



Rückblick und Analyse der Virenbedrohungen im Monat November

Hanau, 10. Dezember 2009: Der russische Sicherheitsspezialist Doctor Web präsentiert seinen Sicherheitsreport für den vergangenen Monat und meldet darin neues Schadpotenzial durch eine Rootkit-Variante von BackDoor.Tdss. Darüber hinaus war Malware aktiv, die über ein Tool zur Ortung des Standorts von Handy-Benutzern die Daten von Computernutzern ausspionierte. Der Versand von Kurzmitteilungen in sozialen Netzwerken bleibt nach wie vor eine der Hauptmethoden zur Verbreitung von Trojanern. Dagegen ließ die Virenverbreitung per E-Mail Ende November nach.

BackDoor.Tdss.565 und seine Varianten

Am 12. November 2009 veröffentlichte Doctor Web eine neue Version des GUI-Scanners. Mit dem aktualisierten Scanner konnte man das von **BackDoor.Tdss.565** (u.a. als TDL3 bekannt) befallene System erfolgreich desinfizieren.

Diese Rootkit-Spezies verfügt über eine Vielzahl von raffinierten Tricks, die fast alle am Markt vorhandenen Antivirentechnologien umgehen, so dass Malware mühelos und für die meisten Antivirenprogramme unsichtbar ins System eindringt. **BackDoor.Tdss.565** verfügt über eine neue Methode der Installation im System und täuscht dadurch alle zur Zeit vorhandenen Tools zur Verhaltensanalyse. Dies belegt, dass Virenschreiber nicht nur die signaturbasierte Suche und Heuristik sondern auch Tools zur Verhaltensanalyse ins Visier genommen haben.

In einem verschlüsselten virtuellen Datenträger, der sich auf der Festplatte des Anwenders einnistet werden Dateien abgelegt, die für das Weiterleben des Trojaners erforderlich sind. Um diesen Datenträger unsichtbar ins System einzuschleusen, wird er durch spezielle Techniken maskiert. Um funktionsfähig zu bleiben, infiziert das Rootkit einen Treiber, der für eine intakte Funktion lokaler Datenträger verantwortlich ist. Dabei wird automatisch festgestellt, welche Art der Oberfläche von Datenträgern auf einem infizierten PC verwendet wird. Anschließend wird der entsprechende Treiber infiziert.

Die Sicherheitsspezialisten von Doctor Web entwickelten das Gegenmittel gegen **BackDoor.Tdss.565** am schnellsten. Der Scanner von allen Dr.Web Antivirenprodukten für Windows ist aktualisiert.

Gefälschte Navigationssoftware

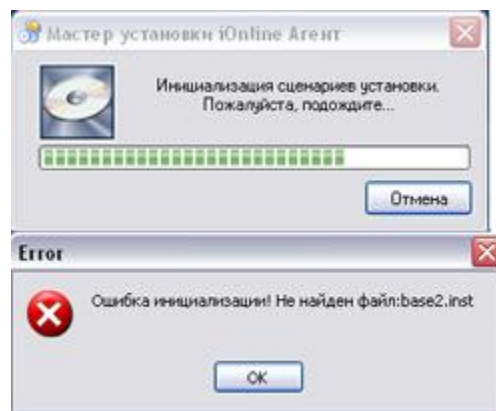
Gefälschte Antivirensoftware wird zur Zeit weiter aktiv verbreitet. Darüber hinaus war Handy-Software das bevorzugte Ziel von Cyberkriminellen. Im November wurden E-



Mails mit Informationen über eine kostenlose Software versendet, die vermeintlich den aktuellen Standort eines Handy-Benutzers bestimmen kann. Potenzielle Interessenten handelten sich über die angehängte Datei einen Trojaner ein (**Trojan.PWS.AccHunt.11**), der Passwörter des Nutzers ausspionieren kann.



Trojan.PWS.Multi.109 wurde ähnlich verbreitet, hieß aber diesmal etwas anders. Im Anhang gab es zwei Dateien: einen Installationsassistenten und ein extra vorbereitetes Installationspaket. Die Installation des Programms erfolgte zunächst erfolgreich, danach wurde ein weiteres fehlendes Installationspaket angefordert. Auf diese zweistufige Art gelangten die übermittelten Passwörter in die Hände der Malware-Entwickler.

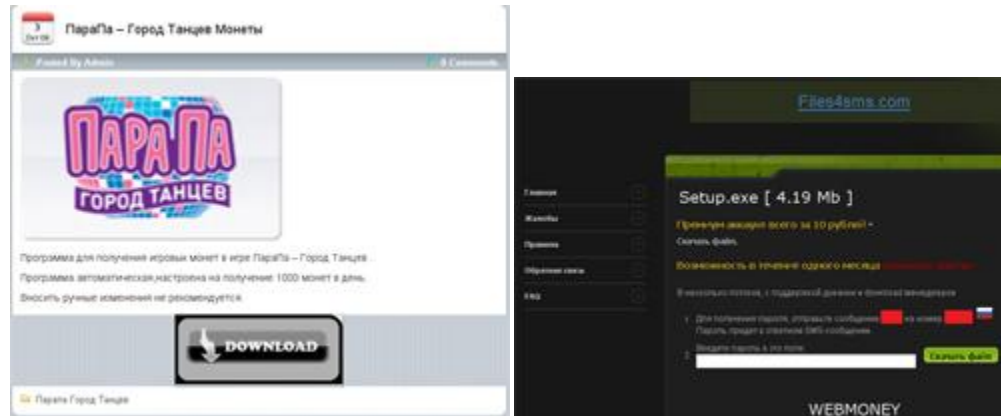


Tricks in Online-Spielen

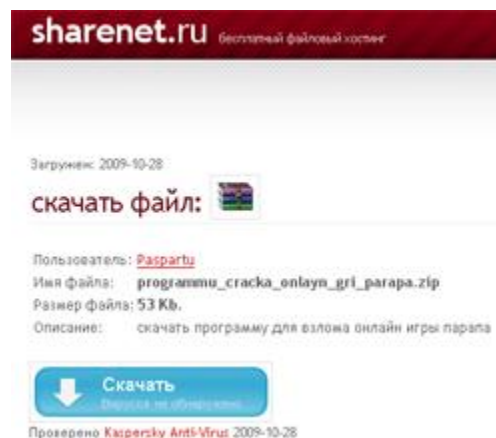
Nachdem Online-Spiele für die Rechteinhaber ein lukratives Geschäft sind, wollen Cyberkriminelle auch hier mitverdienen. Es ist kein Geheimnis, dass Internetnutzer in Online-Spielen gehörige Geldsummen für verschiedene Privilegien ausgeben. Die Verbreitung von Malware geht mit der Abzocke einher. Ein Beispiel ist das in Russland beliebte Online-Spiel "Para Pa: Gorod Tantsev" (zu Deutsch: Tanzstadt). Die Zahl der Spieler, die virtuelle Vorrechte haben wollen wächst stetig und diese Spieler sind bereit, in virtuelle Guthaben zu investieren. Die Übeltäter bieten Spielern verschiedene Programme an, durch die sie Guthaben täglich aufladen, Vorrechte des Administrators und viele andere Möglichkeiten erhalten können. Schnell werden Spieler, die auf diesen



Deal eingehen, zu Opfern. Sie werden erpresst, ihr Spieler-Profil zu verlieren. Die Übeltäter wollen nicht nur an das Geld des Spielers, sondern auch an private Daten herankommen. Um ein Benutzerkonto zurückzubekommen, muss das Opfer zahlen. Dafür gibt es Plattformen wie files4money.com, files4sms.com, mix-file.com.



Hier werden auch verschiedene Schadprogramme als kostenfreie Software ausgegeben. Auf solche Weise wurde z.B. **BackDoor.Dax.47** verbreitet.



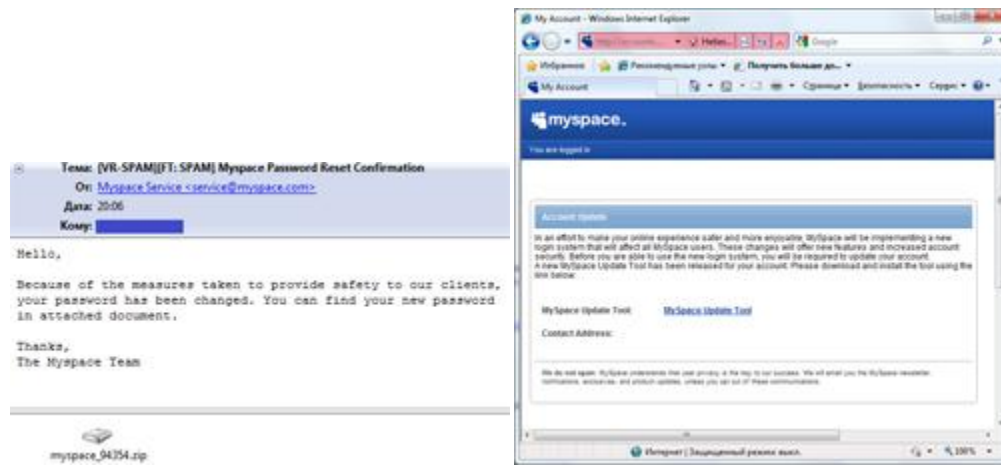
E-Mail-Viren

Für den vergangenen Monat war darüber hinaus der Versand neuer Varianten von **Trojan.PWS.Panda** sowie **Trojan.Proxy** charakteristisch. Da Computernutzer von Antimalware-Herstellern kontinuierlich auf dem Laufenden gehalten werden, sehen sich die Virenschreiber zum Wechsel ihrer Taktik gezwungen.

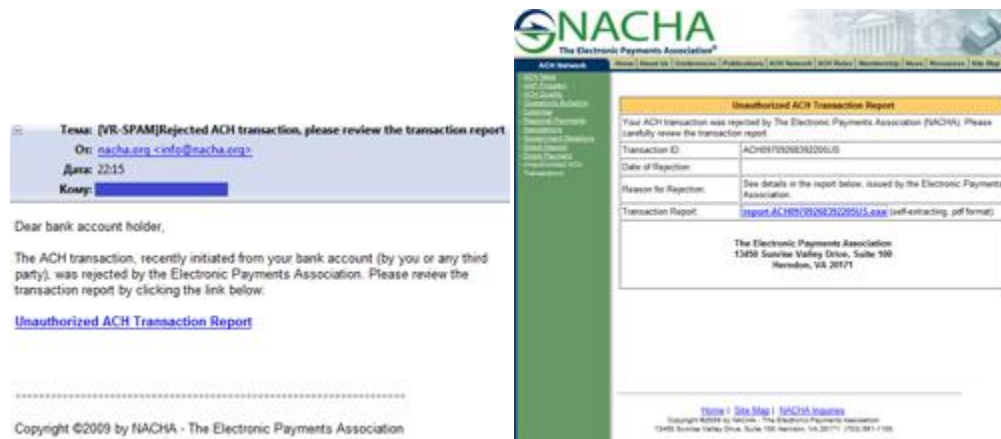
Um den Versand von böswilliger Software zu maskieren, gelangten im November MySpace-Mitglieder ins Visier der Übeltäter. In E-Mails wurde ihnen mitgeteilt, dass ihre Passwörter durch den Administrator geändert wurden. Das neue Passwort war vermeintlich in anhängenden Archiv einsehbar. In anderen Mails wurden Nutzer zum Download eines Tools aufgefordert, um sich weiterhin auf der Website des Social



Networks einloggen zu können. Dabei wurden die Anwender auf eine gefälschte Website weitergeleitet, auf der private Daten ausgelesen werden können.



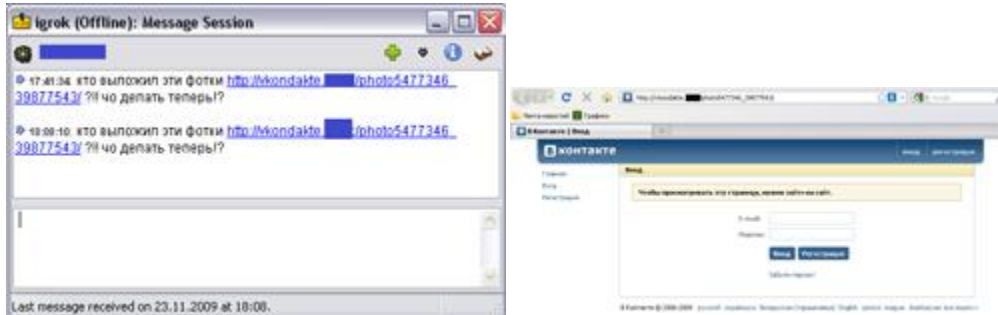
Zur Verbreitung von Malware via E-Mail werden von Cyber-Kriminellen weiterhin bekannte Namen verwendet. Im November fiel NACHA (The Electronic Payment Association) den Angreifern zum Opfer. Den Anwendern wurde mitgeteilt, dass ihr E-Payment abgelehnt wurde. Weitere Informationen sollte man auf der NACHA-Website erhalten. Auf diese Weise wurde auf den PCs der leichtgläubigen Anwender eine neue Variante des **Trojan.PWS.Panda** geladen.



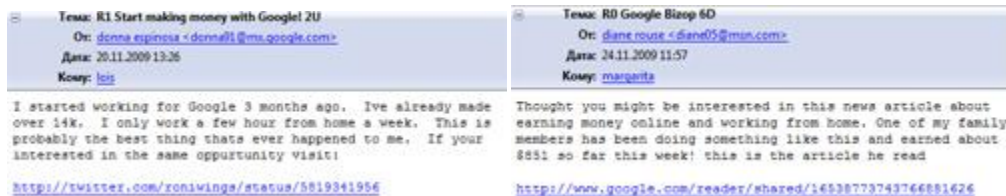
Die Verbreitung von Malware durch Spam-Mails blieb im November auf dem Vormonatsniveau. In der Spamflut konnte man vielfältige Spielarten von Schadprogrammen sowie Links zu Malware-Websites erkennen. In der zweiten Hälfte des Monats ließ der Spam-Versand nach. Ende des Monats reduzierte sich der Anteil von Spam-Mails im Vergleich zum Monatsanfang auf die Hälfte. Es wird spekuliert, dass die Cyberkriminellen diese kreative Pause zum Durchatmen verwenden und um ihre Aktivitäten neu aufzustellen.

Phishing

Durch neue Phishing-Methoden versuchen Cyberkriminelle an die Privatdaten von Anwendern zu gelangen. Um den Zugriff auf Benutzerkonten der Kontakte-Mitglieder zu erhalten, wurden Mails mit Links auf eine Malware-Website versendet. Anwender erhielten die Aufforderung auf der gefälschten Seite Daten einzugeben, die von dort durch die Angreifer abgefangen wurden. Um den Betrug zu kaschieren, wurde der Anwender nach Dateneingabe auf die echte Website weitergeleitet.



Die Komplexität der angewendeten Tricks steigt weiter. E-Mails im Namen von Google waren im Umlauf, in denen Anwender auf eine schnelle Verdienstmöglichkeit hingewiesen wurden. Dafür wurde der Anwender auf eine Website geleitet, um sich mit einem entsprechenden Programm vertraut zu machen.



In anderen Mails war eine Twitter-Kurznachricht mit dem Link zu einem extra vorbereiteten Artikel zu finden. Darüber hinaus wurden Anwender über Links direkt zu Google Services weitergeleitet.



Alle Fällen zielten darauf ab, Opfer auf eine speziell vorbereitete Website zu locken, auf der detaillierte Informationen gesammelt wurden. Um den Nutzer schnell zu unüberlegtem Handeln zu verführen, wurde zusätzlich ein Zeitticker eingebaut.



Malware im E-Mail-Traffic

01.11.2009 00:00 - 01.12.2009 00:00		
1	Trojan.Download.37236	10313930 (13.36%)
2	Trojan.Download.47256	9528637 (12.34%)
3	Trojan.Fakealert.5115	6663095 (8.63%)
4	Trojan.MulDrop.40896	6638234 (8.60%)
5	Trojan.Packed.683	5457677 (7.07%)
6	Trojan.Fakealert.5238	4991544 (6.47%)
7	Trojan.Download.50246	3843797 (4.98%)
8	Trojan.Fakealert.5825	3266072 (4.23%)
9	Trojan.Fakealert.5437	2387930 (3.09%)
10	Win32.HLLM.Netsky.35328	2332183 (3.02%)
11	Trojan.Fakealert.5356	2164543 (2.80%)
12	Trojan.Fakealert.5784	1871829 (2.43%)
13	Trojan.PWS.Panda.122	1756350 (2.28%)
14	Trojan.Fakealert.5229	1740878 (2.26%)
15	Trojan.Packed.2915	1618177 (2.10%)
16	Trojan.Fakealert.5457	1525194 (1.98%)
17	Win32.HLLM.Beagle	1273271 (1.65%)
18	Win32.HLLM.MyDoom.33808	1015421 (1.32%)
19	Trojan.Siggen.18256	886946 (1.15%)
20	Trojan.Proxy.7778	839487 (1.09%)

Insgesamt geprüft: 78,826,014,338

Infiziert: 77,187,250 (0.0979%)



Malware auf PCs der Anwender

01.11.2009 00:00 - 01.12.2009 00:00		
1	Win32.HLLW.Gavir.ini	568913 (4.92%)
2	Win32.HLLW.Shadow.based	518583 (4.49%)
3	Trojan.WinSpy.282	449187 (3.89%)
4	Trojan.Redirect.11	441590 (3.82%)
5	Trojan.SqlShell.9	382913 (3.31%)
6	Win32.Sector.17	346204 (3.00%)
7	Trojan.WinSpy.247	312848 (2.71%)
8	Trojan.AppActXComp	303650 (2.63%)
9	Trojan.AuxSpy.74	272309 (2.36%)
10	Win32.Alman.1	256652 (2.22%)
11	Win32.HLLW.Shadow	233635 (2.02%)
12	Win32.HLLW.Autoruner.5555	220766 (1.91%)
13	Trojan.Starter.881	201548 (1.74%)
14	Win32.Rammstein.13346	196029 (1.70%)
15	VBS.Autoruner.8	186965 (1.62%)
16	VBS.Autoruner.4	183627 (1.59%)
17	Trojan.NtRootKit.4672	136259 (1.18%)
18	Trojan.PWS.Multi.110	131735 (1.14%)
19	Trojan.AuxSpy.75	123839 (1.07%)
20	Trojan.AuxSpy.72	123398 (1.07%)

Insgesamt geprüft: 92,781,494,382

Infiziert: 11,558,593 (0.0125%)



Über Doctor Web:

Das russische Unternehmen Doctor Web Ltd. ist einer der führenden Hersteller von Antivirus- und Anti-Spam-Lösungen mit Hauptsitz in Moskau. Das Doctor Web Team verfügt über eine 17-jährige Erfahrung in der Antimalwareentwicklung und beschäftigt 190 Mitarbeiter, davon 100 im Research & Development. Doctor Web ist nicht nur Pionier, sondern auch einer der wenigen Anbieter, die ihre Lösungen vollständig innerbetrieblich entwickeln. Das Unternehmen legt großen Wert auf die effektive Beseitigung von Kundenproblemen und bietet schnelle Antworten auf akute Virengefahren. Die umfangreiche Produktpalette von Doctor Web umfasst effiziente Lösungen zur Absicherung von einzelnen Arbeitsplätzen bis hin zu komplexen Netzwerken. Im deutschsprachigen Raum werden die Produkte von der Doctor Web Deutschland GmbH in Hanau vertrieben. Zu den nationalen und internationalen Kunden zählen neben privaten Anwendern namhafte börsennotierte Unternehmen wie Die Bank von Russland, die Russische Bahn, Gazprom oder Arcelor Mittal sowie Bildungseinrichtungen und öffentliche Auftraggeber wie das Russische Verteidigungsministerium.

Pressekontakt:

Stephan Wild

Fon +49 89 62 81 75 33 | Fax +49 89 62 81 75 11

swild@waggenredstrom.com

Waggener Edstrom Worldwide GmbH
Haimhauserstr. 1
D-80802 München