Virenbefall! Was nun?

Ihr PC ist gut geschützt – glauben Sie! Denn nicht jedes aktuelle Schutzprogramm hilft gegen Spyware, Würmer, Trojaner und die schlimmen Rootkits. CHIP hat **20 VIRENSCANNER** getestet und sagt, welche Tools wirklich helfen – und ob das sogar gratis geht

VON CLAUDIO MÜLLER

Sie sitzen am PC, surfen im Web oder schreiben E-Mails. Dann geschehen plötzlich merkwürdige Dinge: Ihr Textprogramm stürzt ab, der Browser öffnet selbstständig eine völlig fremde Website und der Rechner startet einfach neu. Ganz scheint es, als hätte eine fremde Macht Ihren PC übernommen. Und genau so ist es: Die Internetmafia hat Malware auf Ihren PC geschleust und steuert ihn jetzt fern. Allerdings merken Sie das nur, wenn der Angreifer zu wenig Wert auf Tarnung gelegt hat. Wirklich gefährliche Trojaner und Rootkits verstecken sich meist so gut, dass Ihr PC brav weiterarbeitet – und alle Ihre Geheimnisse an die Mafia verrät.

„Kein Problem", sagen Sie jetzt vielleicht. „Ich habe einen Virenschutz." Aber ist der auch aktuell? Und kann Ihr Schutz zuverlässig Schadsoftware auf dem PC erkennen? CHIP sagt es Ihnen. Wir haben die 20 wichtigsten Virenscanner daraufhin getestet, ob sie sowohl inaktive als auch installierte Viren und Rootkits erkennen und entfernen.

Wie wichtig das ist, zeigen ein paar Zahlen: Jeden Monat registrieren Antiviren-Hersteller über eine Million neuer Schädlinge. Gleichzeitig haben 40 Prozent aller Deutschen PCs keinen aktuellen Malwareschutz, so die Security-Experten von Webroot.

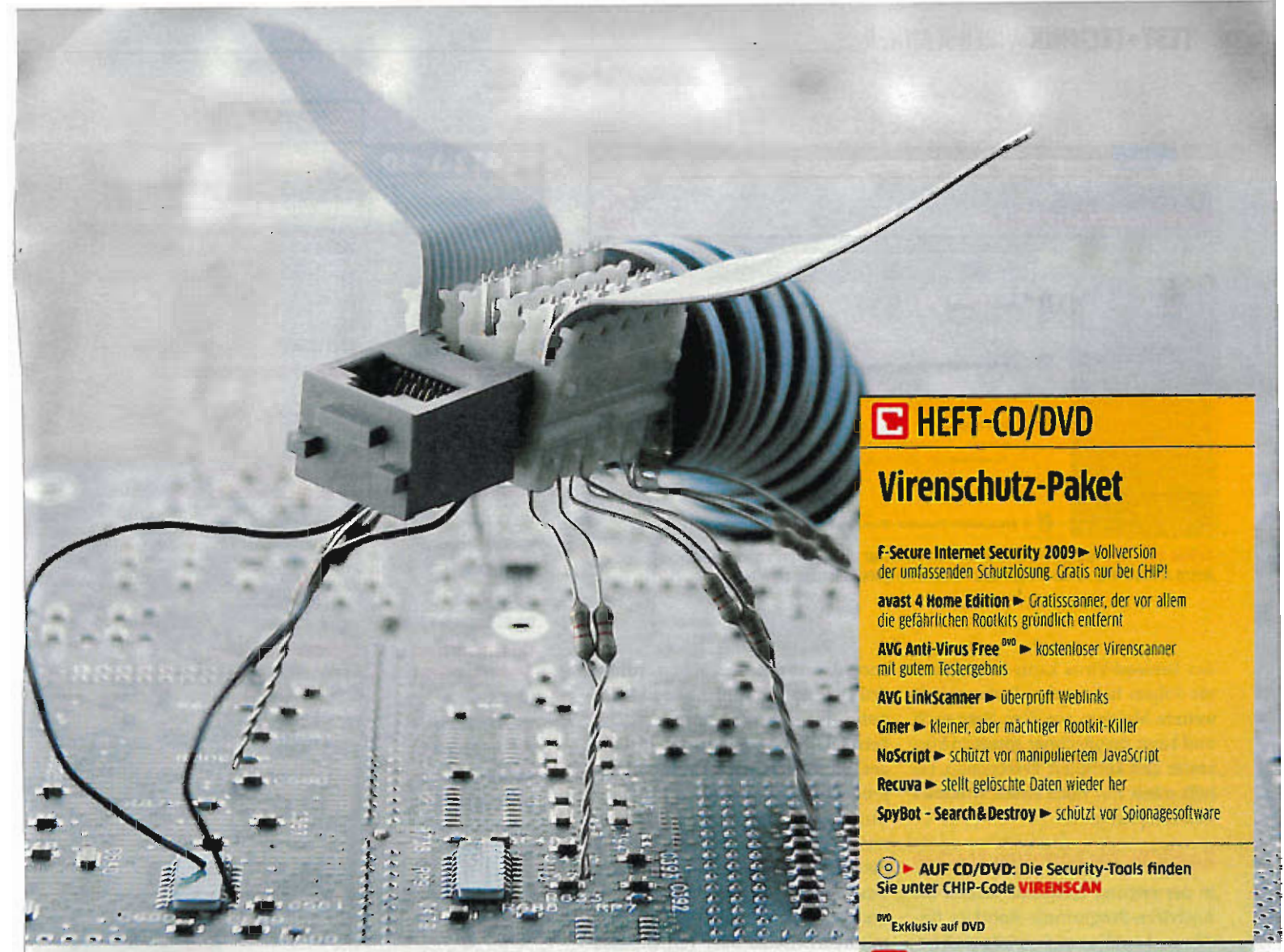
Wir testen aber nicht nur, wir helfen Ihnen auch konkret – mit unserem Virenschutz-Paket auf Heft-CD/DVD (siehe Kasten rechts oben). Sie finden dort einige der getesteten Programme und weitere Security-Tools. Wenn Sie schnell herausfinden wollen, ob Ihr Rechner infiziert ist, können Sie auch einen kostenlosen Onlinescanner nutzen. Fast alle Antiviren-Hersteller bieten solche Webtools an – im Kasten rechts unten finden Sie eine Auswahl. Sind Sie ein Mafiaopfer, muss sofort ein Antiviren-Programm her, das den Schädling entfernt; das können die Webversionen meist nicht. Unser Test sagt, welche Programme dafür die besten sind – und ob kostenlose Helfer ausreichen.

Wächter: Kein Zutritt für Malware

Für den Test haben die Experten von AV-Test zehn Viren installiert, die verschiedene aktuelle Techniken repräsentieren: Spyware klaut Passwörter, Trojaner laden Malware aus dem Netz nach, Würmer verbreiten sich per E-Mail und Rootkits verstecken sich tief im System. Ein guter Virenscanner sollte natürlich alle finden und möglichst gründlich entfernen. Diese Erkennungs- und Entfernungsraten sind die einzigen Kriterien, die in unsere Gesamtwertung einfließen – unabhängig von Ressourcen-Verbrauch und Bedienkomfort zählt nur, was wirklich hilft.

Tadelloser Virenkiller Testsieger Norton AntiVirus schützt den Rechner optimal vor Malware und entfernt aktive Viren

FOTO: ISTOCKPHOTO/LUCA DI FILIPPO



HEFT-CD/DVD

Virenschutz-Paket

F-Secure Internet Security 2009 ► Vollversion der umfassenden Schutzlösung. Gratis nur bei CHIP!

avast 4 Home Edition ► Gratisscanner, der vor allem die gefährlichen Rootkits gründlich entfernt

AVG Anti-Virus Free DVD ► kostenloser Virenscanner mit gutem Testergebnis

AVG LinkScanner ► überprüft Weblinks

Gmer ► kleiner, aber mächtiger Rootkit-Killer

NoScript ► schützt vor manipuliertem JavaScript

Recuva ► stellt gelöschte Daten wieder her

SpyBot - Search&Destroy ► schützt vor Spionagesoftware

► **AUF CD/DVD: Die Security-Tools finden Sie unter CHIP-Code VIRENSCAN**

DVD Exklusiv auf DVD

Idealerweise sollte ein Antiviren-Programm die Malware schon abfangen, bevor sie sich installiert. Die Testkandidaten mussten sich deshalb zunächst einer Datenbank mit 3.194 weitverbreiteten Viren stellen. Damit wird getestet, ob die Programme Signaturen für die Virensamples haben oder die Malware über eine heuristische Analyse erkennen. Die nicht aktive Malware sollten die Kandidaten einmal mit ihrem Scanner und dann mit ihrem Hintergrund-Wächter finden. Diese Pflichtaufgaben bewältigten die meisten Programme sehr gut – 12 Scanner übersahen keinen Virus. Auf der anderen Seite erkannte die schlechte Wächterfunktion des Ashampoo-Scanners deutlich weniger Viren als die Scanfunktion. Als untauglich erwies sich der OpenSource-Scanner ClamWin: Er übersah über 500 Viren – eine Wächterfunktion bietet er gar nicht erst!

Tiefenscan: Aktive Angreifer finden

Nach der Trockenübung kam der Härtetest: Einen verseuchten Rechner von Viren befreien. Entscheidend ist hier, dass die Virenkiller alle aktiven Komponenten der Malware entfernen, also Prozesse und ausführbare Dateien. Bleibt zum Beispiel der Installer einer Malware auf dem Rechner, kann der Virus jederzeit wieder aktiv werden. Die Kür ist es, Reste wie Registry-Einträge zu löschen. Die sind zwar in der Regel harmlos, aber unnötiger Sand im Systemgetriebe. Kein Kandidat schaffte ein perfektes Ergebnis. Aber immerhin haben 15 Scanner alle Viren erkannt und unschädlich gemacht.

Norton AntiVirus, eScan von MicroWorld und Spyware Doctor löschten sogar vier der fünf Viren restlos. Beim Spyware Doctor war das etwas überraschend, da dessen Scanengine bei den nicht installierten Viren die zweitschlechteste Erkennungsrate (98,31 Prozent) hatte. Von den Freeware-Scannern eliminierte nur Avira alle fünf Viren, ließ aber Reste zurück. avast und AVG dagegen entfernten den E-Mail-Wurm Rontokbro, der Systemtools blockiert und Signatur-Updates des Virenscanners zu verhindern versucht, nicht. Negativer Spitzenreiter ist wieder der ClamWin-Scanner: Er erkannte zwar noch drei Schädlinge, konnte aber gegen keinen etwas ausrichten! Ganz besonders im Fall

INFO

Virenscanner im Web

Onlinescanner sind die schnellste Möglichkeit, den Rechner durchzuchecken, falls Sie keinen oder nur einen veralteten Virenschutz installiert haben. Die meisten benötigen den Internet Explorer, Trend Micro und F-Secure unterstützen auch Firefox. Falls Sie ein einzelnes File überprüfen wollen, laden Sie es bei VirusTotal hoch – der Dienst checkt die Datei mit 41 verschiedenen Scanengines.

http://housecall.trendmicro.com

http://security.symantec.com

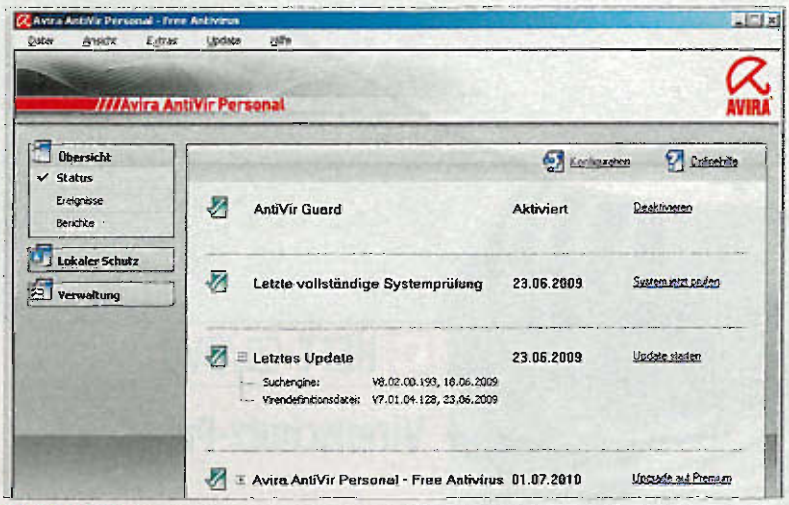
www.bitdefender.com/scanner/online/free

www.f-secure.com/en_EMEA/security

www.kaspersky.com/virusscanner

www.pandasecurity.com/activescan

www.virustotal.com



Gratis-Schutz Freeware-Scanner entfernen zwar nicht jeden Virus, Tools wie Avira AntiVir Personal bieten aber trotzdem gute Leistung zum Nulltarif

des Banload-Virus kann das schlimme Folgen haben: Der Trojaner lädt weitere Malware aus dem Netz nach und kann den Rechner somit in kürzester Zeit komplett verseuchen. Da hilft meist nur noch eines: Windows neu installieren.

Rootkits: Die härtesten Brocken

In der zweiten Testrunde sollten die Antiviren-Programme Rootkits finden und entfernen. Rootkits sind besonders gefährlich, weil sie sich in Windows-Prozesse einklinken, zum Teil sogar in den Kernel selbst. So können sie sich besser tarnen, etwa indem sie ihre Prozesse oder die Kommunikation mit dem Hacker-PC verschleiern. Zudem sind sie sehr schwer zu entfernen. Besonders ein Rootkit machte dem Testfeld zu schaffen: Das NTRootkit ist ein speicherresidenter Trojaner, der – einmal gestartet – im Arbeitsspeicher bleibt und auf Befehle wartet, die über eine Backdoor übermittelt werden. Rund die Hälfte der getesteten Programme scheiterte beim Versuch, ihn zu entfernen.

Schlusslicht im Rootkit-Test ist Ashampoos AntiVirus. Das Tool erkannte zwar die inaktiven Installer, aber sobald die Rootkits installiert waren, fand es keines mehr. Besser machten es die acht Kandidaten, die jedes Rootkit – aktiv und inaktiv – erkannten und beseitigten. Darunter ist als einziger Freeware-Vertreter der avast-Scanner. Ein interessantes Phänomen, das sich im Test zeigte: Einige Scanner übersahen ein inaktives Rootkit, erkannten es aber, sobald es aktiv wurde – obwohl die Rootkit-Tarnung nur bei Aktivität wirkt. Zum Beispiel übersah Panda den Installer des Infostealers; das ist ein Spionageprogramm, das Passwörter klaut. Der Grund: Zum Teil haben die Scanner nur für die aktiven Komponenten Signaturen, nicht aber für die inaktiven. Oder es lag gar keine Signatur vor und der Scanner fand die Rootkits mit heuristischer oder verhaltensbasierter Erkennung.

FAZIT: Erfreulich ist, dass mehr als die Hälfte des Testfelds ein sehr gutes Ergebnis erzielte. Das sind aber durchweg kommerzielle Programme – die beste Freeware ist eine Note schlechter. Voll überzeugt haben die Produkte auf den ersten sechs Plätzen, allen voran Norton und Trend Micro; sie ließen nur wenige unschädliche Installationsreste zurück. Darunter befindet sich auch F-Secure Anti-Virus, dessen Vorgängerversion Sie als Bestandteil der Internet Security Suite auf Heft-CD/DVD finden.

Wer kein Geld ausgeben möchte, ist mit den Freeware-Programmen Avira AntiVir und avast noch recht gut bedient. Sie sind besser als einige kostenpflichtige Programme, die sich als echte Flops erwiesen: Schlechter als die Scanner von Dr. Web und Ashampoo war nur der weit abgeschlagene Open-Source-Virenschutz von ClamWin. Schützen Sie Ihren PC damit, hat die Internetmafia leichtes Spiel – und Ihr PC bleibt weiter infiziert.

CLAUDIO.MUELLER@CHIP.DE

TESTSIEGER 10/2009

PLATZ 1–10	1. PLATZ	2. PLATZ
Produkt	Norton AntiVirus 2009	Trend Micro Internet Security 2009
Build	16.5.0.134	17.1.1250
Anbieter	www.symantec.com	http://de.trendmicro.com
Preis (ca.)	30 Euro	50 Euro
Gesamtwertung	98,6	97,2
Erkennung nicht installierter Malware (gesamt: 3.194 aktuelle Schadprogramme)		
Scanner	100,00 %	100,00 %
Wächter	100,00 %	100,00 %
Desinfektion installierter Malware (Erkennung/Entfernung aktiver Komponenten/komplette Reinigung)		
Win32/Autoit	●/●/●	●/●/●
Win32/Autorun	●/●/●	●/●/–
Win32/Banload	●/●/●	●/●/●
Win32/Mytob	●/●/–	●/●/–
Win32/Rontokbro	●/●/●	●/●/●
Desinfektion installierter Rootkits (Erkennung inaktiver Rootkits/Erkennung aktiver R./Entfernung aktiver R.)		
Win32/Hupigon	●/●/●	●/●/●
Win32/Infostealer	●/●/●	●/●/●
Win32/NTRootkit	●/●/●	●/●/●
Win32/Pigeon	●/●/●	●/●/●
Win32/PolyCrypt	●/●/●	●/●/●

PREISTIPP 10/2009

PLATZ 11–20	11. PLATZ	12. PLATZ
Produkt	Panda Antivirus Pro 2009	Avira AntiVir Personal – Free Antivirus
Build	8.00.00	9.0.0.403
Anbieter	www.pandasecurity.com	www.free-av.de
Preis (ca.)	40 Euro	Freeware
Gesamtwertung	91,8	89,4
Erkennung nicht installierter Malware (gesamt: 3.194 aktuelle Schadprogramme)		
Scanner	100,00 %	100,00 %
Wächter	100,00 %	100,00 %
Desinfektion installierter Malware (Erkennung/Entfernung aktiver Komponenten/komplette Reinigung)		
Win32/Autoit	●/●/–	●/●/–
Win32/Autorun	●/●/–	●/●/–
Win32/Banload	●/●/–	●/●/–
Win32/Mytob	●/●/–	●/●/●
Win32/Rontokbro	●/●/–	●/●/–
Desinfektion installierter Rootkits (Erkennung inaktiver Rootkits/Erkennung aktiver R./Entfernung aktiver R.)		
Win32/Hupigon	●/●/●	●/●/●
Win32/Infostealer	–/●/●	●/●/●
Win32/NTRootkit	●/●/●	●/–/–
Win32/Pigeon	●/●/●	●/●/●
Win32/PolyCrypt	●/●/●	●/●/●

● Spitzenklasse (100–90,0) ● Oberklasse (89,9–75,0) ● Mittelklasse (74,9–45,0) ○ Nicht empfehlenswert (44,9–0) ● ja – nein
Alle Wertungen in Punkten (max. 100)

3. PLATZ	4. PLATZ	5. PLATZ	6. PLATZ	7. PLATZ	8. PLATZ	9. PLATZ	10. PLATZ
BitDefender Antivirus 2009	BullGuard Internet Security	NOD32 Antivirus 4	F-Secure Anti-Virus 2010	eScan Anti-Virus Edition	Kaspersky Anti-Virus 2009	G DATA Anti-Virus 2010	VirusScan Plus 2009
12.0.12.1	8.7.1.17	10.0.977.409	5.3.161	10.0.977.409	8.0.0.506 (a.b)	20.0.4.9	13.3 Build 127
www.bitdefender.com	www.bullguard.com	www.eset.de	www.f-secure.com	www.microworld.de	www.kaspersky.com	www.gdata.de	www.mcafee.com
25 Euro	45 Brit. Pfund	30 Euro	30 Euro	25 Euro	30 Euro	25 Euro	40 Euro
95,8	95,8	94,4	94,3	93,5	93,3	93	91,9
100,00 %	100,00 %	100,00 %	100,00 %	100,00 %	100,00 %	100,00 %	100,00 %
100,00 %	100,00 %	100,00 %	99,97 %	99,97 %	100,00 %	100,00 %	100,00 %
●/●/–	●/●/–	●/●/–	●/●/●	●/●/●	●/●/–	●/●/–	●/●/–
●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	●/●/●	●/●/–	●/●/–
●/●/–	●/●/–	●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	●/●/–
●/●/●	●/●/●	●/●/–	●/●/–	●/●/●	●/●/●	●/●/–	●/●/●
●/●/●	●/●/●	●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	●/●/–
●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●
●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●
●/●/●	●/●/●	●/●/●	●/●/●	●/–/–	●/●/–	●/●/●	●/●/●
●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●
●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/–

13. PLATZ	14. PLATZ	15. PLATZ	16. PLATZ	17. PLATZ	18. PLATZ	19. PLATZ	20. PLATZ
avast! 4.8 Home Edition	AVG Anti-Virus Free 8.5	Spyware Doctor mit Antivirus	VirusBuster Professional Home	VIPRE Antivirus + Antispyware	Dr.Web Anti-Virus	Ashampoo AntiVirus	ClamWin Free Antivirus
4.8.1335.0	8.5.374	6.0.1.445	5.3.161	3.1.2775	5.0.1.06018	1.61	0.95.2
www.avast.de	http://free.avg.de	www.pctools.com	www.virusbuster.de	www.sunbeltsoftware.com	www.drweb-av.de	www.ashampoo.de	http://de.clamwin.com
Freeware	Freeware	40 Euro	25 Euro	30 Dollar	20 Euro	30 Euro	Freeware
89,3	84,5	83,8	81,8	75,8	64,4	66,6	20,8
99,97 %	100,00 %	98,31 %	100,00 %	99,12 %	98,50 %	100,00 %	83,50 %
99,97 %	100,00 %	98,31 %	100,00 %	99,06 %	98,47 %	98,18 %	nicht vorhanden
●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	–/–/–	●/●/–	●/–/–
●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	–/–/–	●/●/–	–/–/–
●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	●/●/–	●/–/–	–/–/–
●/●/–	●/●/–	●/●/–	●/●/–	●/●/–	●/●/–	●/●/–	●/–/–
●/–/–	●/–/–	●/●/●	●/●/–	●/●/–	●/●/–	●/●/–	●/–/–
●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/–/–	●/●/●
●/●/●	●/●/●	●/●/●	●/–/–	●/●/–	●/●/●	●/–/–	●/●/●
●/●/●	●/–/–	●/●/●	●/–/–	●/–/–	●/●/–	●/–/–	●/–/–
●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/–/–	–/●/–
●/●/●	●/●/●	–/●/●	–/●/●	●/●/–	●/●/●	●/–/–	●/●/–