EXHIBIT 5

Microsoft

Malware Protection Center

Account

Sign in

Search Malware Protection Center

Search Microsoft.com

Search the Web

Win32/Dorkbot

Microsoft security software detects and removes this threat.

This family of worms can steal your user names and passwords by watching what you do online. They can also download other malware and stop you from visiting security-related websites. Some variants can use your PC in a denial of service (DoS) attack.

They spread via infected USB flash drives, or in a malicious link sent though instant messaging programs and social networks.

Find out ways that malware can get on your PC.

What to do now

Use the following free Microsoft software to detect and remove this threat:

Windows Defender for Windows 10 and Windows 8.1, or Microsoft Security Essentials for Windows 7 and Windows Vista
Microsoft Safety Scanner
Microsoft Windows Malicious Software Removal Tool
You should also run a full scan. A full scan might find other, hidden malware.

Protect your sensitive information

This threat tries to steal your sensitive and confidential information. If you think your information has been stolen, see:

What to do if you are a victim of fraud
You should change your passwords after you've removed this threat:

Create strong passwords

Scan removable drives

Remember to scan any removable or portable drives. If you have Microsoft security software, see this topic on our software help page:

How do I scan a removable drive, such as a USB flash drive?

Disable Autorun

This threat tries to use the Windows Autorun function to spread via removable drives, like USB flash drives. You can disable Autorun to prevent worms from spreading:

Disable Windows Autorun

Get more help

You can also visit our advanced troubleshooting page or search the Microsoft virus and malware community for more help.

If you're using Windows XP, see our Windows XP end of support page.

Top

Threat behavior

Installation

Win32/Dorkbot variants usually arrive as a link in an instant message or social network message. The link points to a copy of the worm that can be downloaded and run on your PC. The worm might have any of the following file names:

facebook-profile-pic-<random number>-JPEG.exe
facebook-pic00<random number>.exe
skype_<DDMMYYYY>_foto.exe , where <DDMMYYYY> is the day, month, and year, for example, "*skype_06102012_foto.exe*"
skype_<DD-MM-YYYY>_foto.exe , where <DD-MM-YYYY> is the day, month, and year, for example, "*skype_09-10-2012_image.exe*"

When it runs, variants of Win32/Dorkbot might copy themselves to the %APPDATA% folder using a randomly-generated six letter file name, which is based on the HDD serial number, by calling the GetVolumeInformation() API (for example, "*ozkqke.exe*").

We have also seen variants install files in the following locations:

%APPDATA% \c731200
%APPDATA% \ScreenSaverPro.scr
%APPDATA% \temp.bin
%APPDATA% \update\explorer.exe
%APPDATA% \update\cleaner.exe
%APPDATA% \update\update.exe
%APPDATA% \windowsupdate\updater.exe
%APPDATA% \windowsupdate\live.exe
%APPDATA% \Windows Live\<random>.exe, for example *%APPDATA%\Windows Live\dkxjymgruw.exe*
%TEMP% \Adobe\Reader_sl.exe
%TEMP% \c731200
The worm changes the following registry entries to ensure that its copy runs each time you start your PC:

In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Run*
Sets value: "*<randomly generated six letter string>*", for example "*ozkqke*"
With data: "*%APPDATA%\<randomly generated six letter string>.exe*", for example "*%APPDATA%\ozkqke.exe*"

In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Run*
Sets value: "*Screen Saver Pro 3.1*"
With data: "*%APPDATA%\ScreenSaverPro.scr*"

In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Run*
Sets value: "*Adobe System Incorporated*"
With data: "*%TEMP%\Adobe\Reader_sl.exe*"

In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Run*
Sets value: "*Windows Update Installer*"
With data: *%APPDATA%\windowsupdate\updater.exe*

In subkey: *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon*
Sets value: "*Taskman*"
With data: *%APPDATA%\windowsupdate\updater.exe*

In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Run*
Sets value: "*Windows Explorer Manager*"
With data: *%APPDATA%\update\explorer.exe*

In subkey: *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon*
Sets value: "*Taskman*"
With data: *%APPDATA%\update\explorer.exe*

In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Run*
Sets value: "*Windows Live Installer*"
With data: *%APPDATA%\WindowsUpdate\Live.exe*

In subkey: *HKCU\Software\Microsoft\Windows\Currentversion\Policies\Explorer\Run*
Sets value: "*Windows Live*"
With data: *%APPDATA%\Windows Live\<random>.exe*

In subkey: *HKCU\Software\Microsoft\Windows\Currentversion\Run*
Sets value: "*Windows Live*"
With data: *%APPDATA%\Windows Live\<random>.exe*

Spreads via...

Removable drives

Win32/Dorkbot might create a folder named "*RECYCLER*" in all accessible USB drives, and registers it as a Recycle Bin folder. The worm registers a device notification so that it is notified whenever you plug a USB device into your PC. It then copies itself to the USB device, using a variable file name, and creates an Autorun configuration file named "*autorun.inf*" pointing to the worm copy. These autorun.inf files tell the operating system to launch the worm file automatically when the USB drive is accessed from another PC that supports the Autorun feature.

Instant messaging/Instant relay chat

Using backdoor functionality (see Payload - Allows backdoor access and control section below), the worm can be ordered by a remote hacker to spread via instant messaging platforms such as Windows Live Messenger, Pidgin chat, Xchat, mIRC, and Skype. It sends messages to all of your contacts. The messages sent, and the frequency at which the messages are sent are configured by the remote hacker.

Some Win32/Dorkbot variants can spread via Skype by first downloading and installing another malware component (see Payload - Downloads additional malware).

The malicious malware component uses the Skype APIs to send a malicious link to all the contacts at a specified time interval. The message that contains the malicious link might look like the following:

If your contact receives and visit the link, Win32/Dorkbot is downloaded into your PC.

The message might differ based on your current location and locale.

Social networks

Win32/Dorkbot variants can be ordered to spread via social network services such as Facebook, Twitter, Bebo, and Vkontakte (a Russian social network). Similar to instant messaging spreading, the worm will hijack the sent message and replace it with its own message that contains the link to the worm's copy. The number of messages sent before the worm will inject its own message with a malicious link is also configured by the remote hacker.

Payload

Allows backdoor access and control

Variants of Win32/Dorkbot might connect to an IRC server, join a channel and wait for commands. In the wild, we have observed the worm using IRC servers on the following domains for this purpose:

av.shannen.cc
lovealiy.com
shuwhyyu.com
syegyege.com
Using this backdoor, a remote hacker can perform certain actions.

The worm uses a user-mode rootkit to prevent you from viewing or tampering with its files. This is done by hooking the following functions for all processes inside which it is injected:

DeleteFileA/W
CopyFileA/W
NtEnumerateValueKey
NtQueryDirectoryFile
Injects code

When it runs, the worm injects code into "*explorer.exe*", as well as to many other running processes on your PC. It might do this to make itself more difficult to detect and remove.

Note that the number of processes it is capable of injecting into is dependent on whether it has been run with administrator privileges.

Contacts remote host

Win32/Dorkbot generates an IRC 'nickname' by connecting to *api.wipmania*, combining the country code, operating system version, user-type and a random string, using the following format:

n{<country code>|<OS version><user type>}<random string>

where:

Operating system version could be any of the following: XP, 2K3, VIS, 2K8, W7, ERR (Error)
Country code is a two digit country code (for example *US* - USA, *RU* - Russia, etc)
User-type is either '*a*' (administrator) or '*u*' (user)
Example 'nickname': *n{US|XPa}xkfnalw*

Using the generated 'nickname' and the IRC server information from its internal configuration, it connects to the IRC server to retrieve further data or infection parameters such as download link, Windows Live Messenger message, and domain lists among other information.

The worm can accept commands from the hacker to perform one or more of the following actions:

Download and run a file from specified URL
Delete the downloaded file the next time you restart your PC (a command called Ruskill; if the command is on, it deletes the file)
Update its main executable from specified URL and wait until next restart to run (or, if specified in the command, to restart immediately)
Uninstall itself
Try to remove other malware that spread via USB drives and that communicate to IRC servers (a command called PDef)
Collect log on information and passwords from form grabbing, FTP, POP3, Internet Explorer and Firefox cached login details
Block or redirects certain domains and websites
Access certain websites using Internet Explorer, without your knowledge
Show infection statistics
Launch and stop denial of service (SYN,UDP, or SlowLoris flood) attacks
Spread via USB, instant messaging, and social networks
Prepare a message via HTTP, instant messaging, or social networks to accompany a link to its copy, to be used to spread itself
Report back information about the bot
Display bot version information

If logging is enabled by the hacker, every command that it runs is logged and sent to the IRC server and displayed in the IRC channel where the bot is connected.

Downloads other malware

Because Dorkbot can download and run files, it has been used by other malware as a distributing mechanism for their malware. We have seen Dorkbot download and run the following malware:

Ransom:Win32/Crowti
TrojanClicker:Win32/Gingplog.A
Trojan:Win32/Fleercivet.D
Trojan:Win32/Lethic.I
Trojan:Win32/Mustrat.A
Trojan:Win32/Necurs
Trojan:Win32/Neurevt.A
TrojanDownloader:Win32/Cutwail
Worm:Win32/Gamarue.A
Worm:Win32/Kasidet.A

Deletes files

Win32/Dorkbot contains instructions to delete files it downloads and runs after reboot. It needs this feature to be turned on by the hacker. After installation, the worm deletes its initial dropper executable.

The worm uses "behavior monitoring" to identify and delete files that appear to communicate via Internet Relay Chat (IRC) or exhibit worm behavior such as spreading via removable drives or USB media.

Overwrites files

The worm can be instructed to overwrite the following files in order to hinder malware diagnosis and removal:

regsvr32.exe
cmd.exe
rundll32.exe
regedit.exe
verclsid.exe
ipconfig.exe

Steals sensitive information

Win32/Dorkbot is capable of intercepting Internet browser communications with various websites, and obtaining sensitive information. This is done by hooking various APIs within Firefox and Internet Explorer. The worm can also target FTP credentials.

Win32/Dorkbot variants target the following websites from which to steal user names and passwords:

4shared
Alertpay
AOL
Bcointernacional
BigString
Brazzers
Depositfiles
DynDNS
eBay
Facebook
Fastmail
Fileserve
Filesonic
Freakshare
Gmail
GMX
Godaddy
Hackforums
Hotfile
IKnowThatGirl
Letitbit
LogMeIn
Mediafire
Megaupload
Moneybookers
Moniker
Namecheap
Netflix
Netload
NoIP
OfficeBanking
Oron
PayPal
Runescape
Sendspace
Sms4file
Speedyshare
Steam

Thepiratebay
Torrentleech
Twitter
Uploaded
Uploading
Vip-file
Whatcd
Yahoo
YouPorn
YouTube

Infects websites

The worm might be ordered to log into a remote FTP server and infect various HTML files by adding an IFrame. This action may facilitate the worm's spreading function.

Blocks access to security websites

Variants of the worm may be ordered to block user access to sites with the following strings in their domain:

avast
avg
avira
bitdefender
bullguard
clamav
comodo
emsisoft
eset
fortinet
f-secure
garyshood
gdatasoftware
heck.tc
iseclab
jotti
kaspersky
lavasoft
malwarebytes
mcafee
onecare.live
norman
norton

novirusthank
onlinemalwarescanner
pandasecurity
precisesecurity
sophos
sunbeltsoftware
symante
threatexpert
trendmicro
virscan
virus
virusbuster
nprotect
viruschief
virustotal
webroot

The worm may also download an additional or updated domain list from a remote website.

Hooks APIs

Win32/Dorkbot hooks several APIs for various purposes, such as hiding its components (like registry entries and dropped file and process names), spreading and sniffing user names and passwords. Some examples that we have observed Win32/Dorkbot hooking in the wild are:

CopyFileA/W
CreateFileA/W
DeleteFileA/W
DnsQuery_A/W
GetAddrInfoW
HttpSendRequestA/W
InternetWriteFile
LdrLoadDll
MoveFileA/W
NtEnumerateValueKey
NtQueryDirectoryFile
NtResumeThread
PR_Write
RegCreateKeyExA/W
send
URLDownloadToFileA/W

Additional information

When it runs, it performs a self-integrity check. If it fails, it shows the message box below and attempts to corrupt the hard drive by writing garbage data to the hard drive.

It also creates a mutex to avoid multiple instances of itself, and mark its presence. Most variants use "hex-Mutex", but others have been observed using random mutexes such as "t2f-Mutex" and"f4448e25-Mutex".

Additional resources

Analysis of a Dorkbot infection Part 1, Part 2 [MMPC]
Dorkbot: Hunting Zombies in Latin America [Eset]
Ransomware Worm Spreading Via Skype [Forbes]
Dorkbot worm spreading via Skype, installs nasty ransomware [Techspot]
Analysis by Rex Plantado

Symptoms

The following could indicate that you have this threat on your PC:

- You have these files:

  facebook-profile-pic-<random number>*-JPEG.exe*
  facebook-pic00<random number>*.exe*
  %APPDATA%\c731200
  %APPDATA%\ScreenSaverPro.scr
  %APPDATA%\temp.bin
  %APPDATA%\update\explorer.exe
  %APPDATA%\update\cleaner.exe
  %APPDATA%\update\update.exe
  %APPDATA%\windowsupdate\updater.exe
  %APPDATA%\windowsupdate\live.exe
  %APPDATA%\Windows Live\<random>.exe, for example %APPDATA%\Windows Live\dkxjymgruw.exe
  %TEMP%\Adobe\Reader_sl.exe

%TEMP%\c731200

- You see the following message:

Prevention

Take these steps to help prevent infection on your PC.

Top

I want to...

- Get help

Remove difficult malware
Avoid tech support phone scams
See and search the latest threats
Find answers to other problems

- Fix my software
- Download and update
- Submit a file

Alert level: Severe
This entry was first published on: Jun 15, 2011
This entry was updated on: Jul 07, 2015

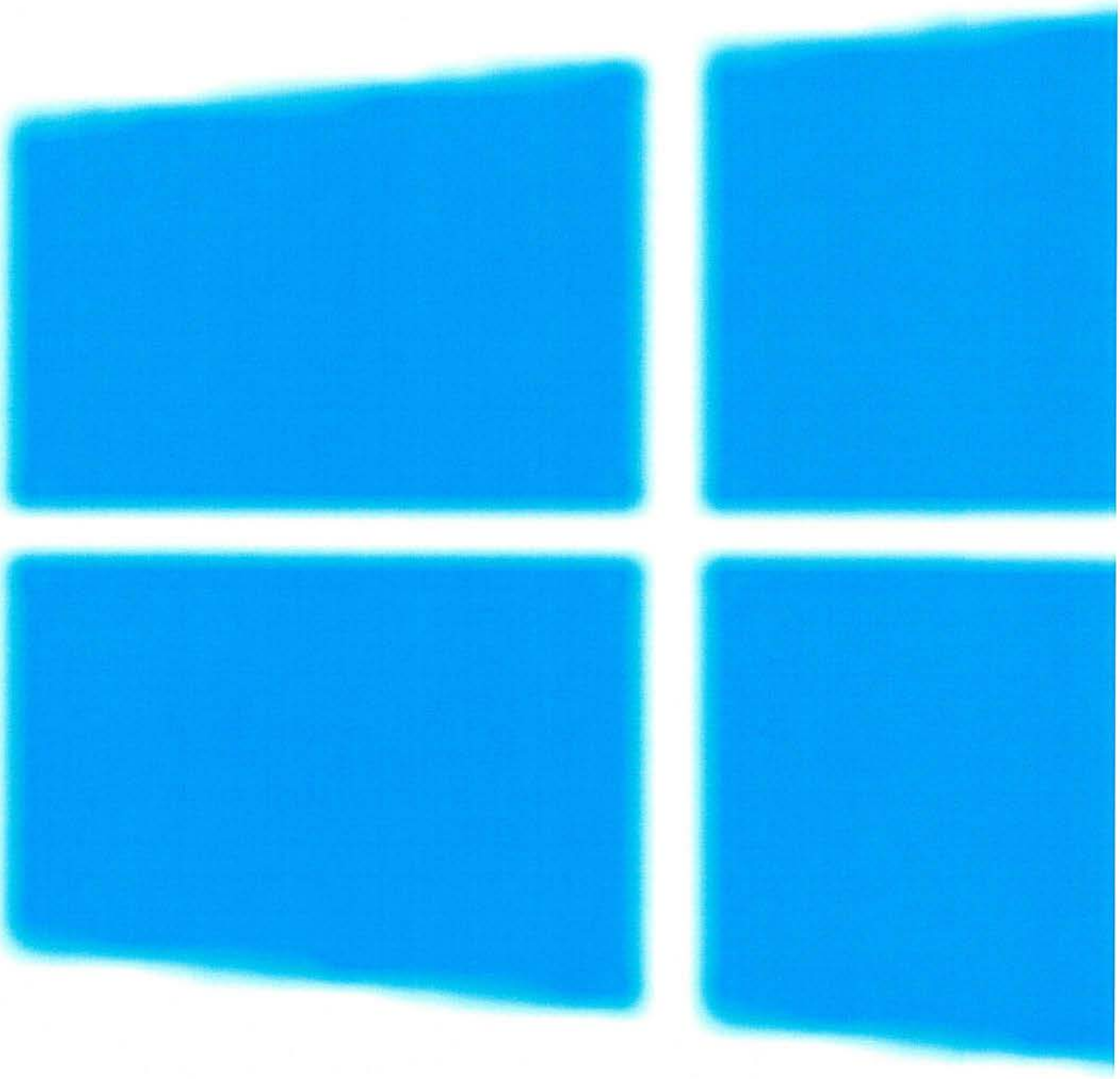
This threat is also detected as:

- Win-Trojan/Injector.636416.D (AhnLab)
- W32/Dorkbot.B.gen!Eldorado (Command)
- Trojan.Injector!mcxcCCeftrA (VirusBuster)
- W32.IRCBot.NG (Symantec)

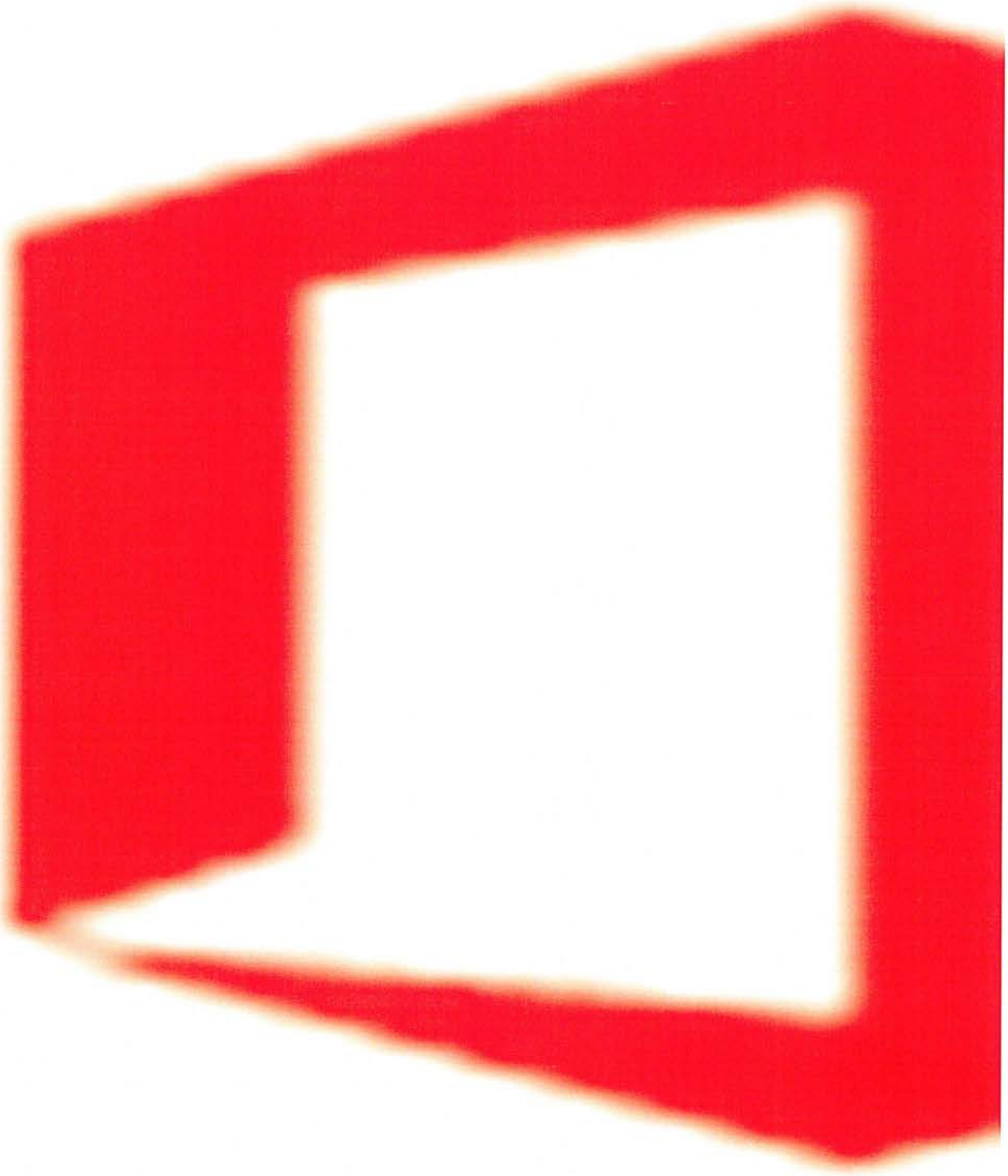
- WORM_DORKBOT.QUN (Trend Micro)
- ngrBot (other)

Provide feedback

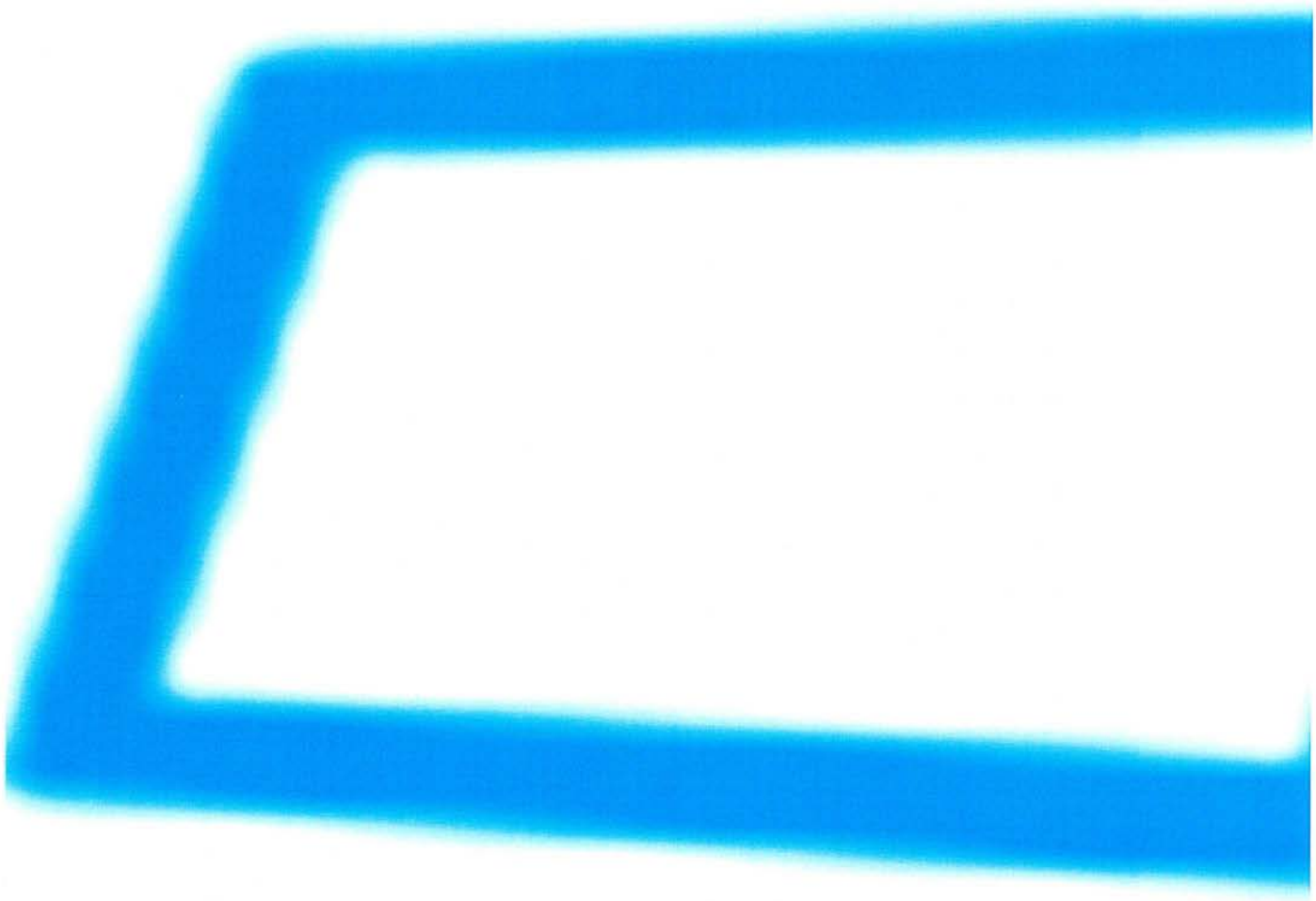
- Other Microsoft sites



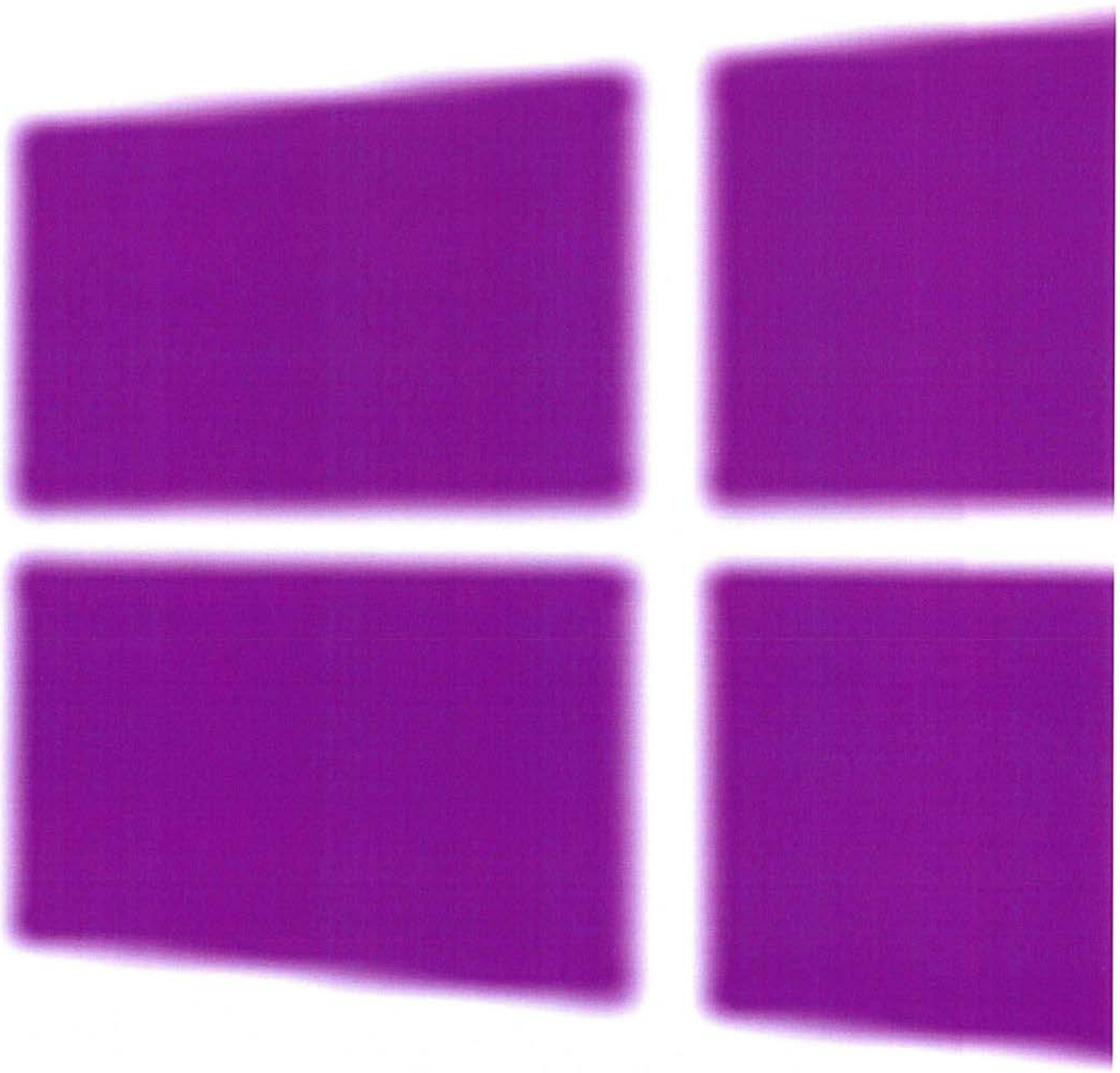
Windows



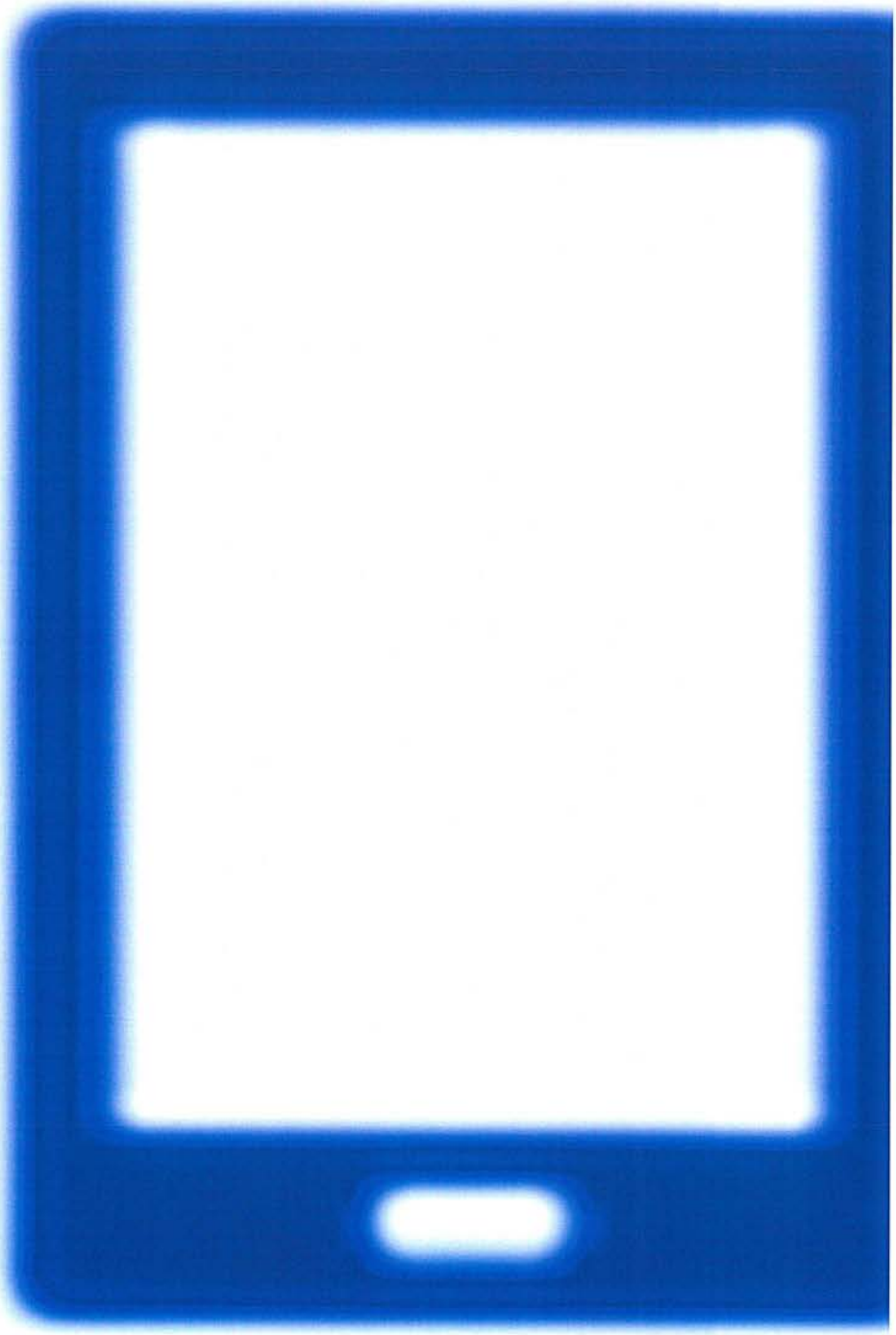
Office



Surface



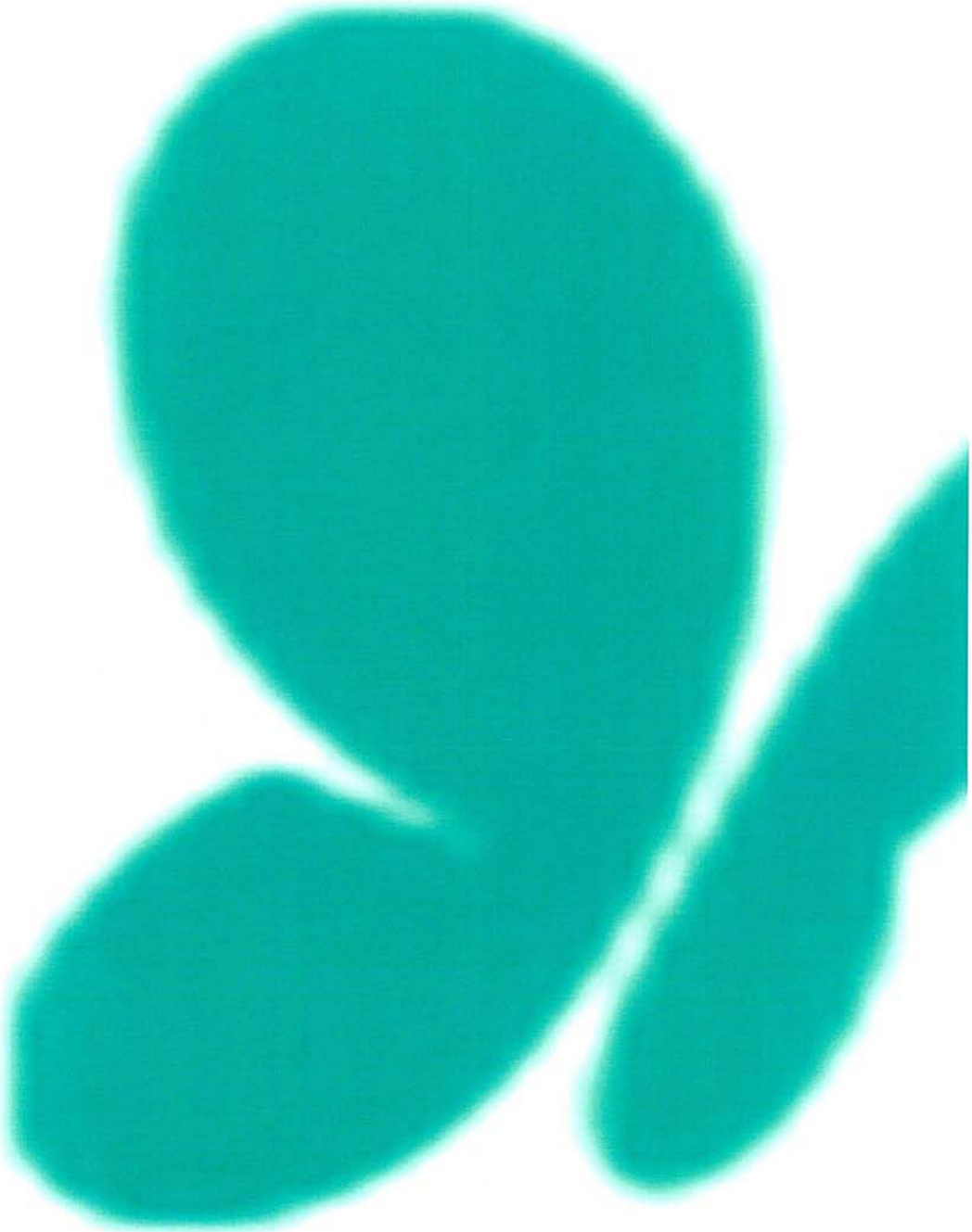
Windows Phone



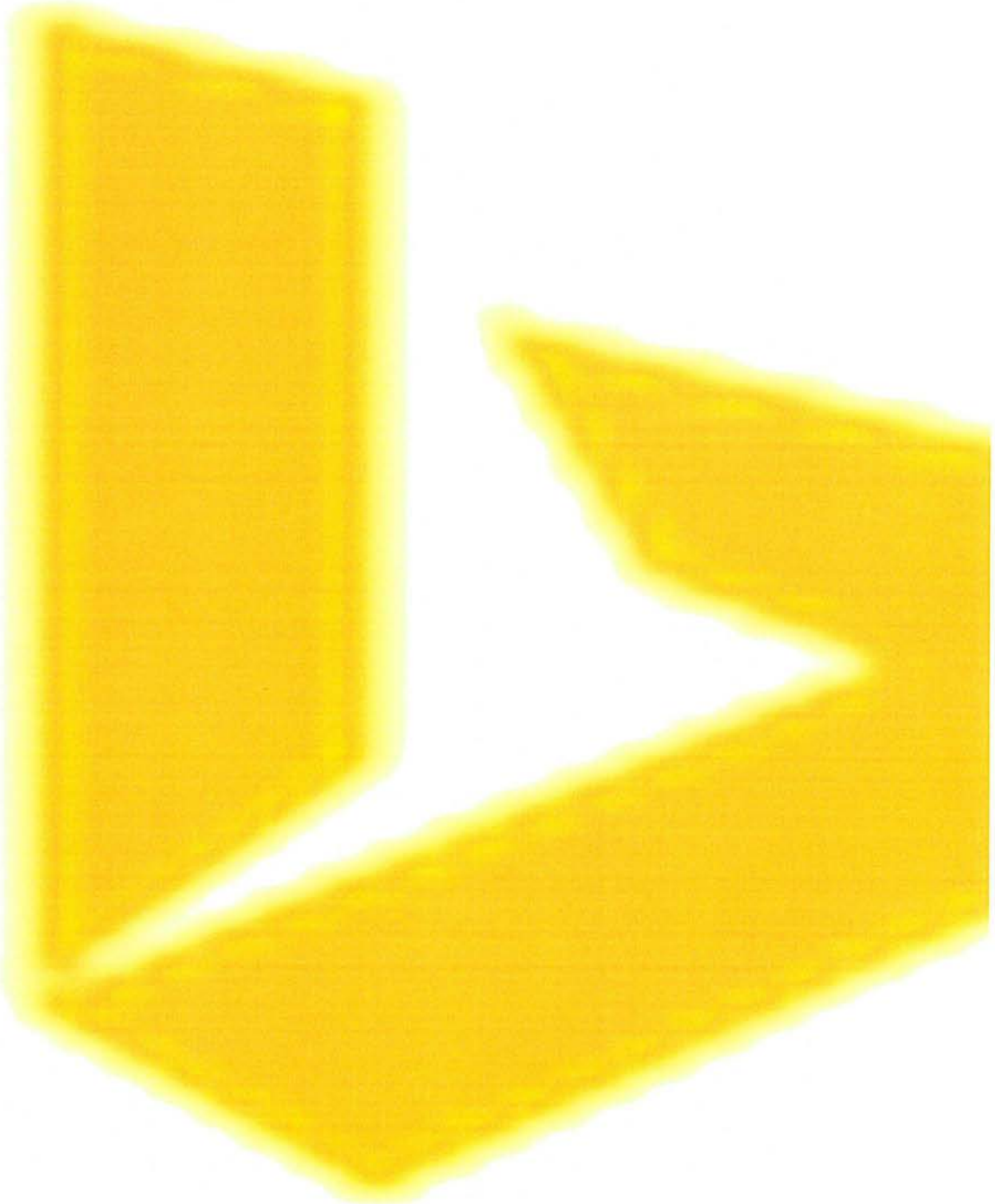
- Mobile devices

Xbox

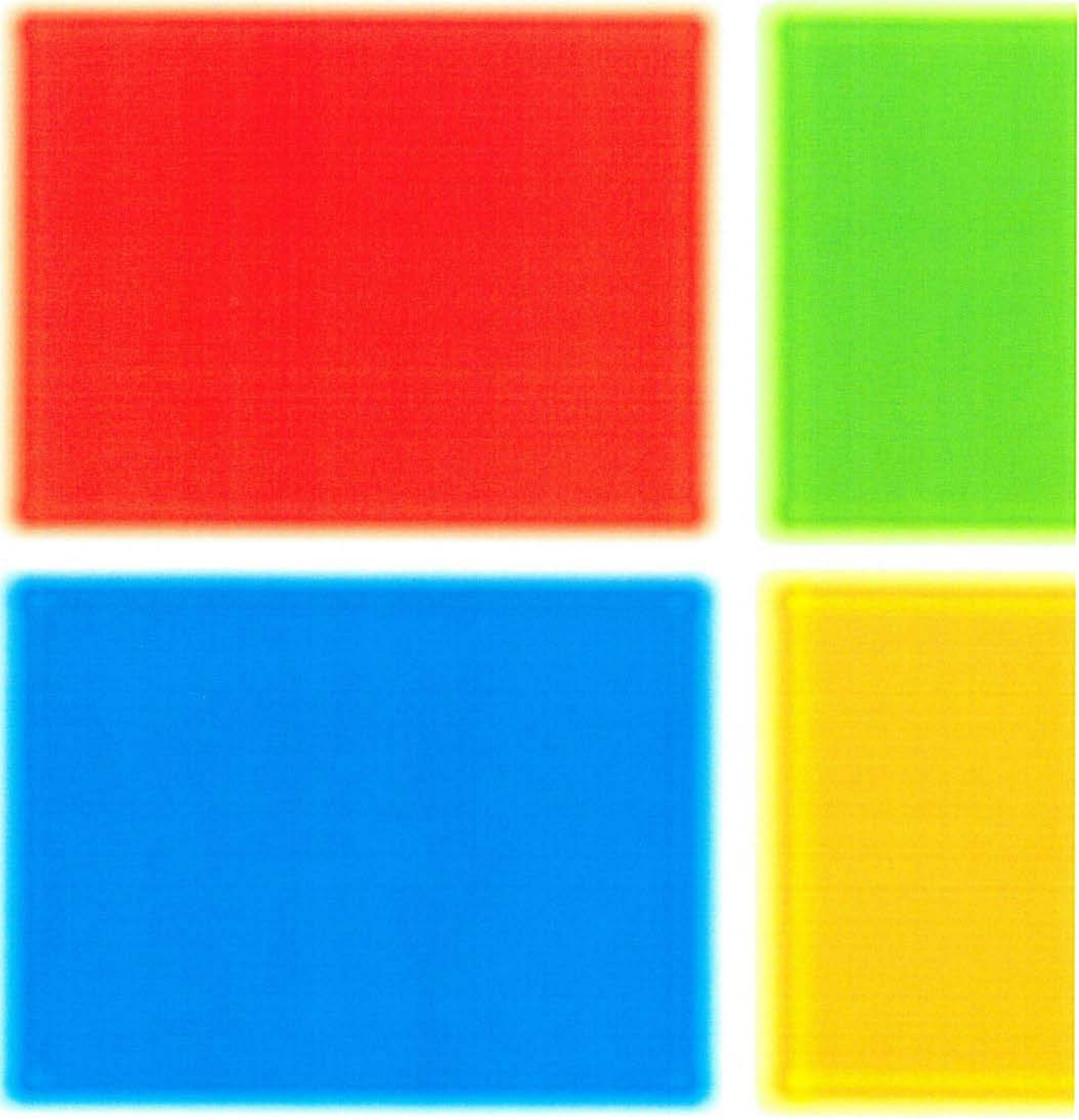
Skype



MSN



Bing



Microsoft Store

- Downloads
  - Download Center
  - Windows downloads
  - Office downloads
- Support
  - Support home
  - Knowledge base
  - Microsoft community
- About
  - The MMPC
  - Evaluating our protection
  - MMPC Privacy Statement
  - Microsoft
  - Careers
  - Citizenship
  - Company news
  - Investor relations
  - Site map
- Popular resources
  - Security and privacy blogs
  - Security Response Center
  - Security Intelligence Report
  - Microsoft Safety & Security Center
  - Malware Protection Center
  - Security for IT Pros
  - Security for developers
  - Trustworthy Computing


United States (English)

Microsoft

- Contact Us
- Terms of Use
- Trademarks
- Privacy & Cookies
- About our ads