

Proaktiver Emailschutz von Pallas für Continental

Dr. Kurt Brand, Pallas GmbH
Stephan Sachweh, Pallas GmbH
Dr. Bernhard Thomas, Continental AG
Thomas Ullrich, Continental AG

Email ist weiterhin die wichtigste internetbasierte Anwendung und auch die mit Abstand größte Einfallstraße für Spam und Malware (Viren, Würmer, Trojaner). Mehr als 85 % des Spam und nahezu 100 % aller durch Malware verseuchten Emails kommen inzwischen aus Botnetzen. Klassische auf dem Scannen von Content basierende Abwehrmaßnahmen werden durch kurzen und intensiven Versand von zahlreichen Malware-Varianten oder durch Umverpackung alter Spaminhalte in Bilder, PDF-Dateien usw. ausgehebelt. Die traditionelle Strategie, mehrere Abwehrprodukte hintereinander einzusetzen, hat Continental deshalb durch die Nutzung von Filterverfahren ergänzt, die proaktiv unabhängig vom Content arbeiten, nämlich Zero-Hour Protection (ZHP) gegen Viren und Real-Time Anti-Spam (RTAS). Dadurch wurden Infrastruktur und Mitarbeiter deutlich entlastet und gefährliche Angriffe, die klassische Verfahren nicht rechtzeitig erkennen, erfolgreich abgewehrt.

Einsatzszenario bei Continental

Continental setzt am Standort Hannover für etwa 12.000 Arbeitsplätze proaktive Verfahren gegen Malware und Spam ein, nämlich ZHP und RTAS, die von Pallas in die Email-Infrastruktur von Continental integriert wurden. Beide Verfahren basieren auf der Recurrent Pattern Detection Technologie (RPD™) von Commtouch Software Ltd. (Netanya, Israel) und nutzen das wichtigste Kennzeichen von Spam und Malware, nämlich die massive Verbreitung über das Internet. RPD verliert keine Zeit mit der Inhaltsbewertung jeder einzelnen Email, sondern analysiert weltweit in Echtzeit große Mengen Internet-Traffic und erkennt Malware an der Art des Massenversands auf der Basis von Message-Trafficströmen und Strukturmustern. Ausbrüche werden innerhalb von Minuten erkannt, und zwar umso besser, je massiver und gefährlicher sie sind. Jede einlaufende Email wird in Echtzeit mit den Verbreitungsmustern verglichen.

ZHP schließt die zeitliche Lücke zwischen dem Ausbruch eines neuen Virus und seiner Erkennung und Einarbeitung in die

Signatur-Datenbanken, die oft mehrere Tage dauert. Diese ansonsten schutzlose Zeit versuchen die Angreifer durch kurzen und massiven Versand zu nutzen (Short-Span-Angriffe).

Hohe Spamerkennung von 99,6 %, großer Produktivitätsvorteil

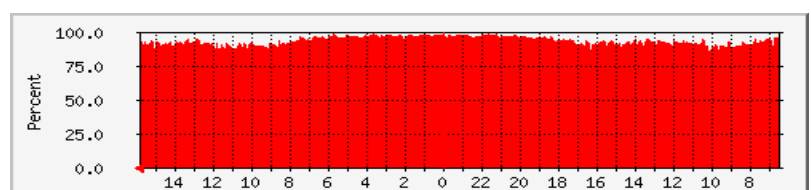
Continental hat am Standort Hannover im Januar 2008 ca. 40 Millionen Emails erhalten, wovon RTAS 96,2 % als Spam klassifiziert hat. Das bei Continental eingesetzte klassische Verfahren gegen Spam hat demgegenüber nur 79 % der Emails als Spam erkannt. Es konnten also 6,9 Millionen Emails zusätzlich ausgesondert werden. Dies entspricht einem Produktivitätsvorteil von mehr als 7.600 €, wenn man einmal sehr konservativ annimmt, dass die Beseitigung einer durch-

gelassenen Spam-Email nur eine Zehntelsekunde braucht (40 € Produktivitätskosten pro Mitarbeiter und Stunde). Der ebenfalls von Pallas integrierte Content-Spamfilter Spamassassin hatte im gleichen Zeitraum eine Erkennungsrate von 91,4 % und hebt die insgesamt als Spam erkannten Emails noch geringfügig auf 96,9 % an. Beide Filterverfahren zusammen haben in einem Testverfahren bei Pallas über 10 Wochen im Mittel 99,6 % des tatsächlich eingegangenen Spam erkannt. Dabei gab es keine falsch positiven Ergebnisse. Commtouch gibt die Falsch-Positiv-Quote von RTAS mit 1 auf 1,5 Millionen Mails an, also weniger als 0,00007 %.

90,6 % der bei Conti Hannover im Januar 2008 eingelieferten Emails wurden nicht an die Mitarbeiter ausgeliefert, weil sie mit hoher Sicherheit als Spam klassifiziert wurden. Damit wurden die Infrastruktur und mehr noch die Mitarbeiter von 36,1 Millionen Müll-Mails entlastet, das entspricht nach obiger Rechnung etwa 40.000 € Produktivitätsgewinn in einem Monat.

8 Malware-Ausbrüche in 4 Wochen von ZHP abgewehrt

Sicherheitsexperten haben 2006 das Jahr der Zombies genannt, in diesem Jahr



Anteil Spam: Nachts nahe 100 %

Datum	Dauer (Min.)	Anz. Malw.	Mass. *)	ΔT **)	Betreff	Anhang	Malware
09.01.08	294	348	1,2	0	Card from Adult Friend Finder o.ä.	card.zip/exe	TROJ_PUSHDO.BG
13.01.08	439	202	0,5	7	Merry Christmas	eCard.zip/exe	TROJ_PAKES.CO
17.01.08	156	649	4,2	5	Card from Adult Friend Finder o.ä.	eCard.zip/scr	TROJ_AGENT.BJI
20.01.08	81	27	0,3	2	Merry Christmas	card.zip/scr	WORM_PANDEX.AZ
22.01.08	387	425	1,1	k. A.	Card from Adult Friend Finder o.ä.	eCard.zip/scr	WORM_PANDEX.AZ
25.01.08	477	394	0,8	1	Hot Pictures o.ä.	video.zip/scr	TROJ_DROPPER.VN
31.01.08	620	379	0,6	k. A.	Naked Britney	video.zip/exe	TROJ_DLOADER.FV
03.02.08	1.019	221	0,2	7	Hot Pictures o.ä.	xvideo.zip/scr	TROJ_DLOADER.EUZ

*) Massivität: durchschnittliche Anzahl pro Minute

**) ΔT : Zeit (in Minuten) zwischen erster Erkennung (Commtouch) und Auftreten bei Continental

haben sich die aus Zombies bestehenden Botnetze als wichtigste Plattform für die Internet-Kriminalität etabliert. Vint Cerf, der "Internet-Vater" und Mitentwickler von TCP/IP, schätzte Anfang 2007, dass von den 600 Millionen Internet-PCs schon etwa ein Viertel als Zombie missbraucht wurde. 2007 sind die Botnetze erwachsen geworden, die bedrohlichsten werden nicht mehr zentral von einem Server gesteuert, sondern sind als Peer-to-Peer-Netzwerk organisiert und können deshalb kaum noch durch Gegenmaßnahmen ausgeschaltet werden. Viele neue Angriffe haben das Ziel, die Botnetze auszubauen, um die Basis für kriminelle Internet-Geschäfte durch Spam, Spionage und Sabotage weiter zu vergrößern.

Zwischen dem 08.01.08 und dem 04.02.08 wurden 8 neue Malware-Ausbrüche von

ten. Denn in den ersten Stunden nach einem neuen Ausbruch liegen naturgemäß die Virenpattern noch nicht vor. Nur der bei Continental benutzte Extension-Filter hätte ohne ZHP eine letzte Barriere gebildet. Er wirkt aber nicht mehr, wenn Angriffe über übliche Dateiformate (.doc u.a.) erfolgen.

Die verseuchten Emails richteten sich überwiegend an sprechende Adressen. Sie hatten also ein hohes Infektionspotential. Die Benennung in obiger Tabelle folgt dem Standard von Trend Micro, die Malware wird inzwischen von diesem Virenschanner erkannt.

Insgesamt wurden in diesen 4 Wochen 2.645 neue Malware-Muster abgefangen. Der Angriff vom 31.01.08 enthielt eine verschlüsselte Datei, um das Auffinden zu

erschweren. Im Mittel war Continental weniger als 4 Minuten nach dem weltweit ersten Auftreten vom jeweiligen Ausbruch betroffen. Besonders massiv erfolgte der Short-Span-Angriff vom 17.01.08. Dieser wurde erst erhebliche Zeit später von den üblichen Virenschannern er-

AntiVir	Worm/Ntech.AG	1:39 hrs.
Avast!	-	No detection
AVG	SHeur.ANDW (Trojan horse)	6:47 hrs.
BitDefender	Trojan.Kobcka.CE	Zero-hour
ClamAV	Trojan.Downloader.Agent-1279	5:04 hrs.
Command	W32/Trojan2.TZD (destructive program)	2:34 hrs.
Dr Web	BackDoor.Bulknet.122	2:19 hrs.
eTrust-VET	Win32/Cutwail.CT	16:56 hrs.
Ewido	-	No detection
Fortinet	suspicious	Zero-hour
F-Prot	W32/Trojan2.TZD	15:01 hrs.
F-Secure	Trojan-Downloader.Win32.Agent.hmc	3:07 hrs.
Ikarus	Win32.Outbreak	0:33 hrs.
Kaspersky	Trojan-Downloader.Win32.Agent.hmc	Zero-hour
McAfee	-	No detection
Microsoft	TrojanDropper:Win32/Cutwail.X	17:20 hrs.
Nod32	Win32/TrojanDownloader.Agent.NUQ	Zero-hour
Norman	W32/Agent.DYTY	6:41 hrs.
Panda	-	No detection
QuickHeal	-	No detection
Rising	-	No detection
Sophos	Troj/Dorf-AT	1:24 hrs.
Symantec	-	No detection
Trend Micro	TROJ_AGENT.BJI	21:53 hrs.
VBA32	-	No detection
VirusBuster	Trojan.DR.Pandex.Gen.4	9:22 hrs.
WebWasher	Worm.Ntech.AG	1:39 hrs.

Verzögerung klassischer Virenschanner gegenüber ZHP für TROJ_AGENT.BJI
(Quelle: Commtouch)

ZHP erkannt und abgewehrt, die die bei Continental eingesetzten klassischen Virenschanner noch nicht erkennen konn-

kannt, wie die Tabelle links zeigt. Die Daten wurden 28:31 Stunden nach dem Ausbruch ermittelt.

Die Continental AG ist einer der weltweit führenden Zulieferer der Automobilindustrie mit umfassendem Know-how in der Reifen- und Bremsentechnologie, der Fahrdynamikregelung, der Elektronik und der Sensorik.

Dr. Bernhard Thomas
CTO Corporate IT Continental AG

Thomas Ullrich
CSO Corporate IT Continental AG

Weitere Informationen

Thomas Ullrich
Continental AG
Vahrenwalder Straße 9
30165 Hannover
Tel: 0511-938-01
Fax: 0511-938-81770
thomas.ullrich (at) conti.de
www.conti-online.com

Pallas Managed Security Service: Vom Mailschutz bis hin zur umfassenden mehrstufigen Sicherheitslösung, TÜV-zertifiziert und mehrfach ausgezeichnet. Sicherheitsberatung und Betrieb abgesicherter Internet-Server.

Dr. Kurt Brand
Geschäftsführer Pallas GmbH
Stephan Sachweh
Technischer Leiter Pallas GmbH

Weitere Informationen

Dr. Kurt Brand
Pallas GmbH
Hermülheimer Straße 8a
50321 Brühl
Tel: 02232-1896-0
Fax: 02232-1896-29
kurt.brand (at) pallas.de
www.pallas.de