

Утро 29 октября ознаменовалось эпидемией почтового червя

Утро 29 октября ознаменовалось началом мощной эпидемии почтового червя I-Worm.Bagle.at, которые объёмом генерируемого трафика парализовал многие локальные сети. Как сообщили корреспонденту интернет-издания «NewsProm.Ru» в Украинском антивирусном центре, червь распространяется по электронной почте в виде прикрепленных файлов. При этом имя файла может быть либо JOKE либо PRICE, а расширение файла выбирается из следующего списка: COM, CPL, EXE, SCR. Исполняемый файл червя имеет изменяющийся размер между 18 и 22 Кбайтами и упакован утилитой сжатия файлов PeX.

После запуска червь создаёт в системной папке Windows файл wingo.exe и создаёт в реестре ключ, приводящий к автоматическому запуску червя при загрузке операционной системы:

```
HKEY_CURRENT_USERSOFTWAREMicrosoftWindowsCurrentVersionRun
```

```
wingo=%SYSTEMDIR%wingo.exe
```

I-Worm.Bagle.at ищет в памяти ряд процессов и при обнаружении таковых выгружает их из памяти. Список выгружаемых процессов: mcagent.exe mcvsshld.exe mcshield.exe mcvsescn.exe mcvsrte.exe DefWatch.exe Rtvscan.exe ccEvtMgr.exe NISUM.EXE ccPxySvc.exe navapsvc.exe NPROTECT.EXE nopdb.exe ccApp.exe Avsynmgr.exe VsStat.exe Vshwin32.exe alogserv.exe RuLaunch.exe Avconsol.exe PavFires.exe FIREWALL.EXE ATUPDATER.EXE LUALL.EXE DRWEBUPW.EXE AUTODOWN.EXE NUPGRADE.EXE OUTPOST.EXE ICSSUPNT.EXE ICSUPP95.EXE ESCANH95.EXE AVXQUAR.EXE ESCANHNT.EXE ATUPDATER.EXE AUPDATE.EXE AUTOTRACE.EXE AUTOUPDATE.EXE AVXQUAR.EXE AVWUPD32.EXE AVPUPD.EXE CFIAUDIT.EXE UPDATE.EXE NUPGRADE.EXE MCUPDATE.EXE pavsrv50.exe AVENGINE.EXE APVXDWIN.EXE pavProxy.exe navapw32.exe navapsvc.exe ccProxy.exe navapsvc.exe NPROTECT.EXE SAVScan.exe SNDSrv.exe symclsvc.exe LUCOMS~1.EXE blackd.exe bawindo.exe FrameworkService.exe VsTskMgr.exe SHSTAT.EXE UpdaterUI.exe

Червь открывает TCP/IP порт 81 и ожидает удалённых команд, отдавая полный доступ к компьютеру злоумышленникам.

I-Worm.Bagle.at пытается обращаться на ряд сайтов и скачать с них файл G.JPG. Список сайтов, к которым он пытается обратиться приведён ниже:

<http://www.24-7-transportation.com>

<http://www.adhdtests.com>

<http://www.aegee.org>

<http://www.aimcenter.net>

<http://www.alupass.lu>

<http://www.amanit.ru>

<http://www.andara.com>

<http://www.angelartsanctuary.com>

<http://www.anthonyflanagan.com>

<http://www.approved1stmortgage.com>

<http://www.argontech.net>
<http://www.asianfestival.nl>
<http://www.atlantisteste.hpg.com.br>
<http://www.aviation-center.de>
<http://www.bbsh.org>
<http://www.bga-gsm.ru>
<http://www.boneheadmusic.com>
<http://www.bottombouncer.com>
<http://www.bradster.com>
<http://www.buddyboymusic.com>
<http://www.bueroservice-it.de>
<http://www.calderwoodinn.com>
<http://www.capri-frames.de>
<http://www.celula.com.mx>
<http://www.ceskyhosting.cz>
<http://www.chinasenfa.com>
<http://www.cntv.info>
<http://www.compsolutionstore.com>
<http://www.coolfreepages.com>
<http://www.corpsite.com>
<http://www.corpsite.com>
<http://www.couponcapital.net>
<http://www.cpc.adv.br>
<http://www.crystalrose.ca>
<http://www.cscliberec.cz>
<http://www.curtmarsh.com>
<http://www.customloyal.com>
<http://www.DarrkSydebaby.com>
<http://www.deadrobot.com>
<http://www.dontbeaweekendparent.com>
<http://www.dragcar.com>
<http://www.ecofotos.com.br>
<http://www.elenalazar.com>
<http://www.ellarouge.com.au>

<http://www.esperanzaparalafamilia.com>

<http://www.eurostavba.sk>

<http://www.everett.wednet.edu>

<http://www.fcpages.com>

<http://www.featech.com>

<http://www.fepese.ufsc.br>

<http://www.firstnightoceancounty.org>

<http://www.flashcorp.com>

<http://www.fleigutaetscher.ch>

<http://www.fludir.is>

<http://www.freesevers.com>

<http://www.FritoPie.NET>

<http://www.gamp.pl>

<http://www.gci-blh.de>

<http://www.gcnet.ru>

<http://www.generationnow.net>

<http://www.gfn.org>

<http://www.giantrevenue.com>

<http://www.glass.la>

<http://www.handsforhealth.com>

<http://www.hartacorporation.com>

<http://www.himpsi.org>

<http://www.idb-group.net>

<http://www.immonaut.sk>

<http://www.ims-i.com>

<http://www.innnewport.com>

<http://www.irakli.org>

<http://www.irinaswelt.de>

<http://www.jansenboiler.com>

<http://www.jasnet.pl>

<http://www.jhaforpresident.7p.com>

<http://www.jimvann.com>

<http://www.jldr.ca>

<http://www.justrepublicans.com>
<http://www.kencorbett.com>
<http://www.knicks.nl>
<http://www.kps4parents.com>
<http://www.kradtraining.de>
<http://www.kranenberg.de>
<http://www.lasermach.com>
<http://www.leonhendrix.com>
<http://www.magicbottle.com.tw>
<http://www.mass-i.kiev.ua>
<http://www.mepbisu.de>
<http://www.mepmh.de>
<http://www.metal.pl>
<http://www.mexis.com>
<http://www.mongolische-renner.de>
<http://www.mtfdesign.com>
<http://www.oboe-online.com>
<http://www.ohiolimo.com>
<http://www.onepositiveplace.org>
<http://www.oohlala-kirkland.com>
<http://www.orari.net>
<http://www.pankration.com>
<http://www.pe-sh.com>
<http://www.pfadfinder-leobersdorf.com>
<http://www.pipni.cz>
<http://www.polizeimotorrad.de>
<http://www.programmierung2000.de>
<http://www.pyrlandia-boogie.pl>
<http://www.raecoinc.com>
<http://www.realgps.com>
<http://www.redlightpictures.com>
<http://www.reliance-yachts.com>
<http://www.relocationflorida.com>
<http://www.rentalstation.com>

<http://www.rieraquadros.com.br>
<http://www.scanex-medical.fi>
<http://www.sea.bz.it>
<http://www.selu.edu>
<http://www.sigi.lu>
<http://www.sljinc.com>
<http://www.smacgreetings.com>
<http://www.soloconsulting.com>
<http://www.spadochron.pl>
<http://www.srg-neuburg.de>
<http://www.ssmifc.ca>
<http://www.sugardas.lt>
<http://www.sunassetholdings.com>
<http://www.szantomierz.art.pl>
<http://www.the-fabulous-lions.de>
<http://www.tivogoddess.com>
<http://www.tkd2xcell.com>
<http://www.topko.sk>
<http://www.transportation.gov.bh>
<http://www.travelchronic.de>
<http://www.traverse.com>
<http://www.uhcc.com>
<http://www.ulpiano.org>
<http://www.uslungiarue.it>
<http://www.vandermost.de>
<http://www.vbw.info>
<http://www.velezcourtesymanagement.com>
<http://www.velocityprint.com>
<http://www.vikingpc.pl>
<http://www.vinirforge.com>
<http://www.wecompete.com>
<http://www.worest.com.ar>
<http://www.woundedshepherds.com>

http://www.wwwebad.com

http://www.wwwebmaster.com

Размножение по электронной почте

Письма с телом червя имеют следующий вид:

Тема письма выбирается из списка:

Re:

Re:Hello

Re:Hi

Re:Thank you!

Re:Thanks:)

Текст сообщения:

:)

:))

Имя присоединённого файла:

JOKE

PRICE

Расширение присоединённого файла:

COM

CPL

EXE

SCR

Адреса электронной почты, на которые производится рассылка и которые подставляются в качестве обратного адреса выбираются из файлов на дисках с расширениями: wab txt msg htm shtm stm xml dbx mbx mdx eml nch mmf ods cfg asp php pl wsh adb tbb sht xls oft uin cgi mht dhtm jsp.

Если в адресе электронной почты фигурирует подстрока из списка, приведённого ниже, то вирус игнорирует данный адрес (не отправляет на него инфицированные письма): @hotmail @msn @microsoft rating@ f-secr news update anyone@ bugs@ contract@ feste gold-certs@ help@ info@ nobody@ noone@ kasp admin icrosoft support ntivi unix bsd linux listserv certific sopho @foo @iana free-av @messagelab winzip google winrar samples abuse panda cafee spam pgp @avp. noreply local root@ postmaster@

Размножение в сетях PeerToPeer (P2P)

Червь размножается в сетях P2P создавая свои копии во всех папках, в имени которых есть подстрока «shar». Имена создаваемых файлов выбираются из списка:

Microsoft Office 2003 Crack, Working.exe

Microsoft Windows XP, WinXP Crack, working Keygen.exe

Microsoft Office XP working Crack, Keygen.exe

Porno, sex, oral, anal cool, awesome.exe

Porno Screensaver.scr

Serials.txt.exe

KAV 5.0

Kaspersky Antivirus 5.0

Porno pics arhive, xxx.exe

Windows Sourcecode update.doc.exe

Ahead Nero 7.exe

Windown Longhorn Beta Leak.exe

Opera 8 New.exe

XXX hardcore images.exe

WinAmp 6 New.exe

WinAmp 5 Pro Keygen Crack Update.exe

Adobe Photoshop 9 full.exe

Matrix 3 Revolution English Subtitles.exe

ACDSee 9.exe

Обновление, детектирующее и нейтрализующее данного червя, доступно для пользователей Украинского Антивирусного Центра. Рекомендуем всем пользователям произвести обновление и проверить системы на наличие вирусов.

Автор: Артур Скальский © NewProm.ru ИНТЕРНЕТ , МИР 👁 3432 29.10.2004, 22:16 📌 217

URL: <https://babr24.com/?ADE=17125> Bytes: 8223 / 8223 Версия для печати

👍 Порекомендовать текст

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:

- [Телеграм](#)

- [ВКонтакте](#)

Связаться с редакцией Бабра:

newsbabr@gmail.com

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot

Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь

Телеграм: @bur24_link_bot

эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова

Телеграм: @irk24_link_bot

эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: [@kras24_link_bot](https://t.me/@kras24_link_bot)
эл.почта: kasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: [@nsk24_link_bot](https://t.me/@nsk24_link_bot)
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: [@tomsk24_link_bot](https://t.me/@tomsk24_link_bot)
эл.почта: tomsk.babr@gmail.com

[Прислать свою новость](#)

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: [@babrobot_bot](https://t.me/@babrobot_bot)
эл.почта: equatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

[Подробнее о размещении](#)

[Отказ от ответственности](#)

[Правила перепечаток](#)

[Соглашение о франчайзинге](#)

[Что такое Бабр24](#)

[Вакансии](#)

[Статистика сайта](#)

[Архив](#)

[Календарь](#)

[Зеркала сайта](#)