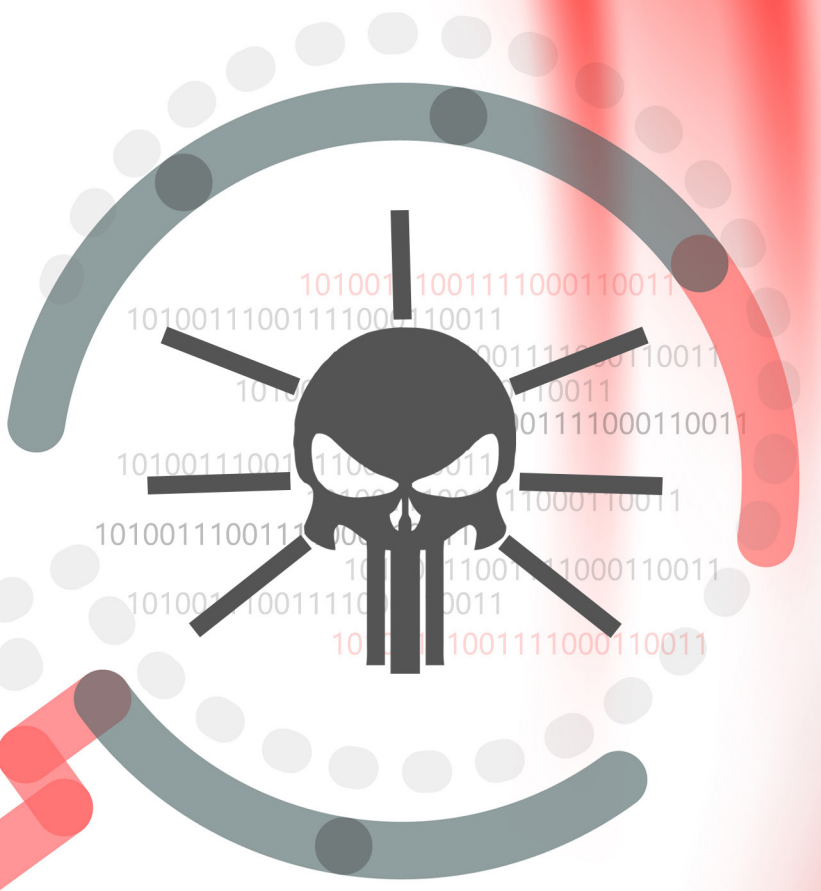
CONFICKER

مجموعه گزارش‌های پلیدهای ابدی



شبکه گستر

امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی

نخستین نسخه از بدافزار Conficker در آبان ۱۳۸۷ شناسایی شد. این بدافزار با عملکردی کرم‌گونه[۱] با بهره‌جویی از یک آسیب‌پذیری امنیتی در سیستم عامل Windows، اجرای حمله‌ای مبتنی بر لغت‌نامه[۲] و آلوده‌سازی حافظه‌های جداشدنی[۳]، در مدتی بسیار کوتاه موفق به تسخیر میلیون‌ها دستگاه در بیش از ۱۹۰ کشور جهان شد. تا فروردین ۱۳۸۸ چهار نسخه دیگر از این بدافزار انتشار یافت.

Downup، Downadup و Kido از دیگر نام‌هایی هستند که از سوی شرکت‌های ضدویروس برای این بدافزار انتخاب شده است. کلمه Conficker نیز از نشانی traf**ficcon**ver**ter**.biz که در کد نسخه A این بدافزار وجود دارد برگرفته شده است:

- (fic)(con)(er) => (con)(fic)(+k)(er) => conficker

در نامگذاری، نسخه‌های Conficker با نویسه‌های[۴] A تا E از یکدیگر متمایز شده‌اند. در توسعه این بدافزار از روش‌های مبهم‌سازی[۵] و رمزگذاری متعددی استفاده شده که در زمان خود کم‌نظیر بوده است.

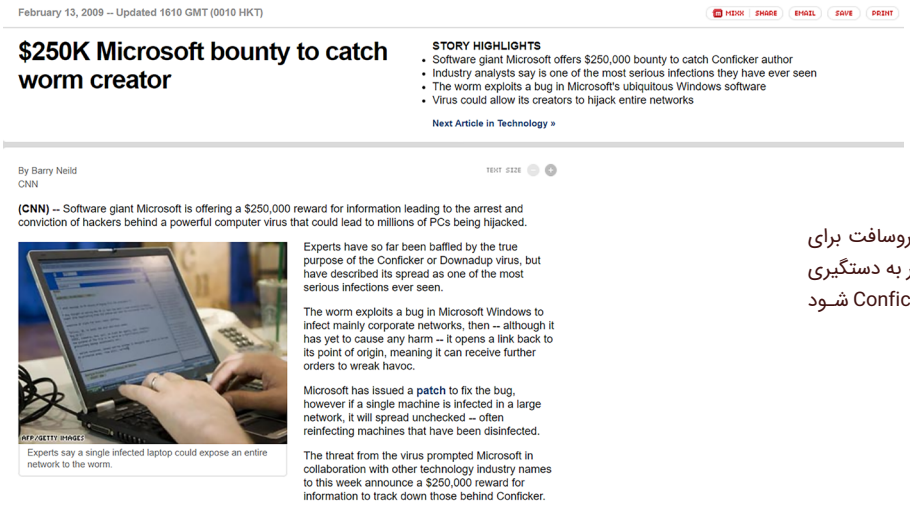
در ۲۵ بهمن ۱۳۸۷، شرکت مایکروسافت اعلام کرد که به ارائه‌دهنده اطلاعاتی که منجر به دستگیری و محاکمه افراد پشت‌صحنه ساخت و انتشار این بدافزار شود پاداشی ۲۵۰ هزار دلاری اعطا خواهد کرد. علیرغم این پاداش هنگفت، هیچگاه هویت نویسندگان Conficker فاش نشد.

برخی کارشناسان، کشور اوکراین را مبداء این بدافزار معرفی کرده‌اند. به‌خصوص آنکه در اکثر نسخه‌های Conficker، بدافزار اجرای خود را بر روی سیستم‌های با نشانی IP متعلق به اوکراین یا قالب صفحه کلید[۶] با زبان این کشور متوقف می‌کند. برای تشخیص کشوری که دستگاه آلوده شده در آن قرار دارد از سایت‌های زیر استفاده می‌شود:

- getmyip.org
- getmyip.co.uk
- checkip.dyndns.org
- whatsmyipaddress.com

نکته قابل توجه اینکه علیرغم گذشت حدود ۱۲ سال از عرضه اصلاحیه امنیتی آسیب‌پذیری مورد بهره‌جویی این بدافزار و غیرفعال شدن مکانیزم به‌روزرسانی آن، Conficker همچنان در حال جولان دادن در شبکه بسیاری از سازمان‌ها در کشورهای مختلف از جمله ایران است.

در این گزارش ضمن بررسی و تحلیل عملکرد Conficker به راه‌های مقابله با این بدافزار و پاکسازی آن پرداخته شده است.



February 13, 2009 -- Updated 1610 GMT (0010 HKT)

$250K Microsoft bounty to catch worm creator

STORY HIGHLIGHTS
- Software giant Microsoft offers $250,000 bounty to catch Conficker author
- Industry analysts say is one of the most serious infections they have ever seen
- The worm exploits a bug in Microsoft's ubiquitous Windows software
- Virus could allow its creators to hijack entire networks

Next Article in Technology »

By Barry Neild
CNN

(CNN) -- Software giant Microsoft is offering a $250,000 reward for information leading to the arrest and conviction of hackers behind a powerful computer virus that could lead to millions of PCs being hijacked.

Experts say a single infected laptop could expose an entire network to the worm.

Experts have so far been baffled by the true purpose of the Conficker or Downadup virus, but have described its spread as one of the most serious infections ever seen.

The worm exploits a bug in Microsoft Windows to infect mainly corporate networks, then -- although it has yet to cause any harm -- it opens a link back to its point of origin, meaning it can receive further orders to wreak havoc.

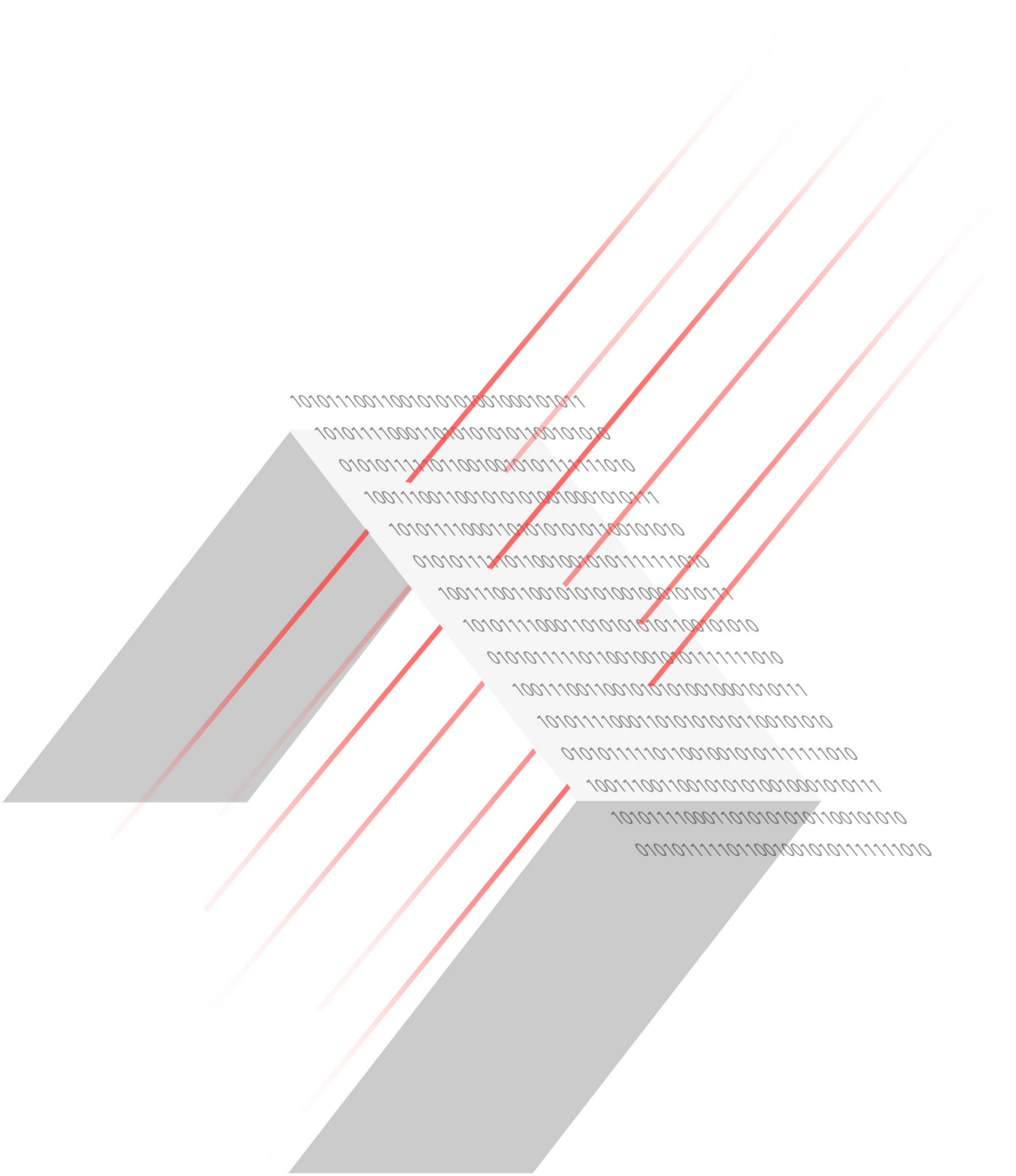
Microsoft has issued a patch to fix the bug, however if a single machine is infected in a large network, it will spread unchecked -- often reinfecting machines that have been disinfected.

The threat from the virus prompted Microsoft in collaboration with other technology industry names to this week announce a $250,000 reward for information to track down those behind Conficker.

پاداش ۲۵۰ هزار دلاری مایکروسافت برای ارائه‌دهنده اطلاعاتی که منجر به دستگیری نویسنده یا نویسندگان Conficker شود

۱ Worm
۲ Dictionary Attack
۳ Removable Storage
۴ Character
۵ Obfuscation
۶ Keyboard Layout

روش کـار



Conficker فایل مخرب خود را در قالب یک فایل DLL مخفی[۱] با نامی تصادفی[۲] در یکی از مسیرهای زیر کپی می‌کند.

- %WinDir%\System32
- %ProgramFiles%\Movie Maker
- %ProgramFiles%\Internet Explorer
- %ProgramFiles%\Windows Media Player
- %ProgramFiles%\Windows NT
- %Application Data%
- %Temp%

نام فایل DLL رشته‌ای[۳] با طول ۵ تا ۹ نویسه تصادفی است که در برخی از نسخه‌ها، درهم‌ساز[۴] نام دستگاه در نحوه انتخاب آنها دخیل بوده است.

Conficker، مالکیت فایل DLL را به کاربر System تخصیص می‌دهد تا بدین‌ترتیب حتی کاربر با سطح دسترسی Administrator نیز قادر به حذف آن نباشد.

این بدافزار با ساخت کلیدی با نام تصادفی در مسیرهای زیر در محضرخانه[۵] سیستم عامل، خود را در هر بار راه‌اندازی شدن[۶] دستگاه از طریق پروسه معتبر rundll32 به اجرا در می‌آورد:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Conficker قادر است که از طریق فایل معتبر svchost.exe خود را در قالب یک سرویس اجرا کند. سرویس (جعلی) مذکور در مسیرهای زیر در محضرخانه ثبت می‌شود:

- HKLM\SYSTEM\CurrentControlSet\Services
- HKLM\SYSTEM\ControlSet001\Services

در نامگذاری سرویس از ترکیب یک رشته از بند نخست و رشته‌ای از بند دوم زیر استفاده می‌شود:

- App, Audio, DM, ER, Event, help, Ias, Ir, Lanman, Net, Ntms, Ras, Remote, Sec, SR, Tapi, Trk, W32, win, Wmdm, Wmi, wsc, wuau, xml
- access, agent, auto, logon, man, mgmt, mon, prov, serv, Server, Service, Srv, srv, Svc, svc, System, Time

نام نمایشی[۷] سرویس نیز با ترکیب دو رشته از موارد زیر ایجاد می‌شود:

- Boot
- Center
- Config
- Driver
- Helper
- Image
- Installer
- Manager
- Microsoft
- Monitor
- Network
- Security
- Server
- Shell
- Support
- System
- Task
- Time
- Universal
- Update
- Windows

۱ Hidden
۲ Random
۳ String
۴ Hash
۵ Registry
۶ Boot
۷ Display Name

Conficker به‌نحوی تنظیمات سیستم را تغییر می‌دهد که کاربر عادی قادر به مشاهده فایل‌های مخفی نباشد. این تغییر با تخصیص "0" به کلید CheckedValue در مسیر زیر صورت می‌پذیرد:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL

همچنین با تخصیص "0x00FFFFFE" – معادل ۱۶,۷۷۷,۲۱۴ – به کلید TcpNumConnections، برقراری تعداد زیادی ارتباط همزمان TCP را از روی دستگاه آلوده شده ممکن می‌کند:

- HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

از آنجا که اعمال تغییرات جدید مستلزم راه‌اندازی شدن مجدد سرویس TCP/IP است، Conficker از فایلی موقت برای این منظور بهره می‌گیرد.

این بدافزار با اجرای فرمان زیر قابلیت TCP/IP Auto-tuning را در سیستم عامل Vista غیرفعال می‌کند:

- netsh interface tcp set global autotuning=disabled

Conficker سرویس‌های بااهمیتی از جمله موارد زیر را متوقف می‌کند:

- Windows Security Center Service که وظیفه آن آگاهی‌رسانی به کاربر در خصوص تنظیمات امنیتی – در بخش‌هایی همچون Firewall، Windows Update و AntiVirus – است.
- Windows Update Auto Update Service که به‌روزرسانی خودکار سیستم عامل را فراهم می‌کند.
- Background Intelligence Transfer Service که توسط بخش Windows Update برای دریافت به‌روزرسانی‌ها در زمان اشغال نبودن پهنای باند مورد استفاده قرار می‌گیرد.
- Windows Defender که در نقش ضدویروس فعالیت می‌کند.
- Error Reporting Service و Windows Error Reporting Service که خطاها را استخراج و گزارش آنها را ارسال می‌کنند.

Conficker اقدام به حذف کلید Windows Defender در مسیر زیر در محضرخانه کرده و در عمل موجب عدم اجرای آن در زمان راه‌اندازی شدن سیستم می شود:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

همچنین هر پروسه‌ای را که در نام ماژول آن یکی از رشته‌های زیر وجود داشته باشد از تبادل داده در بستر شبکه منع می‌کند.

- ahnlab
- arcabit
- avast
- avira
- castlecops
- centralcommand
- clamav
- comodo
- PCassociates
- cpsecure
- defender
- drweb
- emsisoft
- esafe
- eset
- etrust
- ewido
- f-prot
- f-secure
- fortinet
- gdata
- grisoft
- hacksoft
- hauri
- ikarus
- jotti
- k7computing
- kaspersky
- malware
- mcafee
- microsoft
- networkassociates
- nod32
- norman
- norton
- panda
- pctools
- prevx
- quickheal
- rising
- rootkit
- securecomputing
- sophos
- spamhaus
- spyware
- sunbelt
- symantec
- threatexpert
- trendmicro
- virus
- wilderssecurity
- windowsupdate

اکثر این رشته‌ها در نامگذاری محصولات ضدویروس و نرم‌افزارهای امنیتی مورد استفاده قرار گرفته‌اند و بنابراین با این روش به‌نحوی مؤثر از به‌روز شدن آنها جلوگیری می‌شود.

از دیگر خرابکاری‌های این بدافزار دست‌درازی به تنظیمات System Restore، با هدف ناتوان کردن کاربر در بازگرداندن دستگاه آلوده به حالت قبل است.

Conficker با در اختیار گرفتن کنترل DNSAPI.DLL دسترسی کاربر به سایت‌هایی که در نشانی آنها از یکی از کلمات زیر استفاده شده مسدود می‌کند:

- activescan
- adware
- agnitum
- ahnlab
- anti-
- antivir
- arcabit
- avast
- avgate
- avira
- av-sc
- bdtools
- bothunter
- castlecops
- ccollomb
- centralcommand
- clamav
- comodo
- computerassociates
- conficker
- cpsecure
- cyber-ta
- defender
- downad
- drweb
- dslreports
- emsisoft
- esafe
- eset
- etrust
- ewido
- fortinet
- f-prot
- freeav
- free-av
- f-secure
- gdata
- grisoft
- hackerwatch
- hacksoft
- hauri
- ikarus
- jotti
- k7computing
- kaspersky
- kido
- malware
- mcafee
- microsoft
- mirage
- mitre
- msftncsi
- ms-mvp
- msmvps
- mtc.sri
- networkassociates
- nod32
- norman
- norton
- onecare
- panda
- pctools
- precisesecurity
- prevx
- ptsecurity
- quickheal
- removal
- rising
- rootkit
- safety.live
- securecomputing
- secureworks
- sophos
- spamhaus
- spyware
- sunbelt
- symantec
- technet
- threat
- threatexpert
- trendmicro
- trojan
- virscan
- virus
- wilderssecurity
- windowsupdate

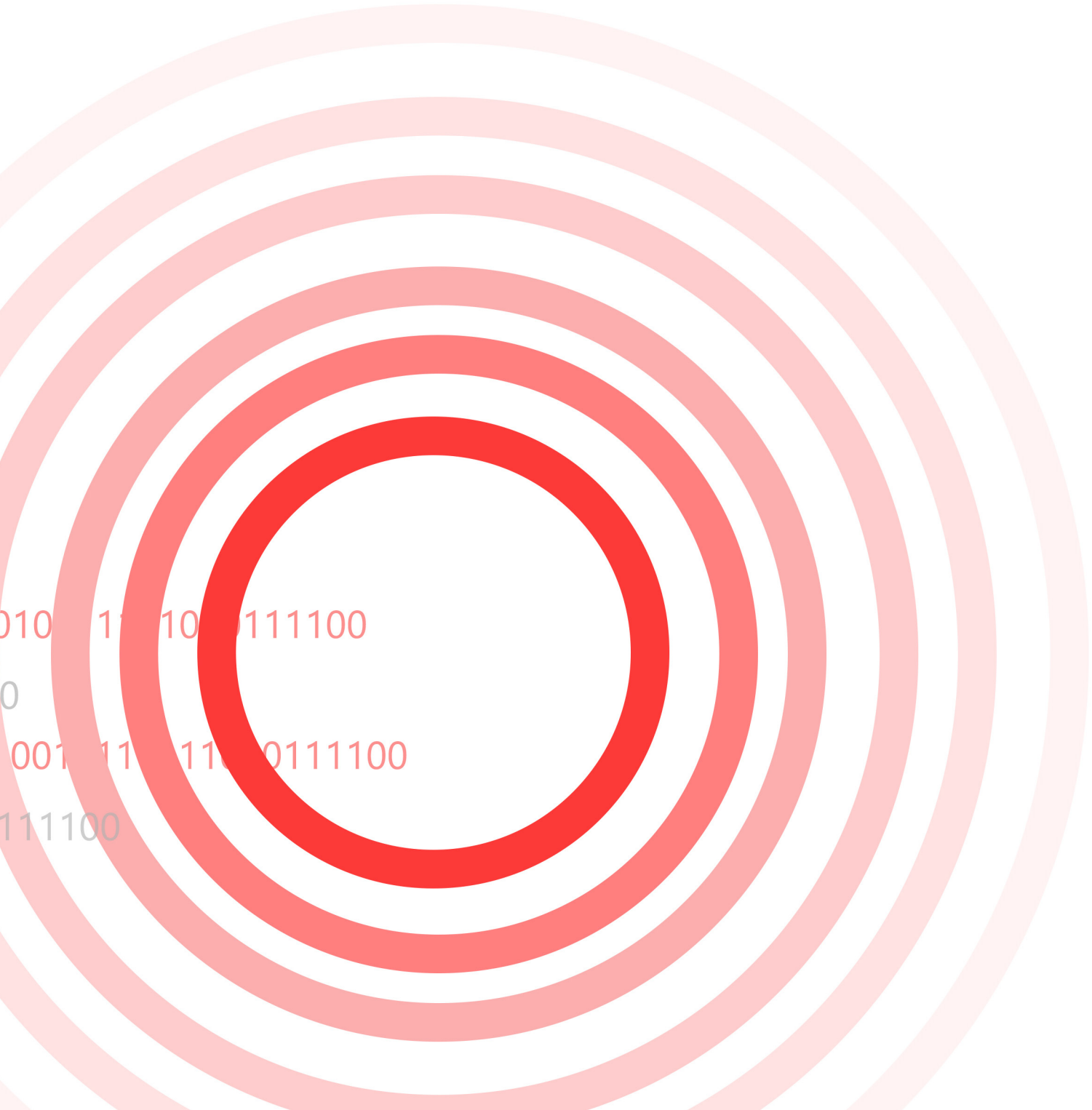
همچنین در صورتی که نشانی سایت فراخوانی شده شامل یکی از رشته‌های زیر باشد به کاربر خطای Time-out داده می‌شود:

- avg.
- avp.
- bit9.
- ca.
- cert.
- gmer.
- kav.
- llnw.
- llnwd.
- msdn.
- msft.
- nai.
- sans.
- vet.

بدافزار هر یک ثانیه یک بار فهرستی از پروسه‌های اجرا شده را استخراج کرده و در صورت وجود یکی از رشته‌های زیر در عنوان هر یک از آنها نسبت به متوقف نمودنشان اقدام می‌کند:

- autoruns
- avenger
- bd_rem
- cfremo
- confick
- downad
- dwndp
- filemon
- gmer
- hotfix
- kb890
- kb958
- kido
- kill
- klwk
- mbsa.
- mrt.
- mrtstub
- ms08
- ms09
- procexp
- procmon
- regmon
- scct_
- stinger
- sysclean
- tcpview
- unlocker
- wireshark

انتشار



Conficker از چندین روش برای انتشار خود در سطح شبکه بهره می‌گیرد که در ادامه به آنها پرداخته شده است.

سوءاستفاده از ضعف امنیتی

بارزترین روش انتشار Conficker بهره‌جویی آن از یک آسیب‌پذیری امنیتی در سرویس Server سیستم‌های عامل زیر است:

- Windows 2000
- Windows XP
- Windows Vista
- Windows Server 2003
- Windows Server 2008 (Core Installation)

سوءاستفاده از ضعف امنیتی مذکور مهاجم را قادر می‌کند تا با ارسال یک بسته RPC دستکاری شده به دستگاه آسیب‌پذیر، کد مخرب مورد نظر خود را به بدون نیاز به هر گونه دخالت کاربر به صورت از راه دور[1] به اجرا در آورد.

بدین‌منظور، Conficker در دستگاه آلوده شده اقدام به راه‌اندازی یک سرور HTTP بر روی درگاهی در بازه ۱۰۲۴ تا ۱۰۰۰۰ می‌کند. سپس با ارسال یک درخواست RPC دستکاری شده، منجر به بروز خطای سرریز حافظه[2] و در ادامه اجرای کد مخرب خود بر روی دستگاه‌های آسیب‌پذیر هدف قرار گرفته شده در دامنه دستگاه آلوده می‌شود.

کد مخرب پس از اجرا با سرور HTTP دستگاه مبدا ارتباط برقرار کرده و رونوشتی از ویروس را در قالب فایل DLL دریافت می‌کند. فایل مذکور نیز خود را به یکی از سرویس‌های اجرا شده توسط Service Host (فایل svchost.exe) یا Windows Explorer متصل می‌کند. روشی که موجب مورد اعتماد تلقی شدن فایل توسط برخی از محصولات ضدویروس می‌شود.

به‌منظور شناسایی دستگاه‌های در محدوده سیستم آلوده، Conficker از NetBIOS بهره می‌گیرد.

مایکروسافت آسیب‌پذیری مورد بهره‌جویی Conficker را در اصلاحیه MS08-067 که در ۲ آبان ۱۳۸۷ عرضه شد برطرف کرد.

پوشه‌های اشتراکی و حافظه‌های جداشدنی

از نسخه B، انتشار از طریق پوشه‌های اشتراکی نیز به قابلیت‌های Conficker افزوده شد.

Conficker پس از شناسایی یک دستگاه در محدوده شبکه‌ای دستگاه آلوده شده، تلاش می‌کند تا رونوشتی از خود را با استفاده از اطلاعات اصالت‌سنجی[3] کاربر جاری در پوشه اشتراکی مخفی ADMIN$ آن دستگاه کپی کند.

[1] Remotely
[2] Buffer Overflow
[3] Credential

در صورت عدم دسترسی کاربر جاری به پوشه مذکور، فهرستی از نام‌های کاربری دستگاه مقصد استخراج شده و در ادامه یک حمله موسوم به لغت‌نامه با هر یک از آن نام‌های کاربری و فهرستی از رمزهای عبور زیر به اجرا در می‌آید:

- 00000000
- 0000000
- 00000
- 0000
- 000
- 00
- 987654321
- 0
- 11111111
- 1111111
- 111111
- 11111
- 1111
- 111
- 11
- 123123
- 12321
- 123321
- 1234567890
- 123456789
- 12345678
- 1234567
- 123456
- 12345
- 1234
- 1234abcd
- 1234qwer
- 123
- 123abc
- 123asd
- 123qwe
- 12
- 1
- 1q2w3e
- 21
- 22222222
- 2222222
- 222222
- 22222
- 2222
- 222
- 22
- 2
- 321
- 33333333
- 3333333
- 333333
- 33333
- 3333
- 333
- 33
- 3
- 4321
- 44444444
- 4444444
- 444444
- 44444
- 4444
- 444
- 44
- 4
- 54321
- 55555555
- 5555555
- 555555
- 55555
- 5555
- 555
- 55
- 5
- 654321
- 66666666
- 6666666
- 666666
- 66666
- 6666
- 666
- 66
- 6
- 7654321
- 77777777
- 7777777
- 777777
- 77777
- 7777
- 777
- 77
- 7
- 87654321
- 88888888
- 8888888
- 888888
- 88888
- 8888
- 888
- 88
- 8
- 987654321
- 99999999
- 9999999
- 999999
- 99999
- 9999
- 999
- 99
- 9
- a1b2c3
- aaa
- aaaa
- aaaaa
- abc123
- academia
- access
- account
- admin123
- admin12
- admin1
- Admin
- adminadmin
- administrator
- anything
- asddsa
- asdfgh

- asdsa
- asdzxc
- backup
- boss123
- business
- campus
- changeme
- cluster
- codename
- codeword
- coffee
- PC
- controller
- cookie
- customer
- database
- default
- desktop
- domain
- example
- exchange
- explorer
- file
- files
- foo
- foobar
- foofoo
- forever
- freedom
- fuck
- games
- home123
- home
- ihavenopass
- Internet
- intranet
- job
- killer
- letitbe
- letmein
- Login
- lotus
- love123
- manager
- market
- money
- monitor
- mypass
- mypassword
- mypc123
- nimda
- nobody
- nopass
- nopassword
- nothing
- office
- oracle
- owner
- pass123
- pass12
- pass1
- pass
- passwd
- password123
- password12
- password1
- Password
- private
- public
- pw123
- q1w2e3
- qazwsx
- qazwsxedc
- qqq
- qqqq
- qqqqq
- qwe123
- qweasd
- qweasdzxc
- qweewq
- qwerty
- qwewq
- root123
- root
- rootroot
- sample
- secret
- secure
- security
- server
- shadow
- share
- sql
- student
- super
- superuser
- supervisor
- system
- temp123
- temp
- temporary
- temptemp
- test123
- test
- testtest
- unknown
- web
- windows
- work123
- work
- xxx
- xxxx
- xxxxx
- zxccxz
- zxcvb
- zxcvbn
- zxcxz
- zzz
- zzzz
- zzzzz

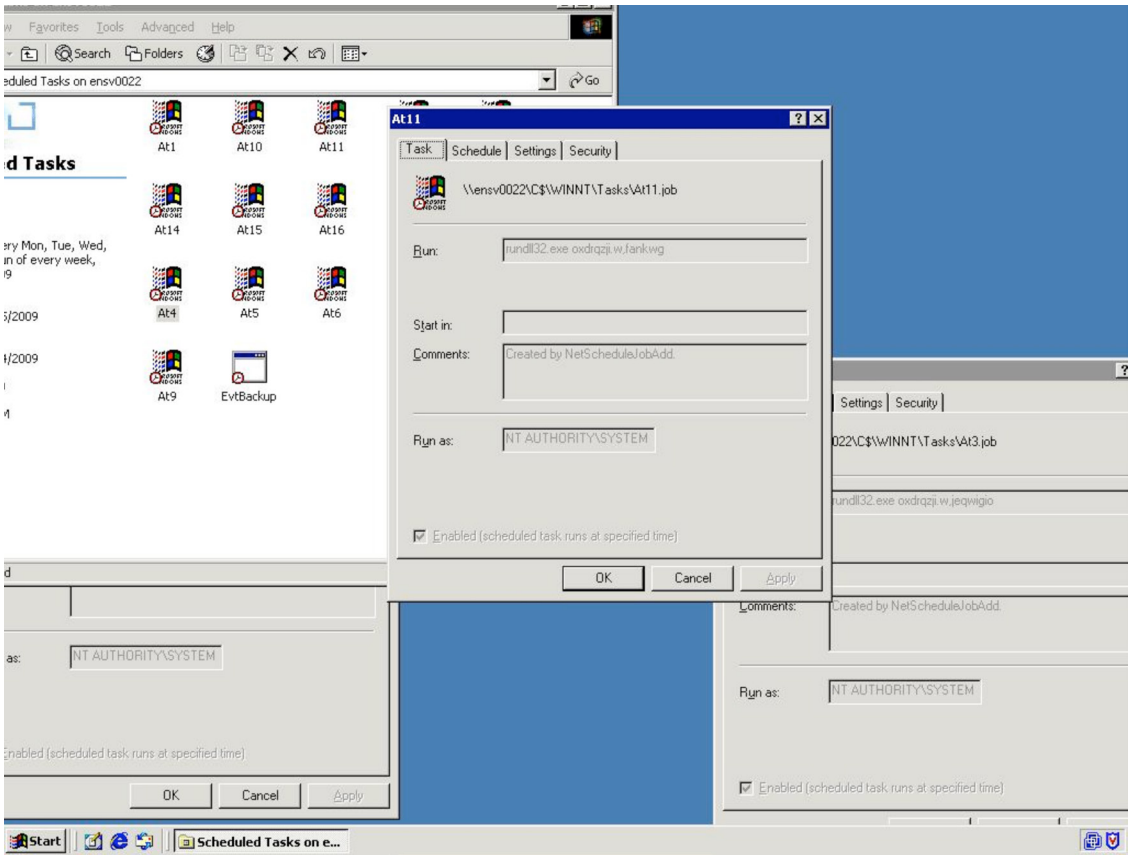
در صورتی که بر روی تنظیمات دستگاه / دامنه[1] سیاست Account Lockout فعال شده باشد اجرای حمله لغت‌نامه‌ای ممکن است منجر به غیرفعال شدن حساب کاربری شود.

با فراهم شدن دسترسی با هر یک از روش‌های فوق، فایل بدافزار با پسوند DLL در مسیر زیر بر روی دستگاه مقصد کپی می‌شود.

- %WinDir%\System32\

در ادامه به‌صورت از راه دور یک فرمان زمانبندی شده[2] در قالب زیر تعریف می‌شود:

- rundll32.exe <malware file name>.dll,<malware parameters>



فرامین ایجاد شده توسط Conficker در بخش Scheduled Tasks

[1] Domain
[2] Scheduled Task

همچنین Conficker رونوشتی از خود را نیز با الگوی زیر – که در آن %d به نویسه‌ای تصادفی اشاره دارد – بر روی تمامی درایوهای موسوم به Map Drive و حافظه‌های جداشدنی متصل به دستگاه کپی می‌کند:

- <drive:>\RECYCLER\S-%d-%d-%d-%d%d%d-%d%d%d-%d%d%d-%d\<random letters>.dll

در ریشه این درایوها یک فایل autorun.inf که در آن به مسیر و فایل بدافزار اشاره شده کپی می‌شود. در نسخه‌های قدیمی Windows، هر زمان که یکی از این درایوها توسط کاربر مورد دسترسی قرار می‌گیرد، autorun.inf فایل اشاره شده در خود را به‌طور خودکار بر روی دستگاه اجرا می‌نماید.

مکانیزم به‌روزرسانی

بدافزار دسترسی داشتن دستگاه آلوده به اینترنت را با اتصال به سایت‌های زیر مورد بررسی قرار می‌دهد:

- aol.com
- cnn.com
- ebay.com

نسخه A این بدافزار در هر روز از طریق پنج دامنه سطح بالا[1]، ۲۵۰ نشانی دامنه جدید ایجاد می‌کرد. در نامگذاری از یک مولد اعداد شبه تصادفی[2]، با ورودی تاریخ روز جاری استفاده می‌شد. بنابراین فهرست ایجاد شده تمامی نمونه‌های بدافزار کاملا یکسان با یکدیگر می‌بود.

Conficker از سایت‌های زیر برای بررسی تاریخ فعلی بهره می‌گیرد:

- adobe.com
- answers.com
- baidu.com
- bbc.co.uk
- comcast.net
- disney.go.com
- ebay.co.uk
- facebook.com
- imdb.com
- megaporn.com
- miniclip.com
- rapidshare.com
- torrentz.com

```
[c:\]netcat youtube.com 80
GET / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Tue, 31 Mar 2009 10:57:06 GMT
Server: Apache
Content-Length: 291
nnCoection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache Server at www.youtube.com Port 80</address>
</body></html>
```

استخراج تاریخ با اتصال به سایتی اینترنتی با استفاده از فرامینی همچون netcat و telent

در ادامه تلاش می‌کند تا با برقراری یک ارتباط HTTP به هر نام دامنه، کد مخرب امضا شده[3] جدید Conficker را دریافت کند.

در نسخه B، تعداد دامنه‌های سطح بالا که Conficker برای ایجاد نشانی‌های دامنه از آنها بهره‌جویی می‌کرد از پنج به هشت افزایش پیدا کرد.

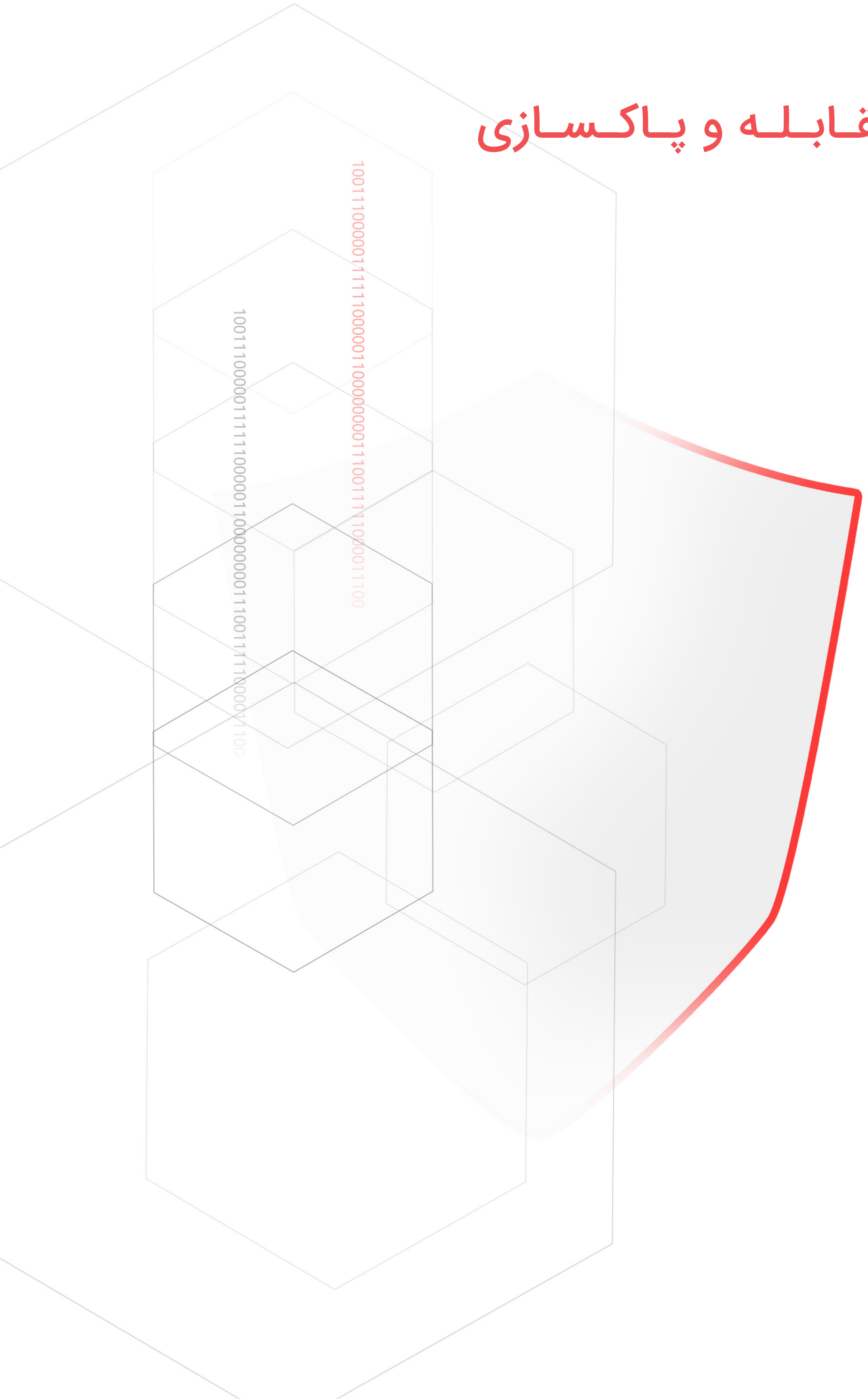
نسخه C مجهز به قابلیتی شد که دستگاه متصل به اینترنت با روش خروج به ترتیب ورود[4] نشانی‌های URL را به سایر ماشین‌های آلوده در سطح شبکه داخلی اطلاع‌رسانی می‌کرد.

در نسخه D ضمن افزایش تعداد دامنه‌های سطح بالا به ۱۱۰، از پودمانی سفارشی مبتنی بر UDP برای شناسایی دستگاه‌های آلوده شده در سطح شبکه و سپس انتقال نسخه جدید به آنها از طریق TCP استفاده می‌شد. این مکانیزم شناسایی و انتقال در نسخه E نیز ادامه پیدا کرد.

در فاصله اسفند ۱۳۸۷ تا فروردین ۱۳۸۸ در اقدامی مشترک و هماهنگ میان مراکز دامنه سطح بالا، تمامی نام‌های دامنه مورد استفاده Conficker مسدود و به‌روزرسانی این بدافزار برای همیشه متوقف شد.

[1] Top-level Domain (TLD)
[2] Pseudorandom Number Generator (PRNG)
[3] Signed Payload
[4] FIFO

مـقـابـلـه و پـاکـسـازی



از جمله نشانه‌های آلودگی یک دستگاه به این بدافزار می‌توان به موارد زیر اشاره کرد:

- غیرفعال شدن حساب‌های کاربری
- ترافیک بالای شبکه‌ای به خصوص بر روی درگاه ٤٤٥
- ایجاد فایل Autorun در ریشه حافظه‌های شدنی و درایوهای Map شده
- متوقف شدن سرویس‌های اشاره شده در این گزارش
- عدم دسترسی به سایت‌های امنیتی
- اجرا نشدن محصولات و ابزارهای امنیتی

اصلی‌ترین راهکار نیز در مقابله با این بدافزار رعایت تمامی موارد زیر است:

- نصب اصلاحیه‌های MS08-067، MS08-068 و MS09-001
- استفاده از رمزهای عبور پیچیده برای تمامی کاربران از جمله کاربران با سطح دسترسی Administrator
- حتی الامکان از ورود[1] به دستگاه با نام کاربری با سطح دسترسی Administrator در سطح دامنه / گروه کاری[2] خودداری شود. ورود چنین کاربری به یکی از دستگاه‌های آلوده شده موجب توزیع بدافزار در سرتاسر شبکه خواهد شد.
- استفاده از ضدویروس قدرتمند و به‌روز
- بکارگیری محصولات موسوم به Device Control بر روی تمامی دستگاه‌ها
- محدودسازی دسترسی به پوشه‌های اشتراکی
- غیرفعال کردن قابلیت Autoplay در نسخه‌های قدیمی سیستم عامل Windows با مراجعه به راهنمای زیر:
https://support.microsoft.com/en-us/help/967715/how-to-disable-the-autorun-functionality-in-windows

به‌منظور پاکسازی دستگاه آلوده شده به Conficker استفاده از ابزار McAfee CleanBoot توصیه می‌شود.

[1] Login
[2] Workgroup

فهرست منابع

- https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/60000/KB60909/en_US/Combatting_W32_Conficker_worm.pdf
- https://support.microsoft.com/en-us/help/962007/virus-alert-about-the-win32-conficker-worm
- https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm%3aWin32%2f-Conficker.A
- https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm%3aWin32%2f-Conficker.B
- https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm%3aWin32%2f-Conficker.C
- https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm%3aWin32%2f-Conficker.D
- https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm%3aWin32%2f-Conficker.E
- https://community.sophos.com/kb/en-us/51169
- https://support.eset.com/kb2209/?locale=en_US&viewlocale=en_US
- https://www.pandasecurity.com/en/security-info/204292/information/Conficker.C
- https://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml
- https://www.blackhat.com/presentations/bh-usa-09/HYPPONEN/BHUSA09-Hypponen-ConfickerMystery-PAPER.pdf
- https://newsroom.shabakeh.net/9258
- https://newsroom.shabakeh.net/6975
- https://newsroom.shabakeh.net/6838
- https://newsroom.shabakeh.net/3740
- https://www.bbc.com/news/technology-44564709
- http://edition.cnn.com/2009/TECH/ptech/02/13/virus.downadup/index.html


آخرین اخبار امنیت فناوری اطلاعات
@SGnewsroom

شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

ISO 9001:2008
Cert No 9150.C528

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار	۰۲۱-۴۲۰۵۲
رایانامه	info@shabakeh.net
تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net