Profiling the Threat Actor Known as “Hagga” and His Work

Table of Contents

Executive Report

Agent Tesla, an infamous data stealer, has been plaguing Internet users since 2014. Much has been revealed about the malware, but the world didn’t come to know about one of its more adept campaign perpetrators—Hagga—until last year.

What the World Knows about Hagga So Far

Hagga is believed to have been using Agent Tesla, 2021’s sixth most prevalent malware, to steal sensitive information from his victims since the latter part of 2021. Latest research published several indicators of compromise (IoCs) related to his infrastructure, including four domains and 18 IP addresses.

We used these data points to find out more about Hagga and his criminal infrastructure. Our in-depth analysis of WHOIS, Domain Name System (DNS), and other network records uncovered:

- An additional IP address that could be part of Hagga’s malicious network
- Four Duck DNS-hosted malicious domains that could be connected to the threat
- 100 subdomains containing the string “cdec22” similar to the possibly connected subdomain artifacts uncovered
- More than 300 domains containing the strings “statusupdate” and “heavy-dutyindustry” akin to the domains identified as threat IoCs

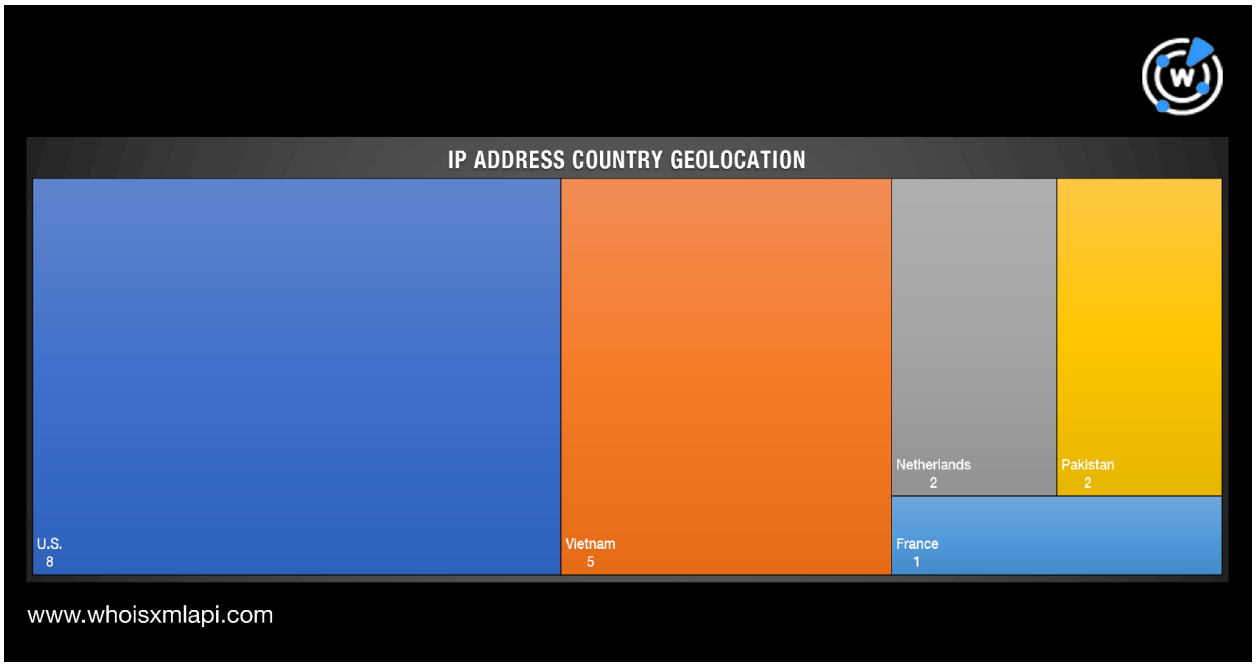
What Hagga Might Currently Be Up To?

Using the published IoCs as a jump-off point, we scoured the DNS for other artifacts that organizations should look out for.

WHOIS history searches for the four domains identified as threat IoCs showed that three of them were created in the latter part of 2021, while one is a newly registered domain (NRD). The four domains' records point to Iceland as their registrant country. Hagga also seemed to favor Namecheap as registrar.

DNS lookups for the four domain IoCs yielded an additional IP address—37[.]252[.]1[.]63—which isn't currently part of publicly accessible data sources. While it isn't currently tagged "malicious," its connection to one of the IoCs makes it suspicious and thus worth monitoring at the very least.

Contrary to the sole registrant country identified for the four domain IoCs, the 18 IP addresses were spread across five different countries, none of which were geolocated in Iceland.



In fact, close to half of the 18 IP addresses pointed to U.S. locations, followed by Vietnam (28%), the Netherlands and Pakistan (11% each), and France (6%).

Reverse IP lookups for the IP address IoCs uncovered an additional four Duck DNS-hosted domains, all of which were tagged "malware hosts" by Threat Intelligence Platform (TIP) malware checks. These are:

- cdec22[.]duckdns[.]org
- abotherrdpajq[.]duckdns[.]org
- mobibagugu[.]duckdns[.]org
- warnonmobina[.]duckdns[.]org

To further expand our list of artifacts and possible IoCs, we searched for other subdomains (hosted on platforms akin to Duck DNS) and domains containing similar strings (i.e., “cdec22,” “abotherrdpajq,” “mobibagugu,” and “warnonmobina” and “workflowstatus,” “statusupdate,” “newbotv4,” and “heavy-dutyindustry”). Domains & Subdomains Discovery provided a list of 100 subdomains with the text string “cdec22.” While none of them are considered malicious to date, their similarities with the identified artifacts should render them worthy of monitoring.

The tool also turned up 305 domains with the strings “statusupdate” and “heavy-dutyindustry,” three of which—heavy-dutyindustry[.]co, jp-statusupdate[.]com, and statusupdate-loanapproval[.]com—have been dubbed “malware hosts,” apart from the IoC heavy-dutyindustry[.]shop to date.

—

Given the threat that Agent Tesla poses—the theft of sensitive information and the repercussions that come with it (e.g., reputational, compliance-related, and financial damages to breached companies)—organizations would do well to block access to the IoCs and connected artifacts, especially the three domains found malicious, and at the very least monitor the suspicious web properties.

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 Subdomains Containing the String “cdec22”

- cdec22[.]duckdns[.]org
- bcdec222[.]skybroadband[.]com
- ea4bcdec22[.]nxcli[.]net
- spcdec22017[.]peatix[.]com
- accdec22[.]ipt[.]aol[.]com
- p4fcdec22[.]dip0[.]t-ipconnect[.]de
- ip51cdec22[.]speed[.]planet[.]nl
- direwolf-9cdec22340[.]herokuapp[.]com
- s0106589630cdec22[.]gv[.]shawcable[.]net

- cdec227f1b3d[.]database[.]azure[.]com
- m001dcdec2202[.]chcg[.]il[.]comcast[.]net
- device8057221-8cdec228[.]wd2go[.]com
- 5ef1f13a7c5c896cdec22c5a[.]keenetic[.]io
- c-cdec225c[.]41-5-64736c10[.]bbcust[.]telenor[.]se
- f5cdec22d3cefe4d823a790cfd1896[.]pamx1[.]hotmail[.]com
- 8d5fcde7-1ee7-cb8e-a6fc-acdec221f7f3[.]z1[.]dca0[.]com
- 7483c21fe8510406da510432581405cdec221[.]id[.]ui[.]direct
- eb9853772cd1548400ece487281d7593cdec2277[.]vercel-workers[.]com
- w-t-loc-4cdec22b[.]ftp[.]private[.]antares-test[.]windows-int[.]net
- z3napitest-d6e07b549029f1bbcdec22f71b6ccd54[.]zendesk[.]com

Sample Domains Containing the Strings “statusupdate” and “heavy-dutyindustry”

- statusupdate[.]ml
- statusupdate[.]ga
- statusupdate[.]us
- statusupdate[.]me
- statusupdate[.]gr
- statusupdate[.]co
- statusupdate[.]de
- statusupdate[.]uk
- statusupdate[.]io
- statusupdate[.]ca
- statusupdate[.]nu
- statusupdate[.]tk
- statusupdate[.]in
- statusupdate[.]it
- statusupdate[.]id
- statusupdate[.]org
- statusupdates[.]de
- statusupdate[.]com
- statusupdate[.]biz
- statusupdate[.]xyz
- statusupdates[.]co
- statusupdater[.]tk
- statusupdate[.]pro
- statusupdate[.]top
- statusupdate[.]net
- statusupdates[.]us
- statusupdates[.]tk
- statusupdates[.]uk
- statusupdater[.]ca
- statusupdate[.]art
- statusupdated[.]com
- statusupdates[.]ooo
- statusupdate[.]asia
- fbstatusupdate[.]tk
- statusupdatebc[.]ca
- statusupdates[.]com
- istatusupdate[.]com
- statusupdate[.]info
- statusupdates[.]org
- statusupdate[.]club
- statusupdate1[.]com
- statusupdates[.]net
- statusupdates[.]xyz
- statusupdater[.]com

- statusupdatebk[.]com
- statusupdate[.]video
- statusupdates[.]info
- statusupdates[.]live
- statusupdatesd[.]com
- heavy-dutyindustry[.]co