WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Both Aged and New Domains Play a Role in the NDSW/NDSX Malware Campaign

Table of Contents

Executive Report

Cyber attackers typically use newly registered domains (NRDs) in their campaigns to evade detection, particularly since the implementation of privacy protection in WHOIS records. But some also use aged domains like the SolarWinds hackers to render a sense of legitimacy to their pages.

The threat actors behind the NDSW/NDSX malware campaign used both NRDs and aged domains, likely to get the best of both worlds. But the digital breadcrumbs they left behind could help investigators get a step closer to catching them. Our in-depth analysis revealed these findings:

- 4 unredacted registrant email addresses from the historical WHOIS records of the domains identified as threat indicators of compromise (IoCs)
- 208 domains that used the same registrant email addresses as the aged domain IoCs
- 1 additional IP address that the domain IoCs resolved to
- 167 domains that shared the domain IoCs' IP addresses, one of which is deemed malicious
- 8 domains that shared common strings with the IoCs ("sync + adv.," "static + visit," and "ads + profit + network")

What Publicly Available Reports Have Told Us

The Parrot TDS campaign, which primarily used NDSW/NDSX malware and has been active since February 2019, has affected 16,500 websites to date. Attackers compromised the sites by injecting malicious JavaScript into their HTML code. When executed, the malware notifies users of infected computers of fake plug-in updates that when installed runs other malware. So even if NDSW/NDSX is removed, the other malware allows threat actors to maintain their foothold in affected networks.

Publicly available sources also identified eight domains and nine IP addresses as NDSW/NDSX malware campaign IoCs. We used these web properties as jump-off points for our deep dive.

What Our Deep Dive Revealed

WHOIS Record Revelations

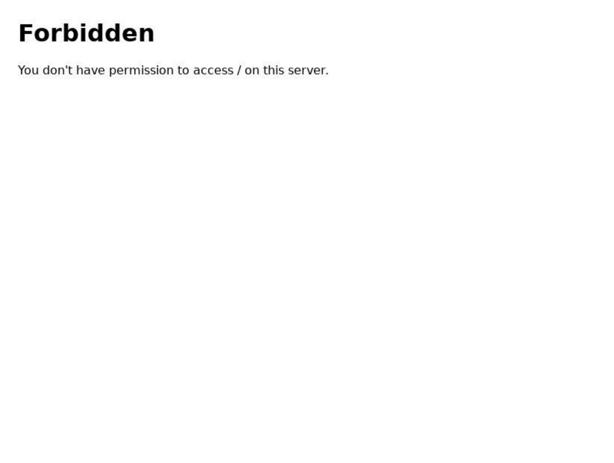
A bulk WHOIS lookup for the eight domain IoCs showed that seven of the domains' WHOIS records are privacy-protected while one is up for sale. Four of the domain IoCs—syncadv[.]com, statclick[.]net, clickstat360[.]com, and cachespace[.]net—are at least 3 years old, the oldest being statclick[.]net.

Even more interesting, however, is the appearance of an unredacted registrant email address in the historical WHOIS records of three of these domains—syncadv[.]com, statclick[.]net, and clickstat360[.]com. Could the email address's owner be part of the NDSW/NDSX malware campaign crew? Or was he simple a domainer or small business owner whose name got raked in the mud?

Two other unredacted registrant email addresses were found in the historical WHOIS records of syncadv[.]com. These seemed to belong to legitimate business owners, however. Another unredacted registrant email address was also found in the historical WHOIS records of adsprofitnetwork[.]com, though this could belong to a domainer.

Screenshot Lookup Findings

All of the domain IoCs seem harmless if accidentally accessed, as they showed either blank or server index pages.

 **Forbidden** You don't have permission to access / on this server. *Screenshot of cachespace[.]net, statclick[.]net, and syncadv[.]com*	*Screenshot of webcachestorage[.]com, webcachespace[.]net, staticvisit[.]net, clickstat360[.]com, and adsprofitnetwork[.]com*

Three of the oldest domains showed an index page error while the NRDs led to blank pages.

Reverse WHOIS Search Results

In an effort to expand the list of potential IoCs and artifacts for this threat, we used the unredacted registrant email addresses as historical reverse WHOIS search terms and found an additional 208 domains. While none of them are currently tagged malicious, having ties to the suspicious registrants, particularly of syncadv[.]com, statclick[.]net, and clickstat360[.]com, may make them worthy of monitoring for signs of malicious activity at least.

DNS Investigation Revelations

Subjecting the domain IoCs to DNS lookups added one IP address—217[.]23[.]6[.]22—to the nine Avast has identified. This IP address hosts 167 additional domains from a reverse IP lookup that could have ties to the threat. A bulk Threat Intelligence Platform (TIP) malware check showed that one of the additional domains—deddi[.]ru—is a malware host.

Domains & Subdomains Discovery Findings

Further expanding the list of possibly connected web properties, we used the following string combinations as Domains & Subdomains Discovery search strings:

- “sync + adv.”
- “static + visit”

- “ads + profit + network”

We discovered 11 additional domains. While none of them have been dubbed malicious so far, they do share common strings with the IoCs.

The Verdict

Our analysis findings revealed interesting insights, such as commonalities among the IoCs that led to the discovery of possibly related web properties. Individuals and organizations alike would do well to treat the artifacts we uncovered as suspicious at least to ensure utmost system and network protection.

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

Domains That Shared Some of the IoCs’ Unredacted Registrant Email Addresses

- multinetfze[.]com
- psladubai[.]com
- europluschemicals[.]com
- crown-uniforms[.]com
- agrocomtrade[.]com
- hellenic-shipping[.]com
- bilalindustries[.]com
- munaff[.]com
- theholymonth[.]com
- claremontintl[.]com
- chamcaar[.]com
- navispec[.]com
- ranchout[.]com
- ataraintl[.]com
- qresume[.]com
- minefert[.]com
- minefertdmcc[.]com
- wordhubble[.]com
- suamc[.]com
- persona-me[.]com
- projectlayer[.]com
- itdxb[.]com
- lexx-zone[.]com
- shaadiclicks[.]com
- kababrecipes[.]com
- ozonelimited[.]com
- jobz[.]one
- edelman[.]tech
- trebuchetadvisory[.]com
- mudassar[.]info
- ozoneconsultants[.]org
- highdecor[.]info
- desertsafari[.]info
- agrocom[.]me
- techneek[.]in
- thinkbig[.]in

- ranchout[.]in
- mivbinfotech[.]co
- supremesteel[.]co
- theholiday[.]guide
- gravitycontracting[.]com
- sync-adv[.]com
- mahafied[.]com
- umlaboratory[.]com
- spoilyourwall[.]com
- sherwoodintl[.]com
- myteestudio[.]com
- hobby55[.]com
- citydunes[.]com
- bizhubble[.]com

Domains That Shared Some of the IoCs’ IP Hosts

- admin[.]dev[.]moseta[.]eu
- admin[.]moseta[.]eu
- ahatova[.]ru
- baysangur[.]ru
- beluygorod[.]ru
- bettuzo[.]ru
- blostera[.]ru
- boffeer[.]ru
- bordearxsa[.]ru
- bristols[.]ru
- bsopen[.]ru
- budasistents[.]com
- bukiid[.]ru
- burotll[.]ru
- caceqyo[.]ru
- codypya[.]ru
- cpanel[.]moseta[.]eu
- cpcalendars[.]moseta[.]eu
- cpcontacts[.]moseta[.]eu
- cyua[.]ru
- dadegoke[.]ru
- de[.]moseta[.]eu
- deddi[.]ru
- derrnail[.]ru
- desf[.]ru
- dev[.]moseta[.]eu
- dinwoll[.]ru
- doeser[.]ru
- domrass[.]ru
- emnuty[.]ru
- englhome-glass[.]ru
- epkeu[.]ru
- expil[.]ru
- fashstyle[.]ru
- forum[.]moseta[.]eu
- greemaz[.]ru
- knopo[.]ru
- koketka[.]top
- kolomensky[.]com
- kshark[.]ru
- kxmnt[.]ru
- lignety[.]ru
- livsa[.]ru
- mail[.]baysangur[.]ru
- mail[.]beluygorod[.]ru
- mail[.]bordearxsa[.]ru
- mail[.]bristols[.]ru
- mail[.]bsopen[.]ru
- mail[.]budasistents[.]com
- mail[.]caceqyo[.]ru

Domains That Shared Some of the IoCs’ Strings

- syncadv[.]it
- syncadv[.]net

- sync-adv[.]com
- syncroadv[.]com
- syncapadv[.]com
- synchroadv[.]com
- staticinvisit[.]tk
- adsprofit[.]network