

# Glupteba Campaign Hits Network Routers and Updates C&C Servers with Data from Bitcoin Transactions

Appendix

## Indicators of Compromise (IoCs)

File Name	SHA-256 Hash	Attribution	Detection Name
<i>_AMQ4Y13 HLQAAqRc CAERFGQA mAFIXOBE A.exe</i>	5486f07cccc300dd939b4936daeb37 b83d4c818d1735470bf791b6fd112db 25d	Glupteba Dropper	TrojanSpy.Win32.GL UPTEBA.A
<i>cloudnet.exe</i>	ab54f3f4851aa06ce6eccafc922f0fba 6e5387bd0220fb2fbd45632a6fe6ace 7	Glupteba	TrojanSpy.Win32.GL UPTEBA.A
<i>vc.exe</i>	20e983e90144c385996eeb2edb584d 654d898c34725e149682170f870ee1 2870	Glupteba browser stealer	TrojanSpy.Win32.GLUP TEBA.A
<i>updateprofil e-0218.exe</i>	46f8d4dcdbec752ba57a682d622652 21e0a2db67a37b5ccd851dcb44b907 a32d	Glupteba browser stealer	TrojanSpy.Win32.GL UPTEBA.A
<i>updateprofil e-0321.exe</i>	1e71965e20aa50df21375a1db003e9 2823abacac1c1850c2d0922d43420e 2d30	Glupteba browser stealer	TrojanSpy.Win32.GLUP TEBA.A
<i>updateprofil e-srv1- 0520.exe</i>	69c40f971402945d188a66e1fd91179 65fd7c11af71514e3f8152a9c873b60 0d	Glupteba browser stealer	TrojanSpy.Win32.GLUP TEBA.A
<i>winboxls- 0225-2.exe</i>	b562ad8c740ba4549be9c7dc693c1f 77bd2ba3bac33128769d5a7e079bfd edec	Glupteba Router Exploiter	TrojanSpy.Win32.GLUP TEBA.A
<i>winboxls- 1008-2.exe</i>	0dedb703da8d7aeae5d6f6da3e37b3 d3fc42d0872b8470a81066a4491f245 5f2	Glupteba Router Exploiter	TrojanSpy.Win32.GLUP TEBA.A

<i>winboxls-0712.exe</i>	07d1ea5c0b4a1b437d2146fd9c918d72a16c2950d24d4c7f1f95f8409d2619b3	Glupteba Router Exploiter	TrojanSpy.Win32.GLUPTEBA.A
--------------------------	------------------------------------------------------------------	---------------------------	----------------------------

## Related URLs, IP Addresses, and Domains

- *5[.]9[.]157[.]50* (Glupteba C&C IP)
- *keepmusic[.]xyz* (Glupteba malvertising domain)
- *playfire[.]online* (Glupteba malvertising domain)
- *venoxcontrol[.]com* (Glupteba dropper C&C domain)
- *okonewacon[.]com* (Glupteba dropper C&C domain)
- *blackempirebuild[.]com* (Glupteba dropper C&C domain)
- *bigtext[.]club* (Glupteba dropper C&C domain)
- *clubhouse[.]site* (Glupteba dropper C&C domain)
- *nxtfdata[.]xyz* (Glupteba dropper C&C domain)
- *lienews[.]world* (Glupteba browser data exfiltration domain)
- *phonemus[.]net* (Glupteba dropper C&C domain)
- *takebad1[.]com* (Glupteba dropper C&C domain)

## TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

[www.trendmicro.com](http://www.trendmicro.com)

