TREND MICRO | research

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
_AMQ4Y13HLQAAqRcCAERFGQAmAFIXOBEA.exe	5486f07cccc300dd939b4936daeb37b83d4c818d1735470bf791b6fd112db25d	Glupteba Dropper	TrojanSpy.Win32.GLUPTEBA.A
cloudnet.exe	ab54f3f4851aa06ce6eccafc922f0fba6e5387bd0220fb2fbd45632a6fe6ace7	Glupteba	TrojanSpy.Win32.GLUPTEBA.A
vc.exe	20e983e90144c385996eeb2edb584d654d898c34725e149682170f870ee12870	Glupteba browser stealer	TrojanSpy.Win32.GLUPTEBA.A
updateprofile-0218.exe	46f8d4dcdbec752ba57a682d62265221e0a2db67a37b5ccd851dcb44b907a32d	Glupteba browser stealer	TrojanSpy.Win32.GLUPTEBA.A
updateprofile-0321.exe	1e71965e20aa50df21375a1db003e92823abacac1c1850c2d0922d43420e2d30	Glupteba browser stealer	TrojanSpy.Win32.GLUPTEBA.A
updateprofile-srv1-0520.exe	69c40f971402945d188a66e1fd9117965fd7c11af71514e3f8152a9c873b600d	Glupteba browser stealer	TrojanSpy.Win32.GLUPTEBA.A
winboxls-0225-2.exe	b562ad8c740ba4549be9c7dc693c1f77bd2ba3bac33128769d5a7e079bfdedec	Glupteba Router Exploiter	TrojanSpy.Win32.GLUPTEBA.A
winboxls-1008-2.exe	0dedb703da8d7aeae5d6f6da3e37b3d3fc42d0872b8470a81066a4491f2455f2	Glupteba Router Exploiter	TrojanSpy.Win32.GLUPTEBA.A

winboxls-0712.exe	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)