# Beware That Software Update, It Could Be Magniber in Disguise

## Table of Contents



## Executive Report

Did you know that a Magniber ransomware infection can cost you a ransom of as much as US$2,500? The operators' favored method of delivery? Fake Windows 10 updates, putting 80% of all Windows operating system (OS) users worldwide at risk. The campaign, believed to have begun in April this year, remains a threat. Are Windows 10 users the only ones at risk, though?

We used WHOIS, IP, and DNS intelligence to uncover additional web properties potentially related to the ongoing Magniber ransomware campaign and found:

- 82 domains containing the Windows-specific strings "windows + update," "windows + patch," and "windows + security," two of which have been dubbed "malicious" by various malware engines
- 102 domains containing the generic software strings "software + update," "software + patch," and "software + security," one of which has been confirmed as a malware host
- 48 subdomains containing the Windows-specific strings "windows + update," "windows + patch," and "windows + security," two of which have been tagged "malicious" by various malware engines
- 215 subdomains containing the generic software strings "software + update," "software + patch," and "software + security," 11 of which were confirmed malware hosts

### What Web Properties Should Windows Users Be Wary Of?

The HP report referenced earlier warned Windows users to steer clear of these eight domains identified as indicators of compromise (IoCs) for the ongoing massive Magniber ransomware campaign:

- totwo[.]pw
- ittakes[.]fun
- catat[.]site
- tinpick[.]online
- pirlay[.]fun
- buyaims[.]online
- orhung[.]space
- actsred[.]site

Historical WHOIS searches for these domain names showed they were all newly created, as evidenced by their creation dates.

- Totwo[.]pw, ittakes[.]fun, catat[.]site, and tinpick[.]online were created on 7 September 2022.
- Pirlay[.]fun, buyaims[.]online, orhung[.]space, and actsred[.]site, meanwhile, were created a few days after, on 12 September 2022.

Our closer look also showed significant similarities among their name server and registrar details, namely:

- Each domain had two name servers each following the pattern "NS1[.]DOMAIN NAME[.]TLD EXTENSION." The table below provides more details.

| Domains Identified as IoCs | Name Servers |
|---|---|
| totwo[.]pw | NS1[.]TOTWO[.]PW<br>NS2[.]TOTWO[.]PW |
| ittakes[.]fun | NS1[.]ITTAKES[.]FUN<br>NS2[.]ITTAKES[.]FUN |
| catat[.]site | NS1[.]CATAT[.]SITE<br>NS2[.]CATAT[.]SITE |
| tinpick[.]online | NS1[.]TINPICK[.]ONLINE<br>NS2[.]TINPICK[.]ONLINE |
| pirlay[.]fun | NS1[.]PIRLAY[.]FUN<br>NS2[.]PIRLAY[.]FUN |
| buyaims[.]online | NS1[.]BUYAIMS[.]ONLINE<br>NS2[.]BUYAIMS[.]ONLINE |
| orhung[.]space | NS1[.]ORHUNG[.]SPACE<br>NS2[.]ORHUNG[.]SPACE |

| | |
|---|---|
| actsred[.]site | NS1[.]ACTSRED[.]SITE<br>NS2[.]ACTSRED[.]SITE |

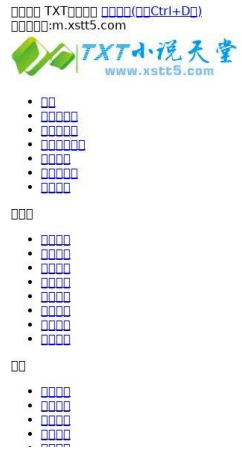
- All of the domains indicated “PDR Ltd. d/b/a PublicDomainRegistry.com” as their registrar and had redacted WHOIS records.

We then sought to find additional artifacts using the Windows-specific strings “windows + update,” “windows + patch,” and “windows + security” for Domains & Subdomains Discovery searches and uncovered 82 domains and 213 subdomains. Bulk malware checks for these showed that two domains—windows-11-update[.]com and windowsupdates-microsoft[.]org—were malicious. In addition, two subdomains—windowsecuritywarm[.]xyz and windows-security-scan[.]com—were confirmed malware hosts.

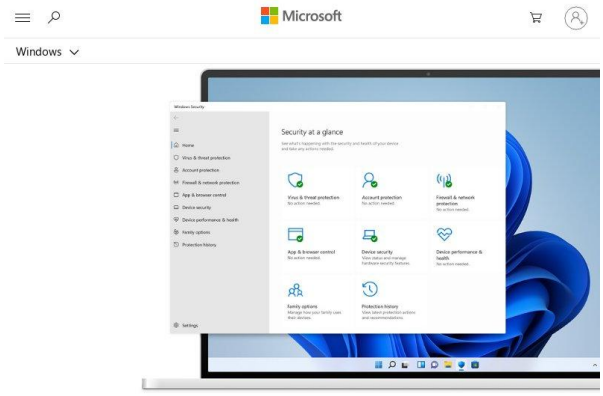
Bulk screenshot lookups, meanwhile, showed that four of these—windowspatch[.]info, windowsupdates[.]cn, windowsupdated[.]ml, and windows-update[.]win—currently host live content. Windows-update[.]win was particularly interesting since it sported the Microsoft logo despite not being owned by the company.


*Screenshot of windowspatch[.]info*


*Screenshot of windowsupdates[.]cn*

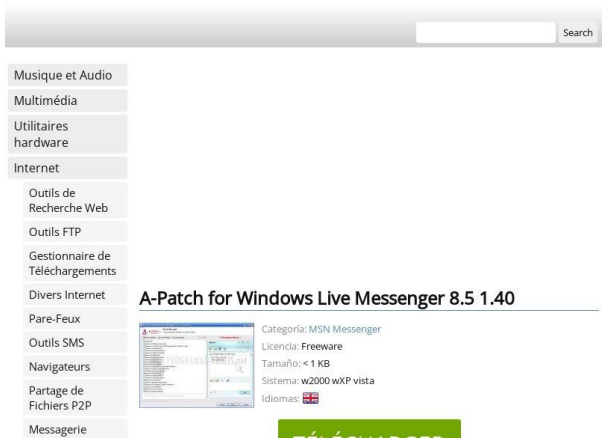



*Screenshot of windowsupdated[.]ml*

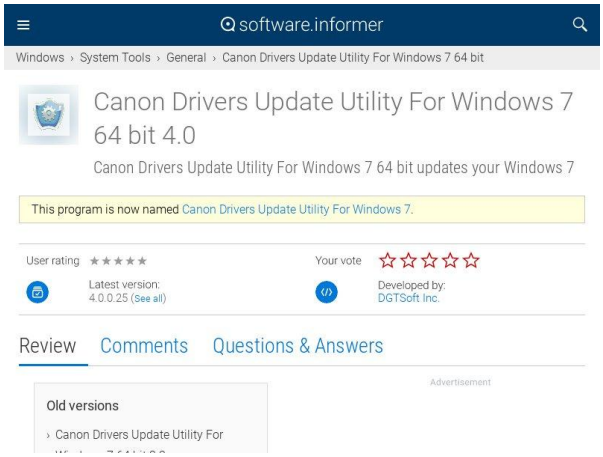



*Screenshot of windows-update[.]win*

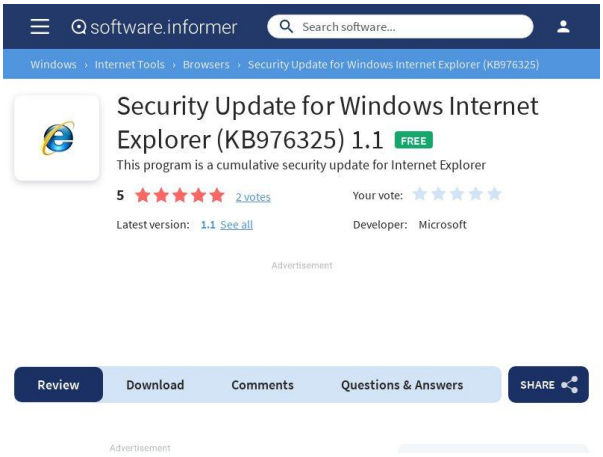
Six subdomains—a-patch-for-windows-live-messenger-8-5[.]programmesetjeux[.]com, canon-drivers-update-utility-for-windows1[.]software[.]informer[.]com, security-update-for-windows-internet-exp53[.]software[.]informer[.]com, security-update-for-windows-xp-kb2079403[.]software[.]informer[.]com, security-update-for-windows-xp-kb923980[.]software[.]informer[.]com, and shutdownwindowssecuritythreat[.]blogspot[.]com—are currently live. None of them looked particularly sinister, though.




*Screenshot of a-patch-for-windows-live-messenger-8-5[.]programmesetjeux[.]com*



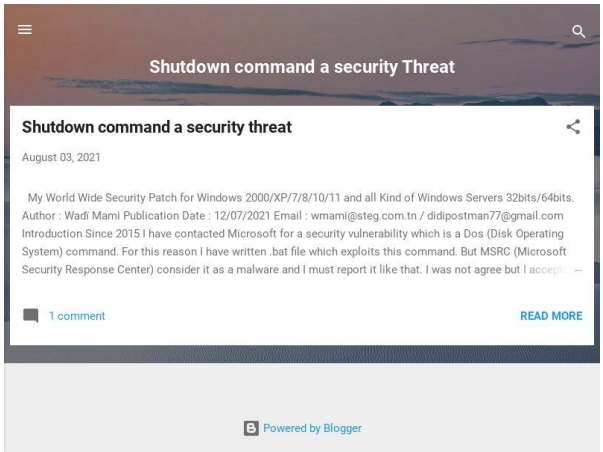

*Screenshot of canon-drivers-update-utility-for-windows1[.]software[.]informer[.]com*




*Screenshot of security-update-for-windows-internet-exp53[.]software[.]informer[.]com*


*Screenshot of security-update-for-windows-xp-kb2079403[.]software[.]informer[.]com*


*Screenshot of security-update-for-windows-xp-kb923980[.]software[.]informer[.]com*




*Screenshot of shutdownwindowssecuritythreat[.]blogspot[.]com*

## Are Windows Users the Only Ones at Risk?

To further expand the publicized list of IoCs, we sought to determine if users of other software were also at risk. We also deemed it worthwhile to identify the potential software targets.

Domains & Subdomains Discovery revealed 102 domains and 215 subdomains containing the generic strings “software + update,” “software + patch,” and “software + security,” indicating risks for users of other programs. Take a look at the word cloud below showing how many times related terms, including company names, appeared in the domains and subdomains.


One of the domains (i.e., bverestsystemsoftwareupdateb[.]xyz) and 10 of the subdomains (i.e., including updatesoftware[.]coolmethod2theupdate[.]life, softwareupdate[.]findmethod4upgrading[.]info)—containing the generic strings were confirmed malware hosts.

—

IoC expansion aided by WHOIS and DNS intelligence yet again led to the discovery of tons more artifacts that could have ties to an ongoing malware campaign or threat actors relying on similar techniques. The results of our in-depth analysis also revealed that Magniber ransomware attacks and similar threats could also put users of other software and hardware at great risk.

***If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to [contact us](#).***

## Appendix: Sample Artifacts and IoCs

### Sample Domains Containing the Windows-Specific Strings

- windowssoftwareupdate[.]net
- windowssoftwareupdate[.]com
- windowssoftwareupdate[.]org
- windowspatch[.]info
- windowsautopatch[.]com
- windows11installcrackpatch[.]ga
- windowsupdates[.]ml
- lwindowsupdate[.]ga
- windows-update[.]be
- windowsupdates[.]cn
- windowsupdated[.]ml
- updateswindows[.]ws
- lwindowsupdate[.]cf
- windows-update[.]tk
- windowsupdate[.]lol
- windows-update[.]vg
- windowsupdates[.]ga
- windows-update[.]ltd
- windowsupdate[.]pics
- windows-updates[.]ws

## Sample Domains Containing the Generic Strings

- patchsoftware[.]xyz
- patch-software[.]xyz
- patchinsoftware[.]com
- dispatchsoftwaremsb[.]com
- 5stardispatchsoftware[.]com
- dispatchdepotsoftware[.]com
- fivestardispatchsoftware[.]com
- freightdispatchingsoftware[.]com
- ztsecurity[.]software
- ezsecuritysoftware[.]ie
- web3security[.]software
- securitysoftwarepc[.]com
- computersecuritysoftwares[.]softwar e
- sipsecuritygye[.]software
- mobsecuritysoftware[.]com
- labosoftwaresecurity[.]tk
- softwaresecuritytest[.]tk
- softwaresecuritylevi[.]tk
- software-security-ap[.]tk
- websoftwaresecurity[.]com
- softwaresecurityguru[.]org
- softwarechainsecurity[.]us
- securitydashsoftware[.]org
- securitydashsoftware[.]com
- antisoftwaresecurity[.]xyz
- softwarechainsecurity[.]org
- softwarechainsecurity[.]com
- bestsecuritysoftware[.]link
- security-eye-software[.]org
- pcsecuritysoftware[.]online
- security-account[.]software
- securityguardsoftwares[.]com
- cybersecuritysoftwares[.]xyz
- bavariasecuritysoftware[.]ca
- securitysystemsoftware[.]net
- securityassurance[.]software
- cybersecuritysoftware[.]buzz
- labosoftwaresecurity2022[.]tk
- enpointsecuritysoftware[.]com
- securityofficersoftware[.]com
- currentsecuritysoftware[.]com
- softwaresecuritybootcamp[.]com
- apexsecuritysoftware[.]monster
- securitysoftwareengineer[.]com
- software-defined-security[.]de
- pc-game-security-software[.]cc
- softwaredeliverysecurity[.]com
- internetsecuritysoftwares[.]co
- internetsecuritysoftware[.]life

- zerotrustsecuritysoftware[.]com

## Sample Subdomains Containing the Windows-Specific Strings

- security-update-for-windows-xp-kb923980[.]software[.]informer[.]com
- security-update-for-windows-xp-kb2079403[.]software[.]informer[.]com
- security-update-for-windows-internet-exp53[.]software[.]informer[.]com
- irsoftwareupdate[.]z6[.]web[.]core[.]windows[.]net
- canon-drivers-update-utility-for-windows1[.]software[.]informer[.]com
- windowspatch[.]info[.]windowspatch[.]info
- windowspatch[.]info[.]wiibooster[.]com
- www[.]windowspatch[.]info[.]windowspatch[.]info
- www[.]windowspatch[.]info[.]wiibooster[.]com
- ww9[.]dispatch[.]ae1windows2008r2[.]payusaklarna[.]com
- windows-10-launch-patch-32-bit[.]en[.]8x8[.]uk
- windows-10-launch-patch-32-bit[.]en[.]booth[.]pm
- windows-10-launch-patch-64-bit[.]en[.]continu[.]nl
- a-patch-for-windows-live-messenger-8-5[.]programmesetjeux[.]com
- windowssecurityhub[.]com
- windowsecuritywarm[.]xyz
- windows365-security[.]com
- windows-securityalert[.]tk
- windowssecuritycheck[.]gdn
- windows-security-scan[.]com

## Sample Subdomains Containing the Generic Strings

- patchsoftware[.]stylohosting[.]xyz
- softwarepatches[.]blogspot[.]fi
- www[.]patchsoftware[.]stylohosting[.]xyz
- despatchpal[.]software[.]informer[.]com
- www-softwarepatch-com[.]translate[.]goog
- software-dispatch[.]teams[.]cloudflare[.]com
- update-p-patchs-hq[.]software[.]informer[.]com
- besttruckingdispatchsoftware[.]tech[.]blog
- www[.]besttruckingdispatchsoftware[.]tech[.]blog
- x-dispatch-hosted-client[.]software[.]informer[.]com
- hostmaster[.]software-background-patcher-p8473[.]123-free-download[.]com
- softwaresecurity[.]goriv[.]co
- securitysoftware[.]echosign[.]com
- software-security[.]blogspot[.]com
- sapsecuritysoftware[.]mystrikingly[.]com
- securitysoftwaretips[.]webnode[.]page

- securitysalessoftware[.]azurewebsites[.]net
- securitysoftwaretech[.]slimmerstappen[.]com
- 02-software-security[.]8x8[.]uk
- www[.]pcsecuritysoftware[.]hostingadvice4u[.]com
- securitygaurdsoftware[.]jkmonitor[.]org
- software-security-bot[.]azurewebsites[.]net
- lepidesecuritysoftware[.]convertosttopst[.]co[.]uk
- softwaresecurityteacher[.]ezyro[.]com
- www[.]securitysoftwaretech[.]slimmerstappen[.]com
- internet-security[.]software[.]informer[.]com
- www[.]securitygaurdsoftware[.]jkmonitor[.]org
- borelli-security-software[.]myshopify[.]com
- software-dahuasecurity-com[.]translate[.]goog
- antivirus-security-software[.]netlify[.]app
- security[.]dev[.]software-manager[.]siemens[.]com
- bestinternetsecuritysoftware1[.]wordpress[.]com
- desktopsecuritysoftwareguide[.]pinkcameracase[.]biz
- networkingsecuritysoftware[.]com[.]soulmatescetch[.]com
- networkingsecuritysoftware[.]com[.]productreviewpages[.]com
- esafe-security-co-ltd[.]software[.]informer[.]com
- hostmaster[.]securitysoftwaretech[.]slimmerstappen[.]com
- networkingsecuritysoftware[.]com[.]foreclosedcondos[.]net
- nextgenerationsecuritysoftware[.]cn[.]org
- networkingsecuritysoftware[.]com[.]odessaaccountant[.]com
- www[.]desktopsecuritysoftwareguide[.]pinkcameracase[.]biz
- www[.]desktopsecuritysoftwareguide[.]backpackvacuumguide[.]biz
- security[.]api[.]dev[.]software-manager[.]siemens[.]com
- zonealarm-security-suite[.]software[.]informer[.]com
- hostmaster[.]www[.]securitysoftwaretech[.]slimmerstappen[.]com
- www[.]securitythemes[.]quangtrungsoftware[.]xemtruyennhanh[.]com
- softcollection-security-system[.]software[.]informer[.]com
- wit-hdip-comp-sci-2021-software-security[.]netlify[.]app
- 02-software-security[.]dev[.]europe-west1[.]dev[.]blockchain[.]info
- hostmaster[.]computer-security-software-p12922[.]123-free-download[.]com