SANS WhatWorks Summit 2008
Forensics and Incident Response

IR/Forensics Team Tactics Panel

October 13, 2008
Las Vegas, NV

Christopher J Novak
chris.novak@verizonbusiness.com

Eric Gentry
eric.gentry@verizonbusiness.com

PROPRIETARY STATEMENT

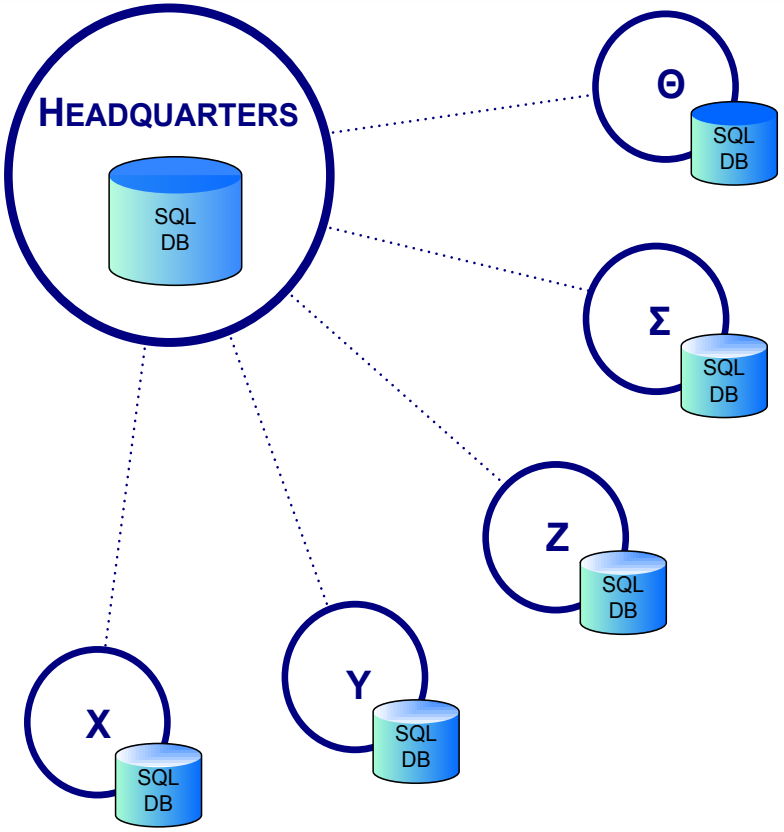
This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed, or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

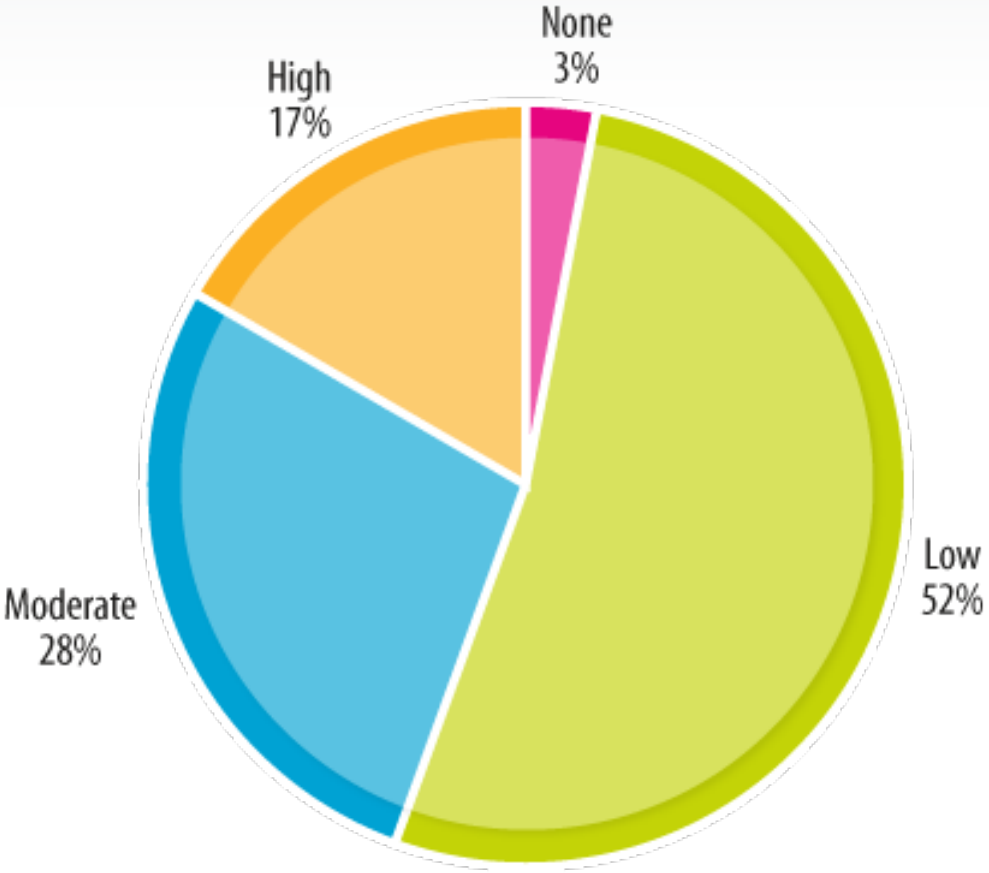
Case Study: Anti-Forensics

European bank suspected of having a data compromise.

- Local forensics firm investigated identity theft complaints, but found no evidence of a compromise.
- Bank wanted second opinion due to continued customer complaints.
- We were engaged to perform the follow-up investigation
- Determined that key evidence was missed due to AF:
  - RootAF to clean logs of IP addresses
  - Systems logs didn't match Firewall
  - Hide4Enc used to cloak data in pics
  - Encryption key extracted from memory
- Perpetrator successfully identified
- Law Enforcement handling prosecution.



How Prevalent is Anti-Forensics?



Attack Difficulty

None: No special skills or resources were used. The average user could have done it.

Low: Low-level skills and/or resources were used. Automated tools and Script Kiddies. Some Basic Anti-Forensics tools (point & click).

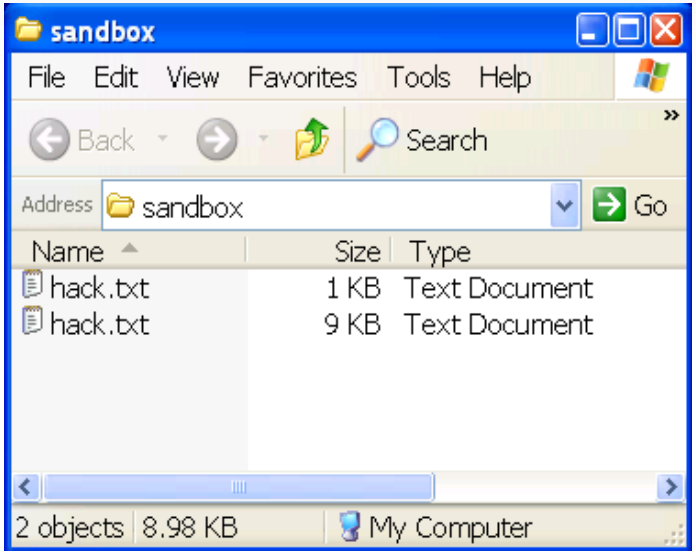
Moderate: The attack employed skilled techniques, minor customization, and/or significant resources. More sophisticated Anti-Forensics tools (some customization).

High: Advanced skills, significant customization and/or extensive resources were used. Multiple sophisticated Anti-Forensics tools (many customizations or home grown).

AF Effectiveness and Our Workarounds

Common AF Techniques Seen in the Wild:

- Zero Footprinting (Evidence Wiping)
- File Packers / Wrappers
- Data Hiding (Steganography, Encryption)
- Data Corruption / Injection
- Data Obfuscation (Letter Substitution)
- Blended Threats (Multiple Mixed AF)



Making our Case Despite Anti-Forensics:

- Many AF tools are not 100% (files may be locked, shared or in use)
- Think outside the box… Copies of wiped data may exist in less convention areas (tape backups, clustered peers, etc…)
- Evidence within the system's running memory (memdump)
- Journaled File Systems may retain some trace information or Metadata re: prior data
- When it comes to Stego… Look at the pictures…

- Understand that the case is going to take more time and set expectations accordingly…

Christopher J Novak
chris.novak@verizonbusiness.com

Eric Gentry
eric.gentry@verizonbusiness.com