

Liste der neuen Funktionen in TraceMagic Version 4 (ab Mai 2004):

2004	Beschreibung / Zusammenfassung
(1)	<p><b>Stapel-Verarbeitung &amp; Analyse-Profile (Analysis Profiles).</b></p> <p><i>Stapel-Verarbeitung via Job-List &amp; Meta-Start:</i></p> <p>Es ist nunmehr möglich, mehrere <b>Trace-Verzeichnisse</b> in einer <b>Job-List</b> zusammen aufzuführen und sodann automatisch abarbeiten zu lassen. Das bedeutet: HostMagic+SpiderMagic werden jeweils einzeln (und automatisch) gestartet zur Verarbeitung der Trace-Dateien jeweils eines Trace-Verzeichnisses. Alle in der Liste hinterlegten Trace-Verzeichnisse werden in einer Art von Stapel-Verarbeitung durchlaufen.</p> <p><b>AutoStart</b> hatte TMv3 auch schon: HostMagic/SpiderMagic laufen automatisch hinter einander durch. <b>MetaStart</b> kommt jetzt mit TMv4 und bedeutet:</p> <p>Es können beliebig viele Trace-Verzeichnisse in einer Job-Liste hinterlegt werden. TraceMagic durchläuft dann alle diese Trace-Verzeichnisse und verarbeitet die Trace-Daten voll-automatisch mit der AutoStart-Funktion.</p> <p>Alle Daten aller Verzeichnisse der Job-Liste werden also mit HostMagic/SpiderMagic verarbeitet.</p> <p><b>Diese Funktion ist nur in der Lizenz-Stufe „TraceMagic Professional“ nutzbar.</b></p>



## Analysis Profiles:

Weiterhin können für jedes dieser Trace-Verzeichnisses **Analyse-Profile** hinterlegt werden, die festlegen, mit welchen Analyse-Funktionen SpiderMagic arbeiten soll. Es ist sogar möglich, je Trace-Verzeichnis mehrere SpiderMagic-Analysen zu veranlassen mit jeweils eigenen (getrennten) Analyse-Funktionen (je SpiderMagic-Durchlauf ein eigenes Analyse-Profil).

Je Trace-Verzeichnis können nunmehr Verarbeitungs-Profile hinterlegt werden. Oder, andere Sicht: HostMagic/SpiderMagic können mit benutzer-definierten Einstellungen betrieben werden. Diese Einstellungen werden in "Analyse-Profilen" gespeichert.

Wird mit MetaStart und Job-Liste gearbeitet, können jedem Trace-Verzeichnis beliebig viele Analyse-Profile zugeordnet werden.

Werden z.B. für ein bestimmtes Trace-Verzeichnis 3 SpiderMagic Analyse-Profile hinterlegt, wird TraceMagic die Daten dieses Trace-Verzeichnisses 3 Mal verarbeiten.

**Diese Funktion ist nur in der Lizenz-Stufe „TraceMagic Professional“ nutzbar.**

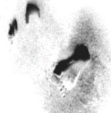
(2)

## Unix-Protokolle.

Es werden jetzt folgende klassische Unix-Protokolle mit „simple decoding“ unterstützt:

FTP, TELNET, SMTP, POP3, RPC-PMAP, RPC-MOUNT, RPC-NFS, LPR.

„Simple Decoding“ bedeutet, dass die entsprechenden LAN-Pakete im Event-Log dargestellt werden; eine eigene Analyse-Intelligenz ist nicht gegeben.



	<p>Bei der SMTP-Analyse kann automatisch ein spezifischer Fehler zwischen Outlook-Mail-Servern und SMTP-Mail-Servern erkannt werden, der teils zu Timeouts führt, teils zur Nicht-Erkennung von Mail-Attachments.</p>
(3)	<p><b>SpiderMagic → Rx/Tx</b></p> <p>SpiderMagic unterstützt erstmals Statistiken, die nicht nur die <b>Tx-Richtung</b> (Tx = Transmit = Senden) erfassen, sondern auch die <b>Rx-Richtung</b> (Rx = Receive = Empfangen); es werden also auch Ereignisse der Empfänger-IP-Adresse zugeordnet, nicht mehr nur der Sender-IP-Adresse. Dies ist insbesondere bei ICMP-Meldungen von großer Bedeutung.</p>
(4)	<p><b>SpiderMagic → "rc.files"</b></p> <p><u>Reconstructed Files Menu:</u></p> <p>Wurde zur Darstellung der durch SpiderMagic rekonstruierten Dateien ("reconstructed files" = "rc.files") noch der Windows-Explorer aufgerufen (was die Suche nach einer bestimmte Datei sehr behindern konnte),</p> <p>so wird ab TMv4 ein eigenes Datei-Menü aufgerufen, das es über einfache Filter erlaubt, die gesuchte(n) Datei(en) sehr schnell zu finden.</p> <p><u>Script Follow-Up:</u></p> <p>Außerdem wird der Nachweis von Script-Zeilen und Client/Server-Aktionen erleichtert.</p>



(5)

### **SpiderMagic → HostView**

#### Host-bezogene Darstellung:

Das neue **HostView**-Menü stellt die erkannten Ereignisse nicht nach Protokoll dar (wie das bekannte Event-Log-Fenster), sondern nach IP-Adresse dar (also auf den einzelnen IP-Host bezogen).

#### Status-Anzeige: \*\* / Farben:

Da gleichzeitig neben den üblichen **Status-Angaben** in Stern-Form (\*/\*\*/\*\*\*) auch Farben verwendet werden (Grün=OK; Grau=auffällig; Gelb=Warnung; Rot=Alarm), ist eine schnelle Übersicht zur Erkennung solcher IP-Hosts möglich, die von Fehlern am massivsten betroffen sind.

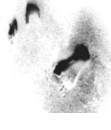
Diese Sichtweise unterstützt TraceMagic-Benutzer, die weniger Protokoll-bezogen arbeiten als vielmehr Host-bezogen: Wenn Anwender sich beschweren, sind ihr Name und ihre IP-Adresse bekannt, nicht aber unbedingt das Protokoll, das am gemeldeten Fehler gemeldet sein könnte.

(6)

### **Trace Support: VLAN Tags**

LAN-Pakete, die VLAN-Tags enthalten (nach dem Standard IEEE 802.1q) werden ab TMv4 ebenfalls verarbeitet.

Somit sind nun auch Traces aus Backbone-Trunks immer auswertbar.



(7)

### HostMagic Statistik / Ergebnis-Tabelle

Entsprechend der Änderungen bzw Erweiterungen im Umfeld der Namensdienste (siehe unten) wurde die DNS-Ergebnis-Tabelle von HostMagic massiv erweitert.

Es wurden weitere Statistik-Spalten rechts (neben den bisher bekannten Ergebnis-Spalten) eingefügt.

Das Verständnis dieser Ergebnisse setzt zwar Kenntnisse in den fortgeschrittenen DNS-Funktionen voraus, erlaubt aber wichtige Fortschritte in der Deutung der Ergebnis-Tabellen.

(8)

### Protocol Analysis: Name Services → NetBIOS, WINS, DNS

Ganz allgemein wurden die Namensdienste sehr wesentlich erweitert.

Typische (häufige wie seltene) Fehler in DNS, WINS, NetBIOS werden automatisch erkannt und im Event-Log ausgegeben.

Weiterhin können "illegale" Host/Domain-Namen in einer Black-List hinterlegt werden. Auf diese Weise kann TraceMagic nach benutzer-definierten Namen-Profilen entscheiden (und automatisch bewerten), welche Host/Domain-Namen zulässig und welche unzulässig sind. Dies erlaubt \*optimale\* Unterstützung in Migrations-Phasen.

(Siehen unten, DNS)

Besonders wichtig ist die Analyse und Fehler-Erkennung im Routing-Umfeld, wo mit sog. IP-Helper-Adressen gearbeitet wird. Die letzten Jahre haben gezeigt, dass weit häufiger als zuvor angenommen IP-Helper-Probleme ganze LANs lahm legen können.

(Siehe unten, IP-HELPER)



(9)

## Protocol Analysis: DNS

Spätestens seit der Einführung von Windows-2003-Server ist die Verwendung von dynamischem DNS (insbesondere in Active-Directory-Umgebungen) in die lokalen Netze eingezogen.

Während TMv3 die DNS-Dialoge (zwischen DNS-Client und DNS-Server) jeweils nur mit 1 Zeile im Event-Log darstellte,

gibt TMv4 den Inhalt der DNS-Pakete in Mehr-Zeilen-Technik aus (Multi-Line Events).

Weiterhin wurde in sehr erheblichem Umfang eigene Analyse-Intelligenz geschaffen, um in komplexen DNS-Umgebungen auch schwierige und versteckte Fehler nachweisen zu können.

Weiterhin können über benutzer-definierte Tabellen falsche oder unerwünschte DNS-Aktionen erkannt und im Event-Log angezeigt werden:

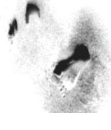
- die Verwendung unerlaubter bzw. veralteter DNS-Namen
- die Verwendung von DNS-Namen, die Syntax-Fehler aufweisen

Dies wird gesteuert durch die Pflege der folgenden Tabellen:

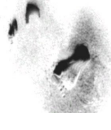
C:\Programme\Synapse\_Networks\TraceMagic\data\lang\ger\..\

```
..\TM.PROT.DNS.Illegal_Names.TXT  
..\TM.PROT.DNS.Illegal_Suffixes.TXT  
..\TM.PROT.DNS.Legal_Suffixes.TXT
```

Auch werden ab TMv4 die Fehler-Kennungen aufgelöst und angezeigt, welche die DNS-Servern den DNS-Clients zurück melden (etwa: angefragten DNS-Namen gibt es nicht; Forwarder-Timeout; etc.).



	<p>Der Bezug zu Timeouts wird erheblich heraus gearbeitet:</p> <ul style="list-style-type: none"><li>- Timeout am Server (weil der DNS-Forwarder zu lange wartete)</li><li>- Timeout am Client (weil die Server-Antwort zu spät eintraf)</li></ul> <p>Auch das Erkennen von Firewall-Blockungen erleichtert die Analyse erheblich.</p>
(10)	<p><b>IP HELPER: Fehler-Erkennung im Router-Verhalten (BOOTP-DHCP, WINS)</b></p> <p>Zusätzlich gibt es eine umfangreiche und tief greifende Analyse der IP-HELPER auf Routern bzw Layer-3-Switches.</p> <p>Diese Erkennung von IP-HELPER-Fehlern ist weltweit einmalig und schlägt vermutlich alles, was bislang LAN-Analyse hat liefern können.</p>
(11)	<p><b>User Administration / User Login</b></p> <p>Bis TMv3 warn das Anmelde-Passwort lesbar; ab TMv4 ist es durch *** verborgen.</p> <p>Das vorgegebene Admin-Passwort ist gleich geblieben (und kann immer noch nachträglich geändert werden).</p>
(12)	<p><b>TCP Port Attack / Virus Attack</b></p> <p>TCP SYN Attacken (Denial-of-Service Attacks) werden weitgehend automatisch erkannt. So konnten schon bei mehreren Kunden BLASTER- und LOVSAN-Angriffe aus den Trace-Daten heraus automatisch nachgewiesen werden.</p>



(13)

## **Security Problem**

Ein neues Sub-Log innerhalb des Event-Logs führt Sicherheits-Probleme auf, die sich in den MessDaten nachweisen lassen.

Diese Funktion wird in der Zukunft erheblich weiter entwickelt werden, um den erhöhten Sicherheits-Anforderungen zu entsprechen.

In TMv4 implementiert sind folgend Erkennungen:

### TCP Port Attack

TCP-SYN-Angriffe werden weitgehend erkannt und als Sicherheits-Problem im Event-Log markiert (s.o.).

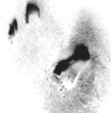
### SNMP:

SNMP Get/Set mit Standard Community-Strings, etwa "public", "private", "internal", "cisco" etc.

Das Profil der nicht erlaubten SNMP-Community-Strings kann vom Anwender selber editiert und angepasst werden. Somit kann im Zuge von Migrationen leicht erkannt werden, ob noch irgendwo "alte" Namen verwendet werden.

### UNIX-RPC

Wenn ein Unix-to-Unix-Zugriff stattfindet über RPC, wird automatisch erkannt, wenn/ob ein sog. ROOT-User (mit vollen Admin-Rechten) über die Leitung auf einen anderen Host zugreift. Dies wird sofort im Event-Log gemeldet.



(14)

### TreeView

In Baum-Struktur werden jetzt die wichtigsten Statistiken und erkannten Router/Server/Services/Ports während der Verarbeitung und offline danach dargestellt bzw. zur Verfügung gestellt.

Das erleichtert die Navigation erheblich.

(15)

### Trace:Statistics / Tabelle 5: SMB Denied Resources

Die "ACCESS\_DENIED"-Ergebnis-Tabelle kann jetzt weitreichend mit automatischen und anpassbaren Datenbank-Abfragen ausgewertet werden.

Es können seitens des Anwenders Filter-Kriterien hinterlegt werden, die von TraceMagic als Makro-Vorlage genommen werden zum automatischen Durchfiltern der Tabelle-5.

Im Ergebnis kommen lesbare Berichts-Statistiken, die 1:1 in Ergebnis-Berichte übernommen werden können.

Der Nachweis bekannter WinXP / Win2K-Fehler wird so ganz leicht:

Etwas die massive Suche von System-DLL/ EXE-Dateien auf den Servern (durch die Clients!) kann per Mausclick und Filter-Makro nachgewiesen werden.