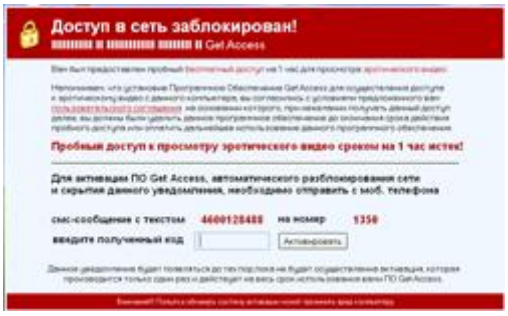
Doctor Web-Virenreport: Trojan.Winlock Infektionen im Januar verdoppelt

Erste Virenepidemie in 2010 mit Trojan.Winlock und zahlreiche neue Betrugsmethoden

Hanau, 9. Februar 2010 – Im Januar 2010 erhielt der Anti-Viren-Spezialist Doctor Web überwiegend Hilferufe von Trojan.Winlock-Opfern. Zu Beginn des Jahres haben die Hacker viel Fantasie entwickelt, um neue Methoden und Verbreitungswege für Schadprogramme zu finden. Zwar ging die Zahl der Schadprogramme im E-Mail-Verkehr gegenüber Dezember 2009 um 30 Prozent zurück und schadhafte Dateien sogar um 35 Prozent. Jedoch hat sich die Zahl der unterschiedlichen Trojan.Winlock Versionen im Januar verdoppelt. Die Mehrzahl der Lösegeldforderungen in diesem Monat erfolgte über das erpresserische Freikaufen infizierter Rechnern per SMS-Nachricht.

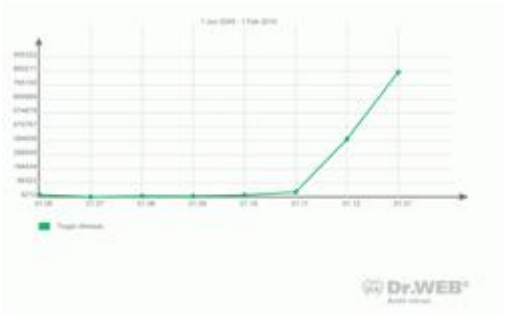
Epidemie neuer Trojan.Winlock-Varianten

Im Januar registrierte Doctor Web vor allem neue Variationen der Trojan.Winlock-Programme. Merkmal der Schadsoftware ist ein eigenes Programmfenster auf dem Bildschirm, das nicht minimiert oder geschlossen werden kann bis ein kostenpflichtiger Freischaltcode eingegeben wurde. Der Trojaner blockiert dafür sogar den normalen Betrieb einiger Programme, die auf dem betroffenen Rechner installiert sind, oder den Zugang ins Internet. Die Absender dieser Malware bieten ihren „Opfern“ in Erpressermanier einen Freischaltcode an, den sie per SMS erwerben können. Zuletzt schwankten die Preise pro Kurznachricht zwischen je 7 und 14 Euro.



Die Statistik-Server von Doctor Web haben allein über 850.000 Infektion auf Rechnern registriert, die durch die Dr. Web Enterprise Suite und Dr. Web Anti-Virus geschützt waren. Die Zahl der registierten Angriffe ist damit mehr als 2,15 so groß wie im vorherigen Monat und sogar 23-mal größer als im November 2009. Die Epidemie grassiert bisher vor allem in

Russland und der Ukraine, Millionen von Rechnern wurden im vergangenen Monat durch die unterschiedlichen Trojaner-Varianten infiziert.



Die russisch-sprachige Internet-Community war im Januar stark durch die Trojaner-Epidemie betroffen. Die Gegenbewegung ließ nicht lange auf sich warten. So boten Anbieter von Kurzwahlnummern kostenlose Entsperrungscode an und die Anti-Virus-Anbieter versorgten ihre Nutzer mit kostenfreien Tools, um die Trojan.Winlock-Programme unschädlich zu machen.

Doctor Web reagierte auf die Angriffswelle und stellte im Januar Betroffenen über seine Website kostenlose Freischaltcodes zur Verfügung. Zusätzlich veröffentlichte das Unternehmen aktualisierte Varianten von Dr.Web CureIt! mit einer speziellen Startkomponente, um die infizierten Rechner von den neuen Trojanern zu säubern.

SMS-Betrug bei Hackern immer beliebter

Die Einfachheit, mit SMS-Betrug Geld zu verdienen, war für viele Cyber-Kriminelle besonders attraktiv. Zusammen mit den Windows-Blockern wurden zahlreiche Webseiten generiert, um für nicht existierende Services zu werben oder für gefälschte Software mit verlockenden Eigenschaften.

Den Nutzern wurden im Internet gefälschte Anti-Virus-Programme angeboten, die denselben Virus in Dateien auf allen Rechnern, ICQ und SMS sniffern gefunden haben, sowie auf Handys, Scannern und ähnlichen Programmen.

In den meisten Fällen bezahlten Nutzer diese Services mit einer SMS. Sobald Telefonanbieter und Polizei begannen, die SMS-Abrechnungssysteme im Zuge der Winlock-Epidemie zu überwachen, wurde es gefährlich für Kriminelle. Um der Kontrolle zu entgehen, griffen die Hacker auf Zahlmethoden zurück, die sie bereits früher erfolgreich verwendet hatten, wie zum Beispiel WebMoney. Sie erfanden sogar komplett neue Wege des Betrugs.

Diebstahl direkt im Mobilfunk-Abo

Eine weitere Methode, die Doctor Web im Januar entdeckte, ist, dass Hacker direkt von Accounts der Mobiltelefonnutzer Gelder abgezogen haben. Die Benutzer geben zuvor ihre Telefonnummer auf einer Website ein und erhalten eine kurze Nachricht mit einem Link, um ihr Abonnement zu aktivieren. Einmal aktiviert, wird die Service-Gebühr automatisch vom Account abgezogen.

Die gefälschte Webseite erlaubt Anwendern, die Nummer einer anderen Person einzugeben. Die Nachricht mit dem Aktivierungs-Link erläutert dem Empfänger nicht näher, um welchen Service es sich handelt. Stattdessen enthält sie falsche Informationen, die den Nutzer ermutigen auf den Link zu klicken, auch wenn er den Service gar nicht abonnieren möchte. Zum Beispiel hieß es in der Nachricht, dass der Link den Nutzer zu einem Bild oder Videoclip führen würde. In den vergangenen Wochen haben Kriminelle Nutzern ebenfalls angeboten, für Dienste mittels eines kostenpflichtigen Anrufs mit Minimum-Laufzeit zu zahlen.

Neue Wege, um Malware und Spam zu verbreiten

Den Virus-Analysten von Doctor Web sind darüber hinaus auch besonders Spam-Mails aufgefallen, die torrent-Dateien als Anhang hatten – angeblich um eCards herunterzuladen, die jedoch Schadprogramme waren. Die E-Mail-Server haben diese Nachrichten nicht blockiert, da die angehängten torrent-Dateien keine gefährlichen Codes enthielten. Spam-Absender haben darüber hinaus neue Wege gefunden, um große Datenmengen zu versenden. So wurden Emails mit mp3-Anhang entdeckt, die mehr als 60 Minuten Wiedergabe enthielten. Die Nutzer bekamen auch Nachrichten mit Links zu Videoclips, die auf den Webseiten der Hacker und auf Youtube verfügbar waren.

Wie erkennt man, dass man einen Trojan.Winlock auf seinem Rechner hat?

Wenn Nutzer feststellen, dass sich auf ihrem Bildschirm ein Fenster geöffnet hat mit der Nachricht, eine SMS an eine Kurznummer zu senden, wurde das System wahrscheinlich mit einer Variante von Trojan.Winlock infiziert. In diesem Fall läss sich das Fenster nicht schließen, sogar wenn das System im abgesicherten Modus gestartet wird,

1. Unter keinen Umständen sollten Nutzer Nachrichten senden, wie von den Hackern gefordert. Jede versendete Nachricht bietet den Angreifern die Möglichkeit, dank der finanziellen Unterstützung neue Schadsoftware zu entwickeln.
2. Nutzer sollten zur Freischalt-Seite gehen.
3. Dort sollten sie die spezielle Version von Dr.Web CureIt! herunterladen und nutzen, um das System zu säubern.
4. Nutzer sollten auf die folgende Webseite gehen http://www.freedrweb.com/ **Dr.Web LiveCD** und Dr.Web LiveCD herunterladen. Einmal installiert ist das System kuriert und Doctor Web empfiehlt, den Rechner zur Sicherheit noch einmal mit Dr.Web CureIt! zu überprüfen.
5. Betroffene Nutzer können sich informieren auf dem Forum von Doctor Web.
6. Nutzer sollten den Anbieter der Kurzwahl kontaktieren, nach einem Freischaltcode

Tipps und Tricks, wie Nutzer ihr System vor Angriffen durch Trojan.Winlock oder ähnlichen Programmen schützen können:

1. Das A und O ist die Installation eines Anti-Virus-Programms sowie regelmäßiger Updates.
2. Die Verwendung eines alternativen Browser wie Mozilla Firefox, Opera oder Google Chrome schützt ebenfalls, auch hier müssen die entsprechenden Sicherheitsupdates des Anbieters installiert werden.
3. Nutzer sollten die Sicherheitsupdates für ihr Betriebssystem installieren, sobald sie veröffentlicht werden.
4. Services, die über Pop-Ups angeboten werden, sind grundsätzlich mit einem Risiko behaftet.
5. Angebote, einen Code oder andere Software herunterzuladen, um auf eine Webseite zu kommen, sollten grundsätzlich ausgeschlagen werden. Nutzer sollten die offizielle Webseite des Herstellers aufsuchen und die Software dort direkt herunterladen und auf ihrem Rechner installieren. In vielen Fällen wurden Trojan.Winlock wurde oft heruntergeladen als Software, um Inhalte auf einer Webseite anzuschauen.

fragen und angeben, dass sie Opfer eines Hackers geworden sind.

Kaum bösartige Dateien im Januar in Mail-Verkehr

Insgesamt geprüft: 139,350,636,730

Infected: 102,115,886 (0.07%)

01.01.2010 00:00 - 01.02.2010 00:00		
1	Trojan.DownLoad.37236 Trojan.DownLoad.37236	13268129 (12.99%) 13268129 (12,99%)
2	Trojan.DownLoad.47256 Trojan.DownLoad.47256	10044467 (9.84%) 10044467 (9,84%)
3	Trojan.MulDrop.40896 Trojan.MulDrop.40896	7096903 (6.95%) 7096903 (6,95%)
4	Trojan.Fakealert.5115 Trojan.Fakealert.5115	7023800 (6.88%) 7023800 (6,88%)
5	Win32.HLLM.MyDoom.44 Win32.HLLM.MyDoom.44	6490377 (6.36%) 6490377 (6,36%)
6	Trojan.Packed.683 Trojan.Packed.683	5749108 (5.63%) 5749108 (5,63%)
7	Trojan.Fakealert.5238 Trojan.Fakealert.5238	5261760 (5.15%) 5261760

		(5,15%)
8	Win32.HLLM.Netsky.35328 Win32.HLLM.Netsky.35328	4772813 (4.67%) 4772813 (4,67%)
9	Trojan.DownLoad.50246 Trojan.DownLoad.50246	4051880 (3.97%) 4051880 (3,97%)
10	Trojan.Botnetlog.zip Trojan.Botnetlog.zip	3758307 (3.68%) 3758307 (3,68%)
11	Trojan.Fakealert.5825 Trojan.Fakealert.5825	3442880 (3.37%) 3442880 (3,37%)
12	Trojan.Fakealert.5437 Trojan.Fakealert.5437	2517200 (2.47%) 2517200 (2,47%)
13	Win32.HLLM.MyDoom.33808 Win32.HLLM.MyDoom.33808	2392000 (2.34%) 2392000 (2,34%)
14	Trojan.Fakealert.5356 Trojan.Fakealert.5356	2281720 (2.23%) 2281720 (2,23%)
15	Trojan.Fakealert.5784 Trojan.Fakealert.5784	1973160 (1.93%) 1973160 (1,93%)

16	Trojan.PWS.Panda.122 Trojan.PWS.Panda.122	1851377 (1.81%) 1851377 (1,81%)
17	Trojan.Fakealert.5229 Trojan.Fakealert.5229	1835120 (1.80%) 1835120 (1,80%)
18	Trojan.Fakealert.5457 Trojan.Fakealert.5457	1607760 (1.57%) 1607760 (1,57%)
19	Trojan.Siggen.18256 Trojan.Siggen.18256	1526581 (1.49%) 1526581 (1,49%)
20	Win32.HLLM.Beagle Win32.HLLM.Beagle	1505664 (1.47%) 1505664 (1,47%)

Kaum bösartige Dateien im Januar auf den Computern der Nutzer

Insgesamt geprüft: 169,874,198,147

Infected: 23,938,315 (0.01%)

01.01.2010 00:00 - 01.02.2010 00:00		
1	Win32.HLLM.MyDoom.49 Win32.HLLM.MyDoom.49	4020788 (16.80%) 4020788 (16,80%)
2	Win32.HLLM.Netsky.35328 Win32.HLLM.Netsky.35328	1637229 (6.84%) 1637229 (6,84%)
3	Win32.HLLW.Gavir.ini Win32.HLLW.Gavir.ini	1081250 (4.52%) 1081250 (4,52%)

4	Trojan.WinSpy.440 Trojan.WinSpy.440	1053086 (4.40%) 1053086 (4,40%)
5	Trojan.AppActXComp Trojan.AppActXComp	907785 (3.79%) 907785 (3,79%)
6	Trojan.AuxSpy.137 Trojan.AuxSpy.137	734318 (3.07%) 734318 (3,07%)
7	Win32.HLLM.Beagle Win32.HLLM.Beagle	656944 (2.74%) 656944 (2,74%)
8	Win32.HLLM.MyDoom.33808 Win32.HLLM.MyDoom.33808	646730 (2.70%) 646730 (2,70%)
9	Trojan.PWS.Gamania.23481 Trojan.PWS.Gamania.23481	623699 (2.61%) 623699 (2,61%)
10	Trojan.MulDrop.16727 Trojan.MulDrop.16727	584477 (2.44%) 584477 (2,44%)
11	Win32.HLLW.Shadow Win32.HLLW.Shadow	513252 (2.14%) 513252 (2,14%)
12	Win32.Virut.5 Win32.Virut.5	493248 (2.06%) 493248 (2,06%)
13	Win32.HLLW.Shadow.based Win32.HLLW.Shadow.based	380166 (1.59%) 380166 (1,59%)
14	Trojan.MulDrop.13408 Trojan.MulDrop.13408	325488 (1.36%) 325488 (1,36%)
15	JS.Popup.1 JS.Popup.1	316857 (1.32%) 316857 (1,32%)
16	Win32.Virut.14 Win32.Virut.14	295463 (1.23%) 295463 (1,23%)
17	Win32.HLLW.Kazaa.17 Win32.HLLW.Kazaa.17	263143 (1.10%) 263143 (1,10%)

18	Win32.Alman.1 Win32.Alman.1	261298 (1.09%) 261298 (1,09%)
19	Exploit.MySql.11 Exploit.MySql.11	260470 (1.09%) 260470 (1,09%)
20	Trojan.Winlock.715 Trojan.Winlock.715	256356 (1.07%) 256356 (1