Incident Response in a Collegiate University

David Ford, OxCERT
Oxford University Computing Services
OxCERT

• Founded in 1994

• Originally a number of volunteers from across the University who were interested in network security

• Now 3 full time staff members at the Computing Services
  
  Robin Stevens (Team Leader)  
  Jonathan Ashton  
  David Ford
A Collegiate University
(Some background)

• 38 Independent, self-governing colleges
• 6 Permanent Private Halls
• Numerous Faculties, Departments, Research Groups
• All with independent computer systems and IT support
• Over 20,000 full time students
• Over 76,000 registered hosts (in some sense)
• Around 38,000 Users with Accounts
• Each “unit” - typically a college or department gets a single fibre connection to the University Backbone

• The University Backbone then has a connection to the JANET(UK) connecting to the Internet

• The unit then manages their own network
Very Diverse

• Windows (from 3.1 onwards!)
• Mac OS
• Linux
• Solaris
• NeXTStep
• BSD
• Netware

and anything else you can think of!
OxCERT’s role and remit

- OxCERT’s responsibility lies at the backbone level.
- We do not see what happens beyond an individual Unit’s boundary.
- We don’t know what an individual host actually does or what software it is running.
Our Role

• “To protect the integrity of the University backbone network and to keep services running”

• This can encompass a wide range of threats

• But we’re not the network police, we don’t directly deal with copyright infringements, people viewing inappropriate materials, etc
Typical Incident types

• Keylogging malware
• Port Scanners
• Botnets
• Malicious DHCP/DNS/ARP Spoofing
• Weak Passwords leading to compromises of small or large numbers of systems
• Vulnerable Software Installations
• Spam and Phishing
Attempting to visualise our activities

• It’s hard, different types of incident have have different levels of effect on a unit

• Also our level of involvement will differ depending on the type of incident, so numeric comparisons may not be helpful

• I’ve tried to split things into three groups (but it is slightly arbitrary):

• workstation compromises/server compromises/social issues are not included
Typical “Workstation” malware

- Keylogger
- Conficker
- IRC Bot
- Other Malware
- Malicious DNS/DHCP
- Sending Spam
- Port Scanner


0 | 50 | 100 | 150 | 200

0 | 50 | 100 | 150 | 200

Oxford University Computing Services
www.oucs.ox.ac.uk

Thursday, 28 January 2010
More simply (Oct 2008 - Jun 2009)

Keylogger/Info Stealer: 42%
Malicious DNS: 36%
Other Malware: 17%
Conficker: 5%

Oxford University Computing Services
www.oucs.ox.ac.uk

Thursday, 28 January 2010
Other Incidents

• Major server compromises, averaging 1-2 a month, but rather more variable, we will look at one of these in detail later

• Phishing responses, numbers vary - typically more common at the start of the year, we are trying to increase user education

Oxford University Computing Services
www.oucs.ox.ac.uk
OxCERT’s Process

- Identify Compromised systems (or be notified of them) typically using a combination of network flows, darknets, DNS redirection and highly targeted snort rules
- Alert the “Unit” owning the IP of the incident (and impose a router block where ever possible preventing further malicious traffic)
• We do more detailed investigation, especially for major incidents, and wait for the unit to report back to us

• In some cases unit may not need further assistance, in other cases, we may be able to perform log analysis, rudimentary malware analysis, or give names of suspicious filenames/other details to look for

• Unit may report back the usage of the system at this point (eg desktop, server, student system)
• Attempt to identify potential impact:
• Other Infected Hosts
• Compromised Accounts
• Other Accounts using the same passwords
• sensitive material that may have been breached
• How did the attackers get in?

• Attempting to prevent a recurrence - often a challenge, it may well be simpler and quicker for an IT officer to immediately reinstall than to identify the cause

• But we want to avoid repeat incidents

• Also, we wish to improve our detection - what signatures/IPs/DNS-RRs would have identified this earlier
Case study: A typical large incident

- We focus here on one example
- In this case a Compromise of a Windows Domain supplying core services to a single unit
- It could equally be a Linux or Mac set of servers
• Detected by us, due to port scanning
• Brief network flow analysis suggested a compromise via Remote Desktop
• We followed our standard process as outlined earlier
Impact

- All servers used the compromised hosts for DNS, they lost external DNS
- The compromise of 4-5 hosts was leading to several hundred machines losing full connectivity
• Frequently we have incidents where there has been little planning/prior anticipation of impact of an outage

• Small IT departments make this more likely

• Sometimes we have to evaluate what impact our blocks are having and produce a work-around that minimises the impact, whilst keeping the risk of further compromise acceptable
Reports/Lessons

• We produced a full report to the affected unit, including a number of suggestions as to how to reduce the risk of a recurrence

• Unfortunately many of these seem to be common issues in a great many compromises
• Poor planning for incidents, assumption problems won’t happen, lack of ideas as to how to deal with things when they do

• Lack of good staff resources to deal with the unexpected

• Poor patching processes
• Systems allowing privileged access to the world (eg ssh, RDP) when there is no need

• Poor logging and auditing of logs to identify compromises when they happen

• Lack of appropriate separation of privileges (eg using the same credentials for administration on every workstation and server)
Other Activities

• Besides dealing with 600-1300 incidents a year

• Malware Analysis project looking at identifying what malware does so we can trace it, and give advice on how to clean it up

• Resources eg. Keylogger Guidance, NAT logging guidance
Guidance for dealing with keyloggers

These days it is extremely common to encounter sophisticated malicious software that has been designed to capture and transmit data such as passwords and bank details. Attackers are frequently making use of captured details, primarily for financial gain, but not necessarily through the traditional methods of fraudulent credit card purchases or withdrawals from bank accounts; almost any information captured potentially has value.

This document is intended to give some advice to those whose systems have been infected with such malware. If you have been affected then we encourage you to follow the advice in order to reduce the risk of your accounts being attacked. We appreciate that the advice may seem daunting, but in the long-term it may save you work. Please do not be afraid to approach your IT officer or the OUCS helpsdesk for assistance or further advice.

One first piece of advice is that if you believe your machine is infected with such malware, for example if you have been told by an IT officer that your machine is blocked for this reason, do not try to connect it to a network elsewhere until it has been cleaned. There may be data that has been captured and is stored on your machine but not yet transmitted to the attacker's site. There is nothing to be gained by giving them more of your passwords or other data.

Sections in this document:
1. Changing Passwords
2. Saved Passwords
3. Other Passwords
4. Other Information

OUCS documents are available in alternative formats through advance request from the Help Centre.
Written by David Ford, October 2008. Latest revision Thu, 14 Jan 2010

Login
Nexus email
WebLearn
Registration Services

Network Links
Network Security
Wireless Service (OWL)
Internet Telephony
Remote Access Services
Virtual Private Network (VPN)
Network Hardware Support

Document Links:
1. Changing Passwords
2. Saved Passwords
3. Other Passwords
4. Other Information

[About | Contact | Feedback | Accessibility | © University of Oxford]
Other Activities Continued

• Working with others in Academia
  eg darknet mesh project

• Monthly/Annual reports

• Security Bulletins

• Advice on where to find help with other
  "security" matters

Oxford University Computing Services
www.oucs.ox.ac.uk
Comments/Questions

http://www.oucs.ox.ac.uk/network/security

david.ford@oucs.ox.ac.uk

security@oucs.ox.ac.uk