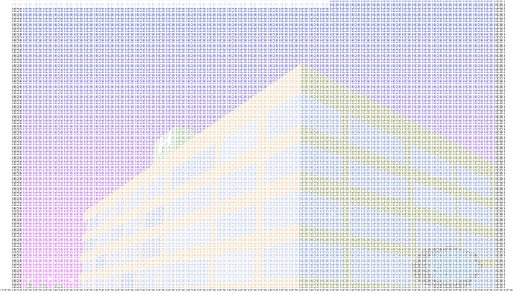
BADGUYS INC.



MALICIOUS ISP

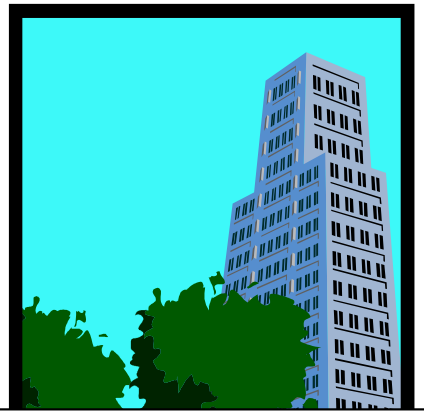


MALWARE INC.

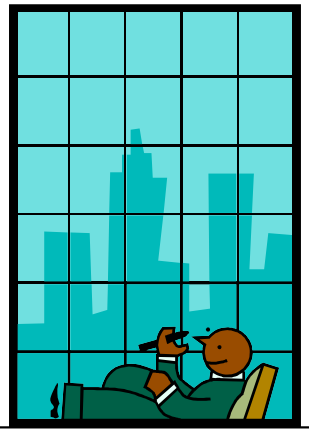


INFECTION INC.

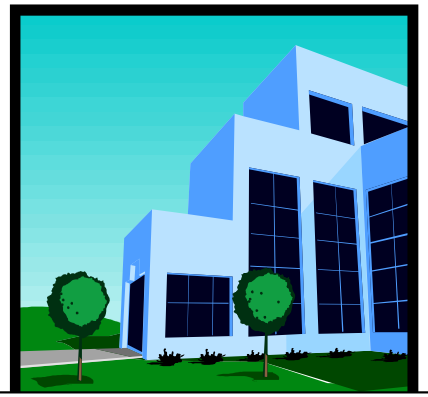
People Involved



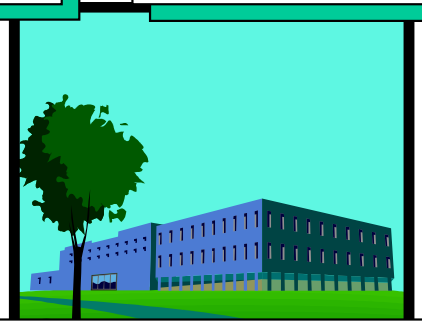
BOTNET INC.



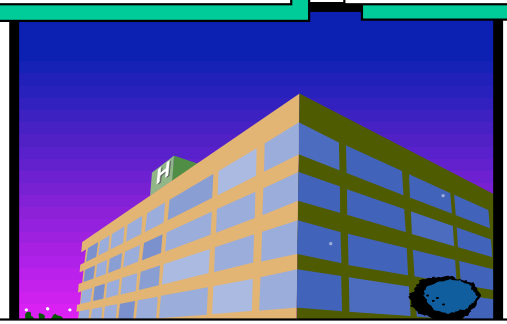
BADGUYS INC.



MALICIOUS ISP



MALWARE INC.



INFECTION INC.

Contents

- Example of Current Threat
- *Today's vs. Yesterday's Threats*
- How to defend

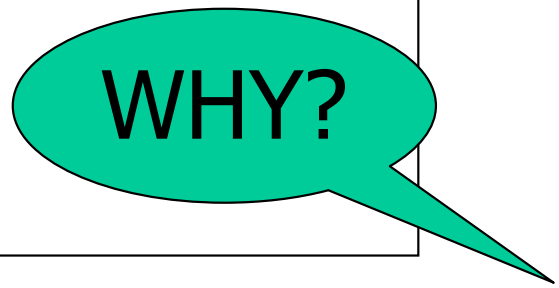
Threats

YESTERDAY

- Web Defacements
- DDoS
- Worms
- …

TODAY

- SPAM
- Phishing
- Malware
- …



Money, Money, Money!!!!!!!!

Contents

- Example of Current Threat
- Today's vs. Yesterday's Threats
- *How to defend*

Prevention

- Firewall
- IPS
- VPN
- Antivirus
- …

Detection

- IDS
- IDS
- Antivirus
- …

Response

- Forensics (Host, Network, Logs)
- Reverse-Engineering Malware
- Collaboration among CERTs
- Law Enforcement
- …

Summary

- Example of Current Threat
- Today's vs. Yesterday's Threats
- How to defend

Current Security Threats

David Perez

SANS Institute

(david.perez.conde AT gmail.com)