W32.Qakbot aka W32/Pinkslipbot or infostealer worm

Archived: 2026-04-06 01:35:51 UTC

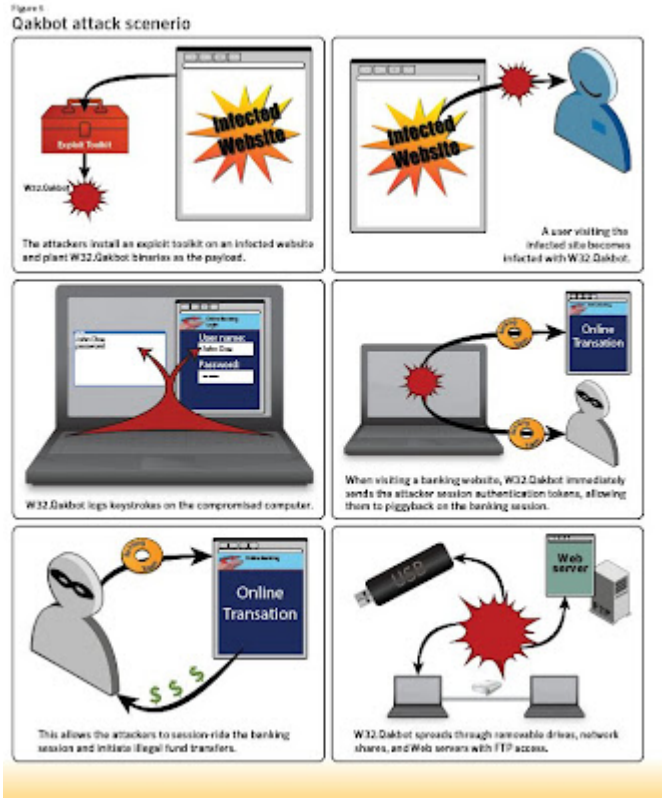
W32.Qakbot aka W32/Pinkslipbot or infostealer worm

W32.Qakbot aka W32/Pinkslipbot

W32.Qakbot in Detail by Symantec Nicolas Falliere

> **W32.Qakbot is a worm that has been seen spreading through network shares, removable drives, and infected webpages, and infecting computers since mid-2009. Its primary purpose is to steal online banking account information from compromised computers. The malware controllers use the stolen information to access client accounts within various financial service websites with the intent of moving currency to accounts from which they can withdraw funds. It employs a classic keylogger, but is unique in that it also steals active session authentication tokens and then piggy backs on the existing online banking sessions. It then quickly uses that information for malicious purposes.**

The following screenshot is from the paper you see above



General File Information

MD5 076bc0533d63826e1e809ad9fcbe2fb8
SHA1 33d9b4a712c29304478da235f17cd28978a93d2f
File size :55808 bytes
Type: PE32 exe
Distribution: mostly web (worm - spreads through shares, drives, webpages etc)

MD5 120d845ac973b4a0cde2bc88d8530b3d
SHA1 120d845ac973b4a0cde2bc88d8530b3d
File size :87040 bytes
Type: PE32 exe
Distribution: mostly web (worm - spreads through shares, drives, webpages etc)

MD5 150d006eab34528e3305fbbb5ad82164
SHA1 551a9f3ce5b86cf77df90eda61be233c821be6b2
File size :267776 bytes
Type: PE32 exe
Distribution: mostly web (worm - spreads through shares, drives, webpages etc)

Download

Message Headers

Received: (qmail 25793 invoked from network); 19 Nov 2010 08:53:27 -0000
Received: from msr19.hinet.net (HELO msr19.hinet.net) (168.95.4.119)
  by XXXXXXXXXXXX with SMTP; 19 Nov 2010 08:53:27 -0000
Received: from elizabethhamrickpc (61-222-104-222.HINET-IP.hinet.net [61.222.104.222])
by msr19.hinet.net (8.9.3/8.9.3) with ESMTP id QAA04206
for

; Fri, 19 Nov 2010 16:53:09 +0800 (CST)

Reply-To: newscomeon@yahoo.com
From: "Elizabeth Hamrick"

To: XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Subject: Event Invitation from The Heritage Foundation: The Implications of Taiwan's Big City Elections
Date: Fri, 19 Nov 2010 16:53:09 +0800
Message-ID:

MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----=_NextPart_101119164822358103226 85_000"
X-Priority: 3
X-Mailer: DreamMail 4.6.6.0

Automated Scans

File name: 076bc0533d63826e1e809ad9fcbe2fb8

Submission date: 2011-01-04 17:47:53 (UTC)
Result: 38 /41 (92.7%)
Compact Print results Antivirus Version Last Update Result
AhnLab-V3 2011.01.04.03 2011.01.04 Win-Trojan/Injector.55808.U
AntiVir 7.11.1.24 2011.01.04 TR/PSW.Qbot.aff
Antiy-AVL 2.0.3.7 2011.01.04 Trojan/Win32.Qbot.gen
Avast 4.8.1351.0 2011.01.04 Win32:Oficla-BS
Avast5 5.0.677.0 2011.01.04 Win32:Oficla-BS
AVG 9.0.0.851 2011.01.04 PSW.Generic8.AJKY
BitDefender 7.2 2011.01.04 Gen:Variant.Kazy.517
CAT-QuickHeal 11.00 2011.01.04 TrojanPSW.Qbot.aff
Command 5.2.11.5 2011.01.04 W32/MalwareF.RPCP
Comodo 7292 2011.01.04 Heur.Suspicious
DrWeb 5.0.2.03300 2011.01.04 Trojan.DownLoader1.39437
eSafe 7.0.17.0 2011.01.02 Win32.GenVariant.Kaz
eTrust-Vet 36.1.8080 2011.01.04 Win32/QakbotCryptor
F-Prot 4.6.2.117 2011.01.04 W32/MalwareF.RPCP
F-Secure 9.0.16160.0 2011.01.04 Gen:Variant.Kazy.517
Fortinet 4.2.254.0 2011.01.03 W32/Krypt.D!tr.dldr
GData 21 2011.01.04 Gen:Variant.Kazy.517
Ikarus T3.1.1.90.0 2011.01.04 Trojan-PWS.Win32.Qbot
K7AntiVirus 9.75.3435 2011.01.04 Password-Stealer
McAfee 5.400.0.1158 2011.01.04 W32/Pinkslipbot.gen.w
McAfee-GW-Edition 2010.1C 2011.01.04 W32/Pinkslipbot.gen.w

Microsoft 1.6402 2011.01.04 Backdoor:Win32/Qakbot.gen!A
NOD32 5759 2011.01.04 a variant of Win32/Kryptik.IMP
Norman 6.06.12 2011.01.03 Qakbot.CU
nProtect 2011-01-04.01 2011.01.04 Gen:Variant.Kazy.517
Panda 10.0.2.7 2011.01.04 Bck/Qbot.AO
PCTools 7.0.3.5 2011.01.04 Trojan-PSW.Generic
Prevx 3.0 2011.01.04 High Risk Cloaked Malware
Rising 22.81.01.03 2011.01.04 Trojan.Win32.Generic.524A8E11
Sophos 4.60.0 2011.01.04 Troj/QBot-AA
SUPERAntiSpyware 4.40.0.1006 2011.01.04 -
Symantec 20101.3.0.103 2011.01.04 Infostealer
TheHacker 6.7.0.1.110 2011.01.03 Trojan/PSW.Qbot.aff
TrendMicro 9.120.0.1004 2011.01.04 BKDR_QAKBOT.SME
TrendMicro-HouseCall 9.120.0.1004 2011.01.04 BKDR_QAKBOT.SME
VBA32 3.12.14.2 2011.01.04 Trojan-PSW.Win32.Qbot.aff
VIPRE 7952 2011.01.04 Backdoor.Win32.Qakbot
ViRobot 2011.1.4.4236 2011.01.04 Trojan.Win32.PSWQbot.55808
VirusBuster 13.6.127.0 2011.01.04 Trojan.PWS.Qbot!9zgzgM2LbIY
Additional informationShow all
MD5 : 076bc0533d63826e1e809ad9fcbe2fb8

file

http://www.virustotal.com/file-scan/report.html?id=a0fdd16f65c09159c673e82096905a68b772b5efc79259f3cee4cdbba3209724-1287656963
Submission date: 2010-10-21 10:29:23 (UTC)
Result: 34 /42 (81.0%)
Compact Print results Antivirus Version Last Update Result
AhnLab-V3 2010.10.21.02 2010.10.21 Dropper/Win32.Drooptroop
AntiVir 7.10.13.12 2010.10.21 TR/Irux.A
Authentium 5.2.0.5 2010.10.21 W32/Bamital.D.gen!Eldorado
Avast 4.8.1351.0 2010.10.21 Win32:Crypt-HTA
Avast5 5.0.594.0 2010.10.21 Win32:Crypt-HTA
AVG 9.0.0.851 2010.10.21 Generic19.BCWJ
BitDefender 7.2 2010.10.21 Trojan.Generic.4934134
CAT-QuickHeal 11.00 2010.10.21 Backdoor.Qakbot.a
Comodo 6463 2010.10.21 UnclassifiedMalware
eTrust-Vet 36.1.7924 2010.10.21 Win32/Qakbot.EU
F-Prot 4.6.2.117 2010.10.20 W32/Bamital.D.gen!Eldorado
F-Secure 9.0.16160.0 2010.10.21 Trojan.Generic.4934134
Fortinet 4.2.249.0 2010.10.21 W32/Krypt.D!tr.dldr
GData 21 2010.10.21 Trojan.Generic.4934134
Ikarus T3.1.1.90.0 2010.10.21 Trojan-PWS.Win32.Qbot

K7AntiVirus 9.66.2798 2010.10.20 Riskware
Kaspersky 7.0.0.125 2010.10.21 Trojan-Dropper.Win32.Drooptroop.gss
McAfee 5.400.0.1158 2010.10.21 W32/Pinkslipbot.gen.r
McAfee-GW-Edition 2010.1C 2010.10.21 Generic.dx!uhr
Microsoft 1.6301 2010.10.21 Backdoor:Win32/Qakbot.gen!A
NOD32 5550 2010.10.21 a variant of Win32/Kryptik.HJF
Norman 6.06.10 2010.10.20 W32/Smalltroj.ZKOE
nProtect 2010-10-21.01 2010.10.21 Trojan.Generic.4934134
Panda 10.0.2.7 2010.10.20 W32/Qbot.W.worm
PCTools 7.0.3.5 2010.10.21 Malware.Qakbot!rem
Prevx 3.0 2010.10.21 Medium Risk Malware
Rising 22.70.02.05 2010.10.21 Trojan.Win32.Generic.523C21B2
Sophos 4.58.0 2010.10.21 Mal/Oficla-A
Sunbelt 7109 2010.10.21 Backdoor.Win32.Qakbot
SUPERAntiSpyware 4.40.0.1006 2010.10.21 -
Symantec 20101.2.0.161 2010.10.21 W32.Qakbot
TheHacker 6.7.0.1.063 2010.10.20 Trojan/Kryptik.hjf
TrendMicro 9.120.0.1004 2010.10.21 BKDR_QAKBOT.EOF
TrendMicro-HouseCall 9.120.0.1004 2010.10.21 BKDR_QAKBOT.EOF
VirusBuster 12.69.9.0 2010.10.20 Trojan.Kryptik.BHXH

MD5 : 120d845ac973b4a0cde2bc88d8530b3d

150d006eab34528e3305fbbb5ad82164
Submission date: 2011-02-24 01:01:36 (UTC)
Result: 40 /43 (93.0%)
http://www.virustotal.com/file-scan/report.html?id=50f3460bcb2fbf92e97193391e06c955057cc5b81b5f0141ce7c76bbf1b8d99d-1298509296
Compact Print results Antivirus Version Last Update Result
AhnLab-V3 2011.02.24.00 2011.02.24 Win32/Ircbot.worm.variant
AntiVir 7.11.3.207 2011.02.23 BDS/Bot.130361
Antiy-AVL 2.0.3.7 2011.02.23 Trojan/Win32.Zbot.gen
Avast 4.8.1351.0 2011.02.23 Win32:Oficla-AR
Avast5 5.0.677.0 2011.02.23 Win32:Oficla-AR
AVG 10.0.0.1190 2011.02.23 Generic_r.EW
BitDefender 7.2 2011.02.24 Backdoor.Bot.130361
CAT-QuickHeal 11.00 2011.02.23 TrojanSpy.Zbot.asod
Commtouch 5.2.11.5 2011.02.23 W32/Oficla.R.gen!Eldorado
Comodo 7787 2011.02.23 TrojWare.Win32.Fraudpack.ICM
DrWeb 5.0.2.03300 2011.02.24 Trojan.Hottrend.28
Emsisoft 5.1.0.2 2011.02.23 Trojan-Spy.Win32.Zbot!IK
eTrust-Vet 36.1.8179 2011.02.23 Win32/Qakbot.FF
F-Prot 4.6.2.117 2011.02.23 W32/Oficla.R.gen!Eldorado

F-Secure 9.0.16160.0 2011.02.24 Backdoor.Bot.130361
Fortinet 4.2.254.0 2011.02.23 W32/Oficla.AWV!tr
GData 21 2011.02.24 Backdoor.Bot.130361
Ikarus T3.1.1.97.0 2011.02.23 Trojan-Spy.Win32.Zbot
Jiangmin 13.0.900 2011.02.23 TrojanSpy.Zbot.ryt
K7AntiVirus 9.90.3944 2011.02.23 Spyware
Kaspersky 7.0.0.125 2011.02.24 Trojan-Spy.Win32.Zbot.asod
McAfee 5.400.0.1158 2011.02.24 W32/Pinkslipbot.gen.j
McAfee-GW-Edition 2010.1C 2011.02.23 W32/Pinkslipbot.gen.j
Microsoft 1.6603 2011.02.24 Backdoor:Win32/Qakbot.gen!A
NOD32 5901 2011.02.23 Win32/Qbot.AU
Norman 6.07.03 2011.02.23 Qakbot.CH
nProtect 2011-02-10.01 2011.02.15 Trojan-Spy/W32.ZBot.267776.W
Panda 10.0.3.5 2011.02.23 Trj/Downloader.WBX
PCTools 7.0.3.5 2011.02.22 Malware.Qakbot!rem
Prevx 3.0 2011.02.24 Medium Risk Malware
Rising 23.46.02.06 2011.02.23 Trojan.Win32.Generic.125E1D4C
Sophos 4.61.0 2011.02.23 Mal/Qbot-E
SUPERAntiSpyware 4.40.0.1006 2011.02.24 Trojan.Agent/Gen
Symantec 20101.3.0.103 2011.02.24 W32.Qakbot
TheHacker 6.7.0.1.137 2011.02.23 Trojan/Spy.Zbot.asod
TrendMicro 9.200.0.1012 2011.02.23 BKDR_QAKBOT.USK
TrendMicro-HouseCall 9.200.0.1012 2011.02.24 BKDR_QAKBOT.USK
VBA32 3.12.14.3 2011.02.23 TrojanDownloader.Genome.btgl
VIPRE 8518 2011.02.24 Backdoor.Win32.Qakbot.cd (v)
ViRobot 2011.2.23.4325 2011.02.23 -
VirusBuster 13.6.217.0 2011.02.23 TrojanSpy.Zbot!B9r7grTAp/E
Additional informationShow all
MD5 : 150d006eab34528e3305fbbb5ad82164
